Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management

Dissertation

an der

Fakultät für Mathematik, Informatik und Statistik
der
Ludwig-Maximilians-Universität München

vorgelegt von

Wolfgang Hommel

Tag der Einreichung: 18. Juni 2007

Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management

Dissertation

an der

Fakultät für Mathematik, Informatik und Statistik
der
Ludwig-Maximilians-Universität München

vorgelegt von

Wolfgang Hommel

Tag der Einreichung: 18. Juni 2007
Tag des Rigorosums: 27. Juli 2007

1. Berichterstatter: **Prof. Dr. Heinz-Gerd Hegering**, Universität München
2. Berichterstatter: **Prof. Dr. Arndt Bode**, Technische Universität München

Danksagung

Die vorliegende Arbeit entstand im Rahmen meiner Tätigkeiten als wissenschaftlicher Mitarbeiter am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften und als Mitglied des von Prof. Dr. Heinz-Gerd Hegering geleiteten Munich Network Management Teams.

Mein besonderer Dank gilt an dieser Stelle meinem Doktorvater, Prof. Dr. Heinz-Gerd Hegering, der diese Arbeit von den ersten Ideen an unterstützt und durch eine Vielzahl konstruktiver Anregungen maßgeblich zur ihrem Gelingen beigetragen hat. Sehr herzlich bedanke ich mich ebenfalls bei Herrn Prof. Dr. Arndt Bode, der nicht nur wertvolle Hinweise zum Inhalt der Arbeit geliefert hat, sondern auch im Rahmen des Projekts IntegraTUM ein ideales Umfeld schuf, in dem die erarbeiteten Konzepte in die Praxis umgesetzt werden können.

Ich danke ferner allen Kolleginnen und Kollegen am Leibniz-Rechenzentrum, die mir die notwendigen Freiräume für wissenschaftliche Arbeiten eingeräumt und den Rücken im Tagesgeschäft freigehalten haben. Allen früheren und aktuellen Kolleginnen und Kollegen im Munich Network Management Team danke ich für die immer motivierenden Diskussionen und die erfolgreiche Zusammenarbeit in vielen Bereichen, die auch diese Arbeit beeinflusst haben. Ebenso gebührt allen denjenigen mein Dank, die im Rahmen von Diplomarbeiten und Praktika zum Umfeld dieser Arbeit beigetragen haben.

Nicht zuletzt danke ich meinen Eltern aufrichtig für ihre bedingungslose Unterstützung, die mir Zeit meines Lebens alle Wege geebnet hat, die ich beschritten habe. Besonders danke ich Elena; ohne ihren vorbehaltlosen Rückhalt und ihre Geduld wäre diese Arbeit nicht möglich gewesen.

München, im Sommer 2007

Kurzfassung

Als essentielle Komponente des IT-Security Managements umfasst das Identity & Access Management (I&AM) sämtliche organisatorischen und technischen Prozesse der Verwaltung von Dienstnutzern einer Einrichtung und deren Berechtigungen; dabei werden die Datenbestände verschiedenster autoritativer Datenquellen wie Personal- und Kundenverwaltungssysteme aggregiert, korreliert und in aufbereiteter Form den IT-Services zur Verfügung gestellt. Das Federated Identity Management (FIM) hat zum Ziel, die so geschaffenen integrierten Datenbestände auch organisationsübergreifend nutzbar zu machen; diese Funktionalität wird beispielsweise im Rahmen von Business-to-Business-Kooperationen, Outsourcing-Szenarien und im Grid-Computing zunehmend dringender benötigt. Die Vermeidung von Redundanz und Inkonsistenzen, aber auch die garantierte Verfügbarkeit der Daten und die Einhaltung von Datenschutzbestimmungen stellen hierbei besonders kritische Erfolgsfaktoren dar.

Mit der Security Assertion Markup Language (SAML), den Spezifikationen der Liberty Alliance und WS-Federation als integralem Bestandteil des Web Services WS-*-Protokollstacks haben sich industrielle und partiell standardisierte technische Ansätze für FIM herauskristallisiert, deren praktische Umsetzung jedoch noch häufig an der nur unzureichend geklärten, komplexen organisatorischen Einbettung und den technischen Unzulänglichkeiten hinsichtlich der Integration in bestehende IT-Infrastrukturen scheitert.

In dieser Arbeit wird zunächst eine tiefgehende und in diesem Umfang neue Anforderungsanalyse durchgeführt, die neben I&AM und FIM auch die als User-Centric Identity Management (UCIM) bezeichnete Benutzerperspektive berücksichtigt; die Schwerpunkte der mehr als 60 strukturierten und gewichteten Anforderungen liegen dabei auf der Integration von I&AM- und FIM-Systemen sowohl auf der Seite der Organisation, der die Benutzer angehören (Identity Provider), als auch beim jeweiligen Dienstleister (Service Provider), und auf dem Einbezug von organisatorischen Randbedingungen sowie ausgewählten Sicherheits- und Datenschutzaspekten.

Im Rahmen eines umfassenden, gesamtheitlichen Architekturkonzepts wird anschließend eine Methodik zur systematischen Integration von FIM-Komponenten in bestehende I&AM-Systeme erarbeitet. Neben der präzisen Spezifikation der technischen Systemschnittstellen, die den bestehenden Ansätzen fehlt, fokussiert diese Arbeit auf die organisatorische Eingliederung aus Sicht des IT Service Managements, wobei insbesondere das Security Management und das Change Management nach ITIL vertieft werden.

Zur Kompensation weiterer grundlegender Defizite bisheriger FIM-Ansätze werden im Rahmen eines Werkzeugkonzepts fünf neue FIM-Komponenten spezifiziert, die auf eine verbesserte Interoperabilität der FIM-Systeme der an einer so genannten Identity Federation beteiligten Organisationen abzielen. Darüber hinaus wird auf Basis der eXtensible Access Control Markup Language (XACML) eine policy-basierte Privacy Management Architektur spezifiziert und integriert, die eine dezentrale Steuerung und Kontrolle von Datenfreigaben durch Administratoren und Benutzer ermöglicht und somit essentiell zur Einhaltung von Datenschutzauflagen beiträgt.

Eine Beschreibung der prototypischen Implementierung der Werkzeugkonzepte mit einer Diskussion ihrer Performanz und die methodische Anwendung des Architekturkonzepts auf ein komplexes, realistisches Szenario runden diese Arbeit ab.

Abstract

Being an essential component of IT security management, Identity & Access Management (I&AM) covers the organizational and technical processes of administering an institution's users and their authorizations; by aggregating and correlating user profiles from various authoritative data sources, such as human resource and customer relationship management systems, refined account information can be provided to the IT services. Using these integrated user databases in a cross-organizational context is the overall goal of Federated Identity Management (FIM); the demand for such functionality is increasing by leaps and bounds, e. g. in business-to-business co-operations, outsourcing scenarios and the field of Grid computing. Avoiding redundancy and inconsistencies as well as the guaranteed availability of remote data and compliance with privacy laws and user acceptance criteria are highly critical success factors.

Currently, three industrial and partially standardized FIM approaches are available: the Security Assertion Markup Language (SAML), the Liberty Alliance's specifications, and WS-Federation, which is tightly coupled with several other parts of the web services WS-* protocol stack. However, their practical adoption often fails due to the organizational and technical complexity of the major task to integrate them into existing IT infrastructures, especially because a concise specification of the interfaces to I&AM systems is missing.

In the first part of this thesis, a profound and comprehensive analysis is presented, which additionally covers the so-called User-Centric Identity Management (UCIM) that focuses on identity management from the user's point of view and introduces several new concepts which are also relevant to FIM. Categorized into functional, non-functional, organizational as well as privacy- and security-specific categories, more than sixty weighted criteria for the identity provider as well as the service provider side are discussed with a strong focus on the seamless integration of I&AM and FIM systems and the underlying business processes.

As part of the holistic, integrated I&AM and FIM architecture conceived in this thesis, a methodology to systematically integrate FIM components into existing I&AM systems has been developed. Besides the precise specification of technical interfaces to I&AM components, special emphasis has been put on the thorough organizational integration: concerning the IT service management processes, dependencies and effects on the security management and the change management according to ITIL have been investigated in detail.

To compensate several further shortcomings of existing approaches, five new FIM components have been specified in a FIM tool concept, which enhance the interoperability of I&AM and FIM systems in heterogeneous identity federations, especially when an organization is a member of multiple federations. Based on the eXtensible Access Control Markup Language (XACML), a policy-based privacy management architecture has been designed and integrated, which enables administrators and users to restrict and control the flow of personally identifiable information (PII) in a decentralized and fine-grained manner, and thus contributes technical capabilities for the fulfillment of legal constraints.

The thesis is concluded by a description of a prototypical implementation of the tool concepts as well as a discussion of their performance characteristics and the application of the designed architecture to a complex, realistic scenario.

Inhaltsverzeichnis

Kapitel 1.

Einleitung

Inhalt dieses Kapitels

Unter der Prämisse betriebswirtschaftlicher Effizienz variiert das Spektrum der von einem IT-Dienstleister angebotenen Services mit dem Bedarf seiner Kunden. Technologische Fortschritte, Fluktuation der Kunden und deren sich wandelnde Anforderungen führen zu einer hohen Dynamik, die per se die Komplexität des Dienstmanagements erhöht. Ein zentraler Bestandteil des Managements von Diensten ist, dass die Benutzer im Allgemeinen individuell identifiziert werden müssen; Ausnahmen bilden beispielsweise pro Kunde kollektiv oder pauschal abgerechnete und explizit anonym nutzbare Dienste. Die eindeutige Identifikation eines Benutzers ist die Voraussetzung für seine Authentifizierung und Autorisierung; weiterhin wird sie unter anderem für das Abrechnungswesen (Accounting) und die sicherheitstechnische Überwachung (Auditing) im Rahmen des Qualitätsmanagements benötigt. Der Aufwand für diese Managementaufgaben steigt mit der Anzahl der Kunden und Benutzer sowie den von diesen jeweils genutzten Diensten.

Während sich für das Management von Netz- und Systemkomponenten integrierte Lösungen durchgesetzt haben, entwickelten sich Dienste auf Applikationsebene historisch weitgehend unabhängig voneinander, da diese in der Regel nur wenige Abhängigkeiten untereinander aufweisen und lange Zeit keine entsprechende Standardisierung der Schnittstellen existierte; im Rahmen service-orientierter Architekturen (SOA) wird die lose Koppelung und Komposition von Diensten auf Basis formal definierter Schnittstellen inzwischen explizit angestrebt. Die meisten Dienste haben eigene, lokale Benutzerverwaltungen, in denen alle für die Dienstnutzung und das Dienstmanagement notwendige Daten über die Anwender eingetragen und gepflegt werden müssen. Durch die dabei häufig auftretende Redundanz ergeben sich neben einem hohen administrativem Zusatzaufwand im praktischen Betrieb auch Dateninkonsistenzen und damit Sicherheitsprobleme: So kann bei nicht vorhandenem Datenabgleich zwischen den Benutzerverwaltungen der einzelnen Dienste keine automatische vollständige Sperrung

einzelner Benutzer, beispielsweise bei missbräuchlicher Verwendung, erfolgen. Dieses Phänomen äußert sich beispielsweise darin, dass ehemalige Mitarbeiter nicht selten noch monatelang Zugriff auf IT-Ressourcen des früheren Arbeitgebers haben, und ist mit erheblichen wirtschaftlichen Risiken verbunden.

Durch die Zusammenfassung der Benutzerdatenbestände einzelner Dienste in Verzeichnisdiensten wie NIS und LDAP wurden technische Lösungen umgesetzt, die jedoch häufig organisatorische und juristische Aspekte vernachlässigten und aufgrund technischer Inkompatibilitäten nur Dienstgruppen bildeten, aber kein User Management für *alle* Dienste ermöglichten. Erst mit dem Aufkommen des Identity Management Paradigmas rückte die ganzheitliche Betrachtung von Personen einschließlich der von ihnen wahrgenommenen Rollen statt ihrer einzelnen Benutzerkonten und die IT-Unterstützung der Geschäftsprozesse des IT-Dienstleisters durch entsprechende Managementworkflows in den Mittelpunkt.

Mittlerweile hat sich der Begriff **Identity & Access Management (I&AM)** durchgesetzt und bezeichnet Softwaresysteme, die eine organisationsinterne, zentralisierte Verwaltung von Personen und deren Berechtigungen zum Zugriff auf die vorhandenen IT-Ressourcen erlauben. Sie bestehen üblicherweise aus einer Datenbasis, meist in Form eines LDAP-basierten Verzeichnisdienstes, Schnittstellen („Konnektoren“) zu den angeschlossenen Datenquellen und den gespeisten Diensten, sowie webbasierten Managementinterfaces für die Administratoren und Benutzer. Der Abdeckungsgrad von I&AM-Lösungen endet de facto an den Grenzen der jeweiligen Organisation.

Allerdings ist inzwischen sowohl im industriellen als auch im akademischen Umfeld die informationstechnische Unterstützung organisationsübergreifender Geschäftsprozesse essentiell. In den Bereichen des Business-to-Business Outsourcings werden von großen Rechenzentren unter Schlagworten wie Utility Computing und On-Demand Computing für individuelle Aufgaben optimal portionierte IT-Ressourcen zur Verfügung gestellt; im Rahmen des Supply Chain Managements müssen oftmals mehrere tausend Organisationen gemeinsame IT-Ressourcen nutzen und effizient miteinander kommunizieren können. Beim Grid Computing werden so genannte Virtuelle Organisationen (VOs) gebildet, deren Zusammensetzung mit der Weiterentwicklung der Grid-Middleware zunehmend durch Dynamik gekennzeichnet ist.

Da die Verwaltung der Benutzer traditionell nur organisationsintern erfolgte, wurde es notwendig, sämtliche externe Benutzer und deren Berechtigungen auch lokal zu erfassen, wodurch sich wiederum Redundanzen, Inkonsistenzen und massiver Administrationsaufwand ergaben. Unter dem Begriff **Federated Identity Management (FIM)** werden zurzeit Managementarchitekturen entwickelt, die eine **verteilte Benutzerverwaltung** ermöglichen sollen. Jeder Benutzer gehört dabei zu mindestens einer Heimatorganisation, die als **Identity Provider (IDP)** bezeichnet wird. Die Anbieter externer Ressourcen und Dienste, bezeichnet als **Service Provider (SP)**, sollen über dedizierte FIM-Protokolle die benötigten Informationen über einen Benutzer von dessen IDP abrufen können. Die Qualität und Verfügbarkeit der so zu ermittelnden Daten wird über vertragliche Vereinbarungen (Service Level Agreements, SLAs) zwischen den an einer **Identity Federation** beteiligten Organisationen gesichert.

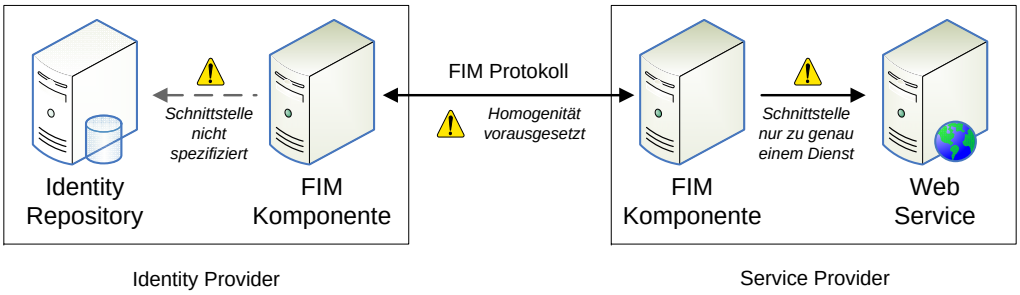


Abbildung 1.1.: Ausgangssituation: Unzureichende Integration von I&AM und FIM

1.1. Motivation und Zielsetzung

I&AM Lösungen sind technisch bereits ausgereift; ihre Umsetzung ist jedoch – insbesondere aufgrund der notwendigen Integration in die lokalen Geschäftsprozesse – in vielen Organisationen noch nicht abgeschlossen. Die FIM-Technologien befinden sich dagegen derzeit noch in einer Entwicklungsphase und haben bislang keine weite Verbreitung gefunden; daraus resultiert in der Praxis das Problem, einerseits für zukünftige Erweiterungen relevante FIM-Aspekte bei der Implementierung von I&AM-Lösungen nur unzureichend zu berücksichtigen und andererseits die Entwicklung von FIM-Komponenten weitgehend unabhängig von etablierten I&AM-Methoden voranzutreiben.

Abbildung 1.1 stellt die unzureichende Integration von I&AM- und FIM-Lösungen stark vereinfacht dar. Standardisierte FIM-Technologien weisen derzeit eine Reihe an Defiziten auf, die in Kapitel 3 im Detail diskutiert werden und die momentan geringe Implementierungsrate, Verbreitung und Akzeptanz mit verursachen:

- Auf der Seite des Identity Providers wird implizit die Existenz einer Datenbasis vorausgesetzt, die den für FIM zu nutzenden Datenbestand enthält. Ein solches **Identity Repository** wird üblicherweise von der eingesetzten I&AM-Lösung implementiert; die FIM-spezifischen **Anforderungen** und die **Schnittstellen** zu den FIM-Komponenten bleiben jedoch unspezifiziert.
- Für Service Provider ist nur die Anbindung einzelner **Web Services** bzw. webbasierter Applikationen spezifiziert; die Versorgung mit zur Diensterbringung notwendigen Benutzerdaten – im I&AM-Umfeld als **User Provisioning** bezeichnet – von mehreren Diensten, insbesondere auch solcher, die – was derzeit auf die überwiegende Mehrheit zutrifft – nicht auf Web Services basieren, wird nicht definiert. Da aktuelle FIM-Ansätze nur einen Bruchteil der Servicepalette abdecken und die zusätzliche Erfassung externer Benutzer nicht vollständig ersetzen könnten, bedeutet der praktische Einsatz derzeit eine Erhöhung statt der erhofften Reduzierung der Managementkomplexität, da eine neue Datenquelle und ein zu den existierenden Workflows paralleler Datenverarbeitungsprozess eingeführt werden.
- Hinsichtlich der **Interoperabilität** erweisen sich insbesondere syntaktische und semantische Differenzen der Informationsmodelle in den I&AM-Lösungen der Föderationsmit-

glieder als sehr hinderlich. Sie kommen primär durch die Heterogenität der eingesetzten Software in den Bereichen der Personal- und Kundenverwaltung zustande, die durch I&AM-Produkte nicht kompensiert werden; beispielsweise haben sich in der Praxis keine Standardisierungsversuche dafür, welche Daten mit welcher Syntax und Semantik über Mitarbeiter und Kunden erfasst und im Rahmen von FIM bereitgestellt werden sollen, so durchgesetzt, dass sie produkt- und organisationsübergreifend vollwertig eingesetzt werden könnten.

- Die Implementierung von FIM stößt bei Administratoren und Change Management Verantwortlichen auf Skepsis, da die **Sicherheitsaspekte** von FIM bislang nur unzureichend untersucht wurden. Zwar existieren Securityanalysen der FIM-Protokolle selbst, über die Sicherheit der Integration mit I&AM-Komponenten und durch FIM erst geschaffene Herausforderungen im Bereich der Sicherheit ganzer Föderationen liegen aber derzeit nur wenige Erkenntnisse vor.

- Benutzern, deren Daten im Rahmen von FIM zwischen Organisationen ausgetauscht werden sollen, werden keine oder nur unzureichende **Steuerungs- und Kontrollmechanismen** für die Freigabe ihrer Daten zur Verfügung gestellt. Diese sind bei einem Einsatz von FIM im Produktionsbetrieb jedoch aus datenschutzrechtlichen Gründen, beispielsweise im Rahmen der informationellen Selbstbestimmung, zwingend erforderlich und die Grundvoraussetzung für die **Akzeptanz** des Systems durch die Benutzer.

Aus diesen Gründen beschränkt sich der praktische Einsatz vom FIM derzeit auf wenige, applikationsspezifische Föderationen und Testumgebungen.

Das **Ziel** dieser Arbeit ist deshalb, auf Basis einer gesamtheitlichen Betrachtung von I&AM und FIM *technische Lösungen* zu entwickeln und *Vorgehensweisen* zu definieren, die es ermöglichen, die Konzeption und Implementierung von FIM-Lösungen so zu flexibilisieren, dass eine nahtlose Integration sowohl in das jeweils lokal vorhandene I&AM-System als auch in bereits bestehende Föderationen effizient umsetzbar wird. Die wesentlichen Bestandteile umfassen dabei die folgenden Aspekte:

- Zur Integration von I&AM- und FIM-Systemen werden die Schnittstellen ihrer Einzelkomponenten definiert, Gruppierungen von Komponenten zu **Architekturmustern** („Design Patterns“) vorgenommen und die Kombination zu **Referenzarchitekturen** demonstriert. Die wesentlichen Aspekte sind dabei die Unterstützung mehrerer **Rollen** der jeweiligen Organisation, die beispielsweise sowohl Identity Provider als auch Service Provider in der Föderation sein kann, sowie die Integration des Security und Change Managements.

- Auf Basis einer Anforderungsanalyse und der Untersuchung der Defizite existierender Lösungen wird die Notwendigkeit zusätzlicher FIM-Funktionalität in den Bereichen **Interoperabilität**, **Privacy Control** und **Service Provisioning** abgeleitet, ohne die eine effiziente Inbetriebnahme von Föderationen nicht möglich ist. In diesen Bereichen werden **neue FIM-Komponenten** entworfen, ihre Funktionsweisen und Schnittstellen spezifiziert und prototypische Implementierungen im Rahmen der konzipierten Gesamtarchitektur demonstriert.

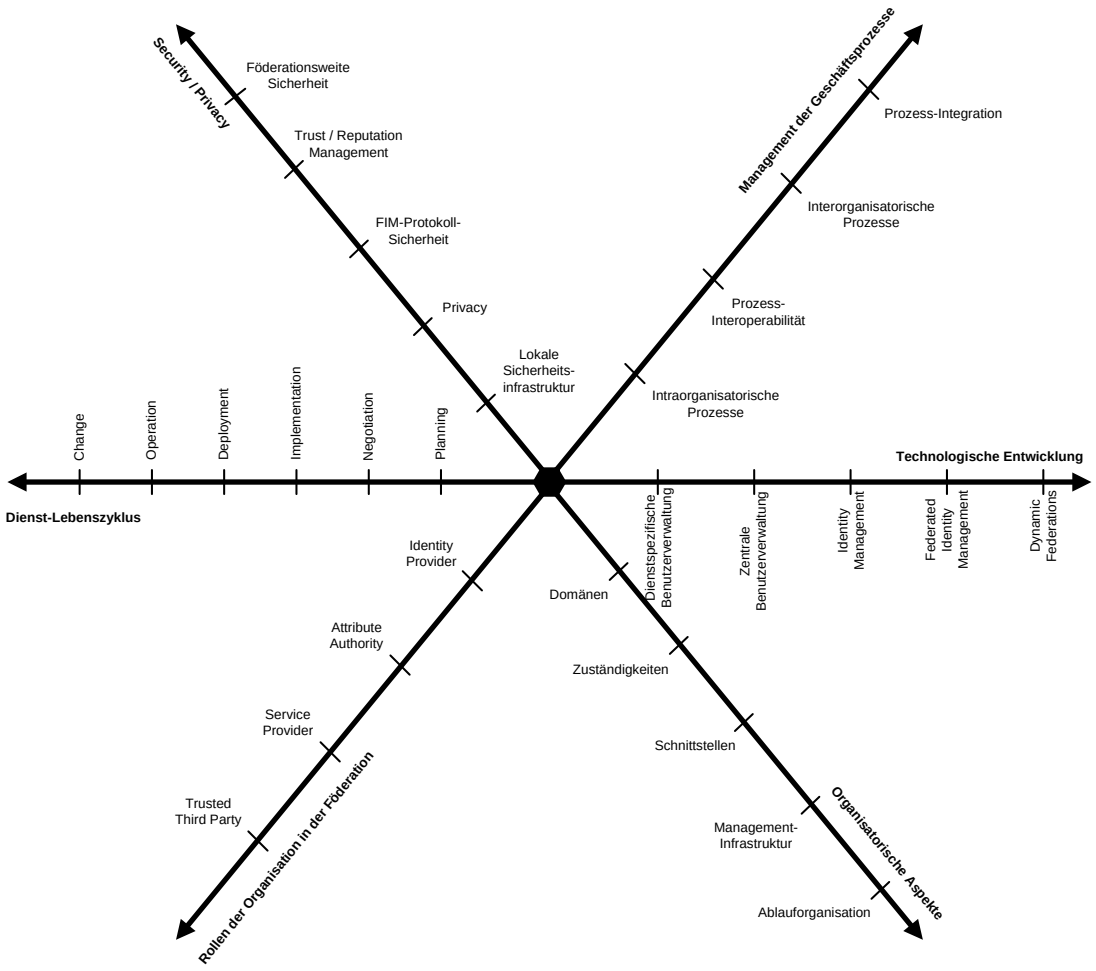


Abbildung 1.2.: Ausgewählte Dimensionen des Federated Identity Managements

Im nachfolgenden Abschnitt werden die in dieser Arbeit untersuchten Fragestellungen vorgestellt; in Abschnitt 1.3 wird das angewandte Vorgehensmodell erläutert. Die Schwerpunkte der eigenen Beiträge dieser Arbeit werden in Abschnitt 1.4 dargelegt; eine Abgrenzung gegenüber anderen Forschungsarbeiten wird abschließend in Abschnitt 1.5 vorgenommen.

1.2. Fragestellungen

Zur Definition des Forschungsumfelds und Verdeutlichung der Komplexität beim Aufbau und Betrieb von FIM-Lösungen zeigt Abbildung 1.2 einige Dimensionen des Federated Identity Managements:

- *Technologische Entwicklung*: Wie einleitend beschrieben hat sich die Verwaltung von Benutzern und deren Berechtigungen über die Zeit von einer pro Dienst individuellen Ausprägung über zentrale Benutzerverwaltungen hin zum Identity Management entwickelt und befindet sich nun im Übergang zum Federated Identity Management, auf das

diese Arbeit fokussiert ist. Föderationen sind dabei Mengen von Organisationen, die untereinander eine geeignete Vertrauensbeziehung aufgebaut und sich auf eine gemeinsame Syntax und Semantik der übertragenen Daten geeinigt haben. Unter den Begriffen *loosely coupled federations* bzw. *dynamic federations* wird langfristig der Identitätsdatenaustausch zwischen Organisationen angestrebt, die diese Voraussetzungen nicht a priori erfüllen, sondern erst zur Laufzeit aushandeln.

- *Organisatorische Aspekte*: Neben den technischen sind beim Management von IT-Infrastrukturen immer auch organisatorische und juristische Aspekte zu integrieren; die organisatorischen Aufgaben umfassen die Definition von Managementdomänen mit einer Festlegung der Zuständigkeiten und ihrer jeweiligen Schnittstellen, den Aufbau einer Managementinfrastruktur und die Definition von Managementprozessen und -abläufen [HAN99, S. 86f.]; diese Arbeit baut auf den durch FIM-Standards vorgegebenen interorganisatorischen Schnittstellen auf und entwickelt daraus Architektur- und Werkzeugkonzepte für das jeweilige intraorganisationale Identity Management. Dabei sollen insbesondere die Dezentralität der Datenhaltung und Administration beibehalten werden und die Autarkie der einzelnen Föderationsteilnehmer gewahrt bleiben.

- *Rollen der Organisation in der Föderation*: Jede Organisation kann in mehreren Föderationen jeweils mindestens eine Rolle ausüben. Grundlegend für das Funktionieren von FIM ist die Existenz mindestens eines Identity Providers und eines Service Providers. So genannte **Attribute Authorities** können die vom Identity Provider eines Benutzers gelieferten Daten entweder um weitere Informationen (im Sinne der Objektorientierung in Form von „Attributen“) *ergänzen* oder deren Korrektheit *bestätigen*; die letztere Eigenschaft ist insbesondere dann relevant, wenn ein Service Provider eine stärkere Vertrauensbeziehung zur Attribute Authority aufgebaut hat als zum Identity Provider oder mehr als eine Organisation benötigt wird, um einem Service Provider eine bestimmte Eigenschaft eines Benutzers glaubhaft zu versichern. Als **Trusted Third Party (TTP)** werden Organisationen bezeichnet, zu denen geeignete Vertrauensbeziehungen bestehen, auf die aber keine der anderen Rollen zutrifft; in diese Kategorie fallen unter anderem Broker und Registrierungsdienste, über die beispielsweise ein Service Provider den für einen Benutzer zuständigen Identity Provider ermitteln kann.

- *Dienst-Lebenszyklus*: FIM ist die Voraussetzung für die effiziente organisationsübergreifende Bereitstellung von Services und selbst ein verteilter Dienst, der von den an einer Föderation teilnehmenden Organisationen betrieben werden muss. In dieser Arbeit spielen die Abhängigkeiten von bereits vorhandenen I&AM-Systemen bei der Planung, Implementierung und dem Change Management von FIM-Lösungen eine zentrale Rolle.

- *Security und Privacy*: I&AM sowie FIM sind Basiskomponenten einer Sicherheitsinfrastruktur auf Applikationsebene und müssen inhärent selbst sicher sein. Bereits vorhandene Securitymechanismen auf Netzwerk- und Applikationsebene dürfen durch die Einführung von FIM-Komponenten nicht kompromittiert werden. Aufgrund der datenschutzrechtlichen Sensibilität der im Rahmen von Identity Management verarbeiteten Daten müssen Mechanismen zur Steuerung und Kontrolle von Datenfreigaben durch Benutzer umgesetzt werden, um eine Einhaltung gesetzlicher Rahmenbedingungen gewährleisten zu können, die insbesondere bei länderübergreifenden Kooperationen stark variieren können. Die Sicherheit FIM-spezifischer Neuerungen, beispielsweise der

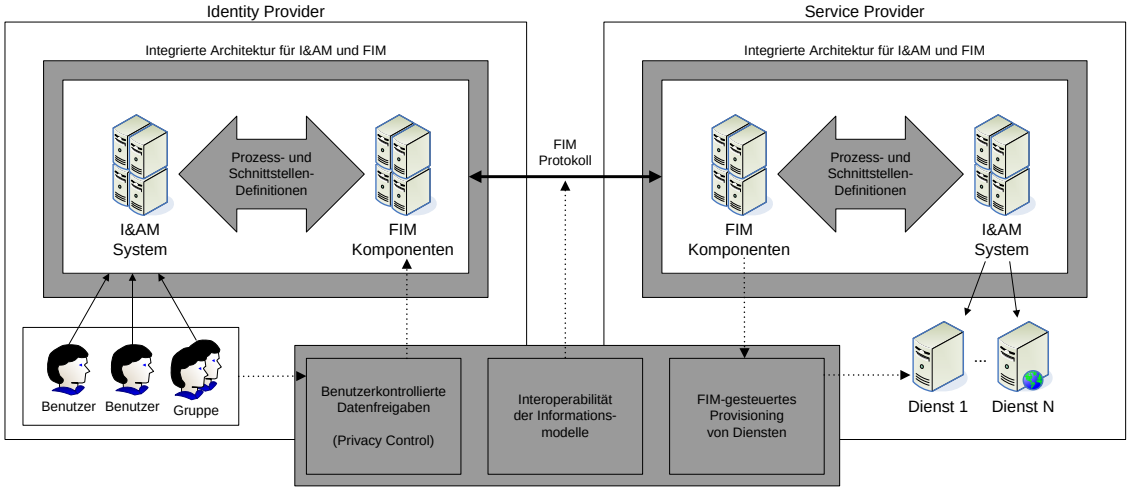


Abbildung 1.3.: Einordnung der untersuchten Fragestellungen

Datenübertragungsprotokolle, muss analysiert und sichergestellt werden. Der Aufbau von Vertrauensbeziehungen zwischen der Gesamtmenge der an einer Föderationen beteiligten Organisationen und Benutzer ist Bestandteil des Trust Managements, wobei dynamische und adaptive Varianten in die Domäne des Reputation Managements fallen. Aufgrund der Verteiltheit von FIM-Systemen müssen Sicherheitsmechanismen nicht nur lokal in jeder Organisation implementiert werden, sondern es muss auf neue Herausforderungen hinsichtlich der Sicherheit der gesamten Föderation eingegangen werden. Diese Arbeit konzentriert sich auf Securityaspekte bei der Kopplung von FIM-Komponenten mit I&AM-Systemen und die FIM-spezifische technische Umsetzung von **Privacy-Mechanismen**, die eine zwingende Voraussetzung für das Zustandekommen von FIM-Datenflüssen unter den Aspekten Conformance und Usability sind.

- *Management der Geschäftsprozesse*: FIM dient der informationstechnischen Unterstützung organisationsübergreifender Geschäftsprozesse und wird durch diese überhaupt erst notwendig. Die effiziente Kopplung intra- und interorganisatorischer technischer Workflows wird durch die Heterogenität der vorhandenen IT-Infrastrukturen erschwert. Im Rahmen dieser Arbeit werden Anforderungen an die durch I&AM-Lösungen umgesetzten intraorganisatorischen Prozesse definiert, die eine **flexible Integration FIM-spezifischer interorganisatorischer Prozesse** ermöglichen. Das langfristige Ziel ist eine aus der Integration von intra- und interorganisationalen Prozessen resultierende Abstraktionsebene, die eine transparente verteilte Umsetzung von auf Föderationsebene definierten Prozessen durch die einzelnen Föderationsteilnehmer und die nahtlose Integration in deren lokale Geschäftsprozesse ermöglicht.

Abbildung 1.3 zeigt den angestrebten Sollzustand im Kontrast zu Abbildung 1.1 und zielt auf die Einordnung der im Rahmen dieser Arbeit konkret bearbeiteten Fragestellungen, die in der Grafik grau hinterlegt sind, in das abstrakte FIM-Architekturkonzept ab. Auf Basis einer Analyse der Defizite aktueller FIM-Lösungsansätze werden die folgenden Aspekte untersucht:

- Welche organisationsinternen Geschäftsprozesse im Bereich des (De-)Provisionings von Services sind von der Einführung eines FIM-Systems betroffen und welche Anpassungen müssen realisiert werden?
- Welche Anforderungen ergeben sich daraus für die Planung und Implementierung von I&AM- und FIM-Systemen?
- Welche Schnittstellen müssen zwischen den Einzelkomponenten von I&AM- und FIM-Systemen existieren und wie können diese in bereits vorhandene Komponenten integriert werden? Wie ist insbesondere eine Koexistenz mit bereits vorhandenen IT-Sicherheitsinfrastrukturen realisierbar?
- Wie ist beim Aufbau integrierter I&AM- und FIM-Lösungen vorzugehen und welche Konsequenzen ergeben sich für das jeweilige Change Management? Wie kann die Implementierung einer gesamtheitlichen Lösung auf Basis von Komponentengruppen (Architekturmustern) erfolgen? Wie sehen Referenzarchitekturen für die verschiedenen organisationsspezifischen FIM-Rollen aus? Wie kann die parallele Einnahme mehrerer Rollen realisiert werden?
- Wie kann die organisationsübergreifende Interoperabilität vor dem Hintergrund heterogener Informationsmodelle im Bereich der Modellierung von identitätsrelevanten Daten gewährleistet werden?
- Wie kann den Benutzern die Möglichkeit gegeben werden, die Übermittlung ihrer personenbezogenen Daten durch Identity Provider und Attribute Authorities an andere Organisationen zu kontrollieren und zu steuern? Wie können diesbezügliche vertragliche Vorgaben integriert und Voreinstellungen durch Administratoren vorgenommen werden?
- Wie können auf Seite des Service Providers mehrere Dienste, insbesondere auch solche, die nicht auf Web Services basieren, mit Benutzerdaten gespeist und dabei Inkonsistenzen mit den Beständen der Identitätsdatenquellen verhindert werden?

Im nächsten Abschnitt wird die zur Analyse und Lösung dieser Problemstellungen gewählte Herangehensweise erläutert.

1.3. Vorgehensmodell

Die im Rahmen dieser Arbeit gewählte Vorgehensweise ist in Abbildung 1.4 visualisiert.

In *Kapitel 2* werden die technischen Grundlagen von I&AM und FIM dargestellt, um zuerst die in dieser Arbeit verwendete **Terminologie** einzuführen, die in Anhang A zusammengefasst ist; dieser Schritt ist notwendig, da sich aufgrund der Neuheit dieser beiden Managementdisziplinen noch keine einheitliche Begriffsbildung durchgesetzt hat. Anhand von **Szenarien** werden konkrete Einsatzmöglichkeiten von FIM vorgestellt, aus denen systematisch Anforderungen an FIM-Systeme und ihre Integration in I&AM-Systeme abgeleitet werden; diese werden zur Bewertung der existierenden und der im Rahmen dieser Arbeit entwickelten FIM-Komponenten in Form eines **Anforderungskatalogs** gruppiert und priorisiert.

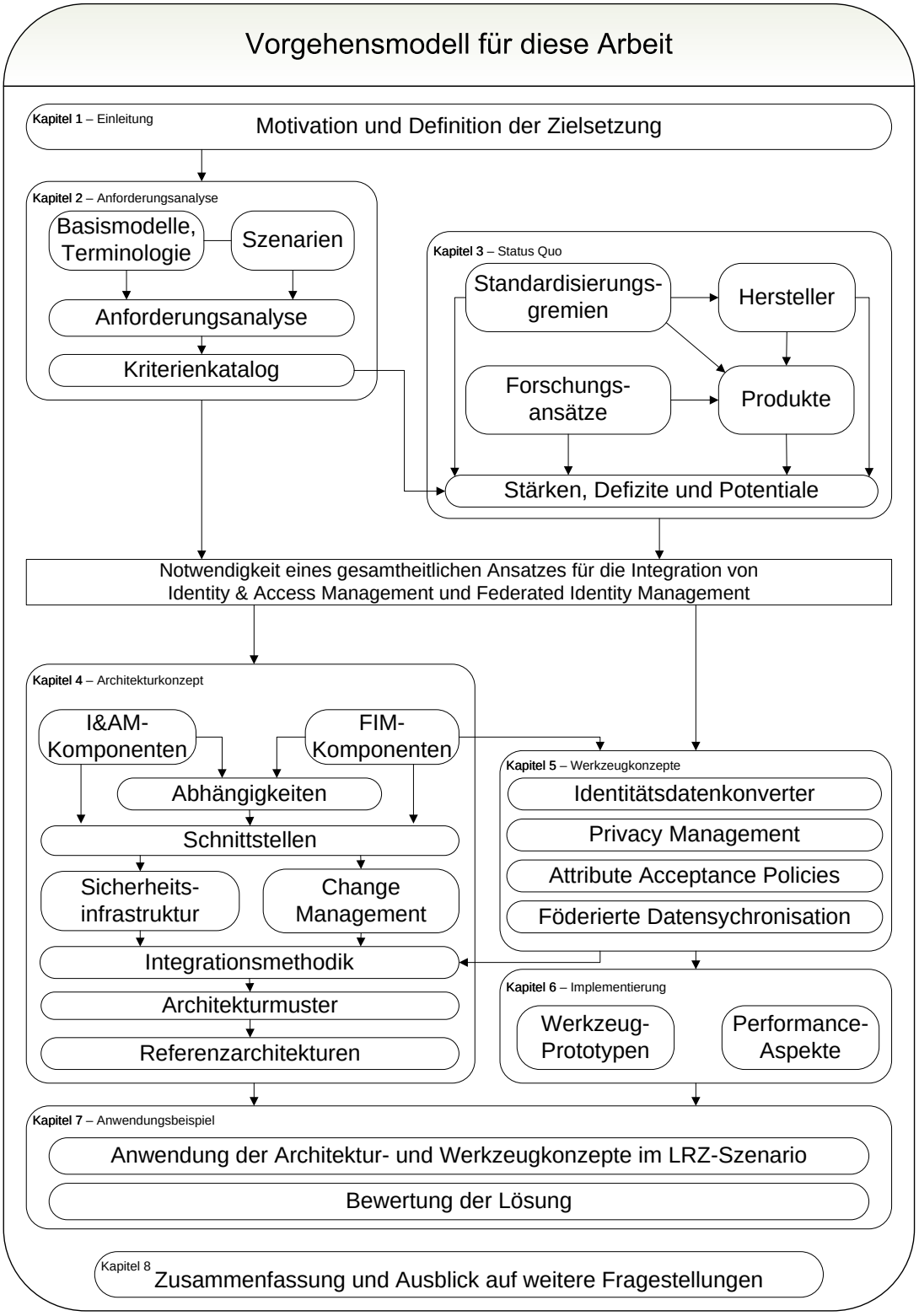


Abbildung 1.4.: Vorgehensmodell

Kapitel 3 geht auf die existierenden Ansätze für FIM und die im Rahmen dieser Arbeit relevanten FIM-Aspekte ein, wobei die von **Standardisierungsgremien** definierten Lösungen aufgrund ihrer praktischen Relevanz eine zentrale Rolle spielen. Ebenso werden aktuelle Ansätze und Implementierungen aus der **Forschung** betrachtet, die insbesondere im Bereich Privacy wesentlich fortgeschrittener sind als Industriestandards. Aufgrund des Bedarfs an FIM-Lösungen haben **Hersteller** auch bereits vor Standardisierungsbemühungen proprietäre Lösungen entwickelt, deren Besonderheiten exemplarisch untersucht werden. Von den meisten Standards, Forschungsansätzen und proprietären Lösungen existieren zumindest prototypische Implementierungen; eine zentrale Stellung nimmt die Software **Shibboleth** ein, die aus einer Kooperation zwischen Forschung und Standardisierungsgremien entstanden ist, als Open Source zur Verfügung steht und als Basis für die eigenen Erweiterungen verwendet wird. Die FIM-Ansätze und -Produkte werden auf Basis des in Kapitel 2 definierten Anforderungskatalogs hinsichtlich ihrer Stärken und Schwächen sowie ihres Weiterentwicklungspotentials bewertet.

Um die so gefundenen Mängel zu beheben, ist insbesondere eine Betrachtung der Schnittfläche notwendig, die sich ergibt, wenn die Integration von FIM-Komponenten in I&AM-Komponenten top-down und die Entwicklung von I&AM hin zum integrierten FIM bottom-up betrachtet wird. In *Kapitel 4* wird deshalb ein Architekturkonzept erarbeitet, das aus der Betrachtung einzelner I&AM- und FIM-Komponenten auf Basis ihrer gegenseitigen Abhängigkeiten fallspezifische Integrationsmethoden bereitstellt. Die Einbeziehung der lokal bereits vorhandenen IT-Sicherheitsinfrastruktur und die Auswirkungen auf die Change Management Prozesse werden diskutiert und gesamtheitlich auf Basis von Schnittstellendefinitionen spezifiziert. Das Zusammenspiel der Einzelkomponenten wird im Rahmen von Architekturmustern aufgezeigt, die sukzessive zu einer Gesamtarchitektur kombiniert werden, die auch die Rollen einer Organisation in den Föderationen berücksichtigt.

Parallel dazu ist die Einführung neuer FIM-Komponenten notwendig, um wesentliche Aspekte der angestrebten I&AM- und FIM-Integration zu flexibilisieren. Entsprechende Werkzeugkonzepte werden in *Kapitel 5* spezifiziert; sie umfassen die Interoperabilität heterogener Informationsmodelle auf Basis eines **Identitätsdatenkonverters**, die Steuerung und Kontrolle übertragener personenbezogener Daten auf Basis von so genannten **Attribute Release Policies**, das policygesteuerte **föderierte Provisioning** von IT-Services durch Attribute Acceptance Policies und die Vermeidung von Dateninkonsistenzen durch **föderierte Datensynchronisation**. Die **prototypische Implementierung** dieser Werkzeuge und ihrer Integration in Shibboleth wird in *Kapitel 6* beschrieben, wobei auch auf Performanceaspekte, die sich durch die Einführung der neuen Komponenten ergeben und die über die praktische Anwendbarkeit der gefundenen Lösung mit entscheiden, eingegangen wird.

Die erarbeiteten Architektur- und Werkzeugkonzepte werden in *Kapitel 7* exemplarisch auf ein realistisches Anwendungsbeispiel appliziert, das aus der Kombination mehrerer in Kapitel 2 vorgestellter Szenarien hervorgeht; die so entstandene Lösung wird wiederum kritisch bewertet, um auch die verbleibenden offenen Fragestellungen zu demonstrieren. Abschließend werden in *Kapitel 8* die Ergebnisse dieser Arbeit zusammengefasst und weitere verwandte Forschungsfragestellungen vorgestellt.

1.4. Fokus der in dieser Arbeit präsentierten eigenen Beiträge

Der Begriff *Federated Identity Management* wird sensu stricto ausschließlich für Lösungsansätze verwendet, die auf den Prinzipien der in Kapitel 3 erläuterten Standards SAML, Liberty Alliance und WS-Federation basieren und somit insbesondere zwischen Identity Providern und Service Providern differenzieren, zwischen denen Identitätsdaten dynamisch bei Bedarf ausgetauscht werden; andere Varianten des organisationsübergreifenden Identity Managements wie der Aufbau gemeinsamer Benutzerdatenbasen werden deshalb zwar an einigen Stellen zur Gegenüberstellung verwendet, aber nicht vertieft, da sie bislang weder konzeptionell über die mit FIM geschaffenen Möglichkeiten hinausgehen noch eine praktische Bedeutung erlangt haben.

In Kapitel 2 werden auf Basis ausgewählter Szenarien systematisch mehr als 60 Anforderungen an FIM-Konzepte und ihre Integration mit I&AM-Systemen definiert und begründet priorisiert. Die in diesem Umfang neue und gesamtheitliche Betrachtung arbeitet diverse Aspekte und Randbedingungen heraus, die von den bisherigen FIM-Ansätzen nicht bzw. nur inadäquat berücksichtigt wurden und untermauert die Argumentation für die Notwendigkeit neuer und erweiterter FIM-Architekturkomponenten. Der Überblick über den aktuellen Stand der Technik in Kapitel 3 erstreckt sich deshalb auch auf relevante verwandte Gebiete wie das Privacy Management, um die Eignung bzw. Übertragbarkeit der dort eingesetzten Methoden, Prozesse und Werkzeuge auf FIM-Szenarien zu beurteilen.

Das in Kapitel 4 vorgestellte umfassende Architekturkonzept konzentriert sich auf die in bisherigen Ansätzen vernachlässigte nahtlose Integration von I&AM- und FIM-Komponenten zu einem redundanzfreien Gesamtsystem. Auf der Basis detaillierter Schnittstellenspezifikationen und Abhängigkeitsanalysen wird eine Methodik für die praktisch essentielle Integration von FIM-Komponenten in vorhandene I&AM-Systeme erarbeitet, deren Unausgereiftheit ein grundlegendes Defizit bisheriger Ansätze darstellt. Ein weiterer Schwerpunkt liegt auf der von bisherigen Ansätzen ebenfalls nur unzureichend berücksichtigten Integration in vorhandene IT-Sicherheitsinfrastrukturen; die in der Praxis unbedingt erforderliche, bislang aber kaum untersuchte Integration in das IT Service Management wird am Beispiel ausgewählter Teilprozesse des Change Managements demonstriert.

Vier neu konzipierte Werkzeuge, die eine präzise, policygesteuerte Kontrolle des organisationsübergreifenden Flusses personenbezogener Daten und deren dynamische Konvertierung auf Basis der jeweils organisationsintern eingesetzten Datenmodelle ermöglichen, werden in Kapitel 5 detailliert spezifiziert; als Tragfähigkeitsnachweis dienen prototypische Implementierungen, die zusammen mit dem Architekturkonzept und der erarbeiteten Integrationsmethodik erfolgreich auf ein komplexes und realistisches Anwendungsszenario angewandt werden.

1.5. Abgrenzung zu verwandten Forschungsarbeiten

Die Voraussetzungen für und die Anwendung von Federated Identity Management und seiner vielfältiger Facetten sind Themen diverser Arbeiten sowohl innerhalb des Munich Network Management Teams (MNM-Team) als auch an anderen akademischen und industriellen Forschungseinrichtungen. Im Folgenden wird kurz auf die Gemeinsamkeiten, Unterschiede und Schnittstellen zu denjenigen anderen Arbeiten eingegangen, die in einem deutlich engeren Zusammenhang mit dieser Arbeit stehen als die übrige Literatur:

- **Latifa Boursas** untersucht in ihrer Dissertation Trust und Reputation Management (TM/RM) in föderierten Umgebungen. Ein gemeinsames Anwendungsbeispiel, das somit aus beiden Perspektiven beleuchtet wird, ist die Verknüpfung von FIM und TM/RM im Rahmen benutzerdefinierter Datenfreigabepolicies. Die vorliegende Arbeit setzt eine geeignete Vertrauensbeziehung zwischen den beteiligten Entitäten (Personen, Maschinen, Organisationen) an vielen Stellen als gegeben voraus und baut diesbezüglich logisch auf den Ergebnissen von Boursas auf.

- **Helmut Reiser** spezifiziert in seiner Habilitation ein Framework für föderiertes Sicherheitsmanagement. Neben kryptographischen Verfahren und der Sicherheit von Netzen auf Basis von Intrusion Detection und Intrusion Prevention wird FIM eingesetzt, um ein effizientes verteiltes Management von Benutzern und Berechtigungen auf Applikationsebene zu erreichen. Reiser greift hierzu im Rahmen dieser Arbeit entstandene Lösungen auf und bettet sie in ein umfassenderes Rahmenwerk ein.

- **Michael Schiffers** analysiert in seiner Dissertation das Management dynamischer virtueller Organisationen (DVOs) im Rahmen des Grid Computings. In Bezug auf Identity Management sind VOs mit Föderationen zu vergleichen, die auch die im Rahmen einer VO zentral definierten Prozesse in der im Allgemeinen heterogenen IT-Infrastruktur der an der VO beteiligten Organisationen umgesetzt werden müssen. Die Anwendung von FIM im Grid-Umfeld wird in dieser Arbeit zur Deduktion von Anforderungen betrachtet; relevant ist diesbezüglich ferner das amerikanische Forschungsprojekt *GridShib*, bei dem die Software Shibboleth an die Anforderungen des Grid-Umfelds angepasst werden soll.

- **Birgit Pfitzmann** und **Michael Waidner** arbeiten im IBM Forschungslabor in Zürich an der Sicherheit von FIM-Protokollen, definieren ein idealisiertes Protokoll für Identitätsdatentransfer zwischen Webseiten (browser based attribute exchange, BBAE) und geben Anforderungen im Bereich Privacy und der service-provider-seitigen Veröffentlichung von Privacy Policies vor. Die vorliegende Arbeit baut zum Teil auf diesen Anforderungen auf und setzt policygesteuerte Mechanismen auf Seiten des Benutzers und seines Identity Providers um; sie ist somit komplementär zu den Konzepten von B. Pfitzmann und Waidner.

- **Marco Casassa-Mont** und **Pete Bramhall** arbeiten im Rahmen ihrer Tätigkeiten in den HP Laboratories Bristol nicht nur an der Spezifikation, sondern auch an der sichergestellten Umsetzung (Enforcement) von Privacy Policies auf der Seite des Service Providers. Dabei gehen sie insbesondere auf die strengen gesetzlichen Auflagen im Gesundheitswesen ein. Diverse Neuerung wie die Einführung so genannter Sticky Policies, bei denen die Policies fest mit den sie betreffenden Daten verbunden sind, werden in der vorliegenden Arbeit wiederum komplementär auf der Seite des Identity Providers betrachtet.

Kapitel 2.

Szenarien und Anforderungsanalyse

Inhalt dieses Kapitels

Um die bereits existierenden Lösungsansätze für Federated Identity Management miteinander vergleichen und ihre Stärken und Schwächen erläutern zu können, wird in diesem Kapitel ein Kriterienkatalog definiert, dessen Komponenten aus der Abstraktion von konkreten Szenarien abgeleitet werden.

Sowohl Identity & Access Management als auch Federated Identity Management sind noch relativ junge Disziplinen, so dass bislang viele Begriffe noch nicht einheitlich definiert und auf breiter Basis anerkannt sind. In Abschnitt 2.1 werden deshalb zur Begriffsbildung die grundlegenden technischen und organisatorischen Aspekte von I&AM und FIM vorgestellt; eine Betrachtung des so genannten User Centric Identity Managements (UCIM), das insbesondere den Datenschutz betont, rundet den Überblick ab. Die in diesem Abschnitt eingeführten Workflows, Kommunikationsprotokolle und Organisationskonzepte spielen eine zentrale Rolle in Kapitel 4.

Die Themengebiete I&AM und UCIM werden anhand jeweils eines Szenarios veranschaulicht (Abschnitte 2.1.1.8 und 2.1.3.6). In Abschnitt 2.2 werden drei Szenarien illustriert, die sich mit verschiedenen Aspekten von FIM befassen. Bei ihrer Auswahl und Darstellung wurde insbesondere auf ein breites Spektrum an erkennbaren Anforderungen und Realitätsnähe geachtet.

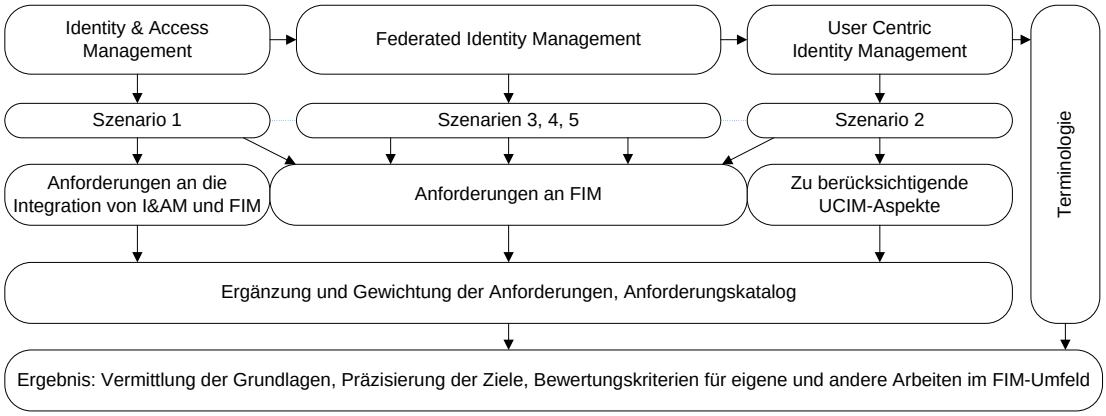


Abbildung 2.1.: Vorgehensmodell in diesem Kapitel

Im Anschluss an die Beschreibung jedes Szenarios folgt die Ableitung von Anforderungen an die jeweils eingesetzte Technologie, insbesondere vor dem Hintergrund ihrer Integration in bereits vorhandene IT-Infrastrukturen. Dabei werden die erörterten Beispiele bewusst abstrahiert, um die ermittelten Anforderungen generisch zu formulieren.

So wie sich die einzelnen Szenarien zu einem Gesamtbild zusammenfügen lassen und dabei neue Fragestellungen aufwerfen würden, werden die ermittelten Anforderungen in Abschnitt 2.3 zusammengefasst und um einige weitere Aspekte ergänzt, die zum Teil aus anderen aktuellen Forschungsarbeiten abgeleitet werden können, auf die in Kapitel 3 detaillierter eingegangen wird.

Die Anforderungen werden schließlich gewichtet und in Form eines tabellarischen Anforderungskatalogs in Abschnitt 2.4 dargestellt, auf den in den weiteren Kapiteln Bezug genommen wird. Abbildung 2.1 stellt das diesem Kapitel zugrundeliegende Vorgehensmodell graphisch dar.

Durch die Kombination von I&AM, FIM und UCIM können komplexe verteilte Systeme realisiert werden, deren aufwendige organisatorische Einbettung und technische Integration in bestehende IT-Infrastrukturen bislang noch nicht umfassend untersucht worden sind. Die in diesem Kapitel dargestellte systematische Anforderungsanalyse zielt deshalb auf eine tiefgehende, gesamtheitliche Betrachtung ab und bildet den ersten Schwerpunkt dieser Arbeit.

2.1. Basismodelle

In den nachfolgenden Abschnitten 2.1.1 bis 2.1.3 werden die technischen und organisatorischen Aspekte der drei Facetten von Identity Management, die sich im Laufe der Zeit herauskristallisiert haben, einführend erläutert:

- Identity & Access Management (I&AM – Abschnitt 2.1.1) ging aus der konsequenten Weiterentwicklung des herkömmlichen, organisationsinternen User Managements hervor, wobei die IT-Unterstützung der zugrundeliegenden Geschäftsprozesse und die

technischen Möglichkeiten zur rezentralisierten Nutzung gemeinsamer Datenbestände ausschlaggebend sind.

- Federated Identity Management (FIM – Abschnitt 2.1.2) fokussiert den organisationsübergreifenden Austausch von personenbezogenen Daten und Benutzerprofilen.
- User Centric Identity Management (UCIM – Abschnitt 2.1.3) betrachtet die Übermittlung personenbezogener Daten aus Benutzerperspektive und konzentriert sich auf datenschutzspezifische Aspekte.

Für I&AM existieren bereits ausgereifte Konzepte und technische Lösungen, auf die im Rahmen dieser Arbeit zurückgegriffen wird; wie in Kapitel 3 vertiefend dargestellt wird, sind FIM und UCIM hingegen noch im Entstehen, so dass existierende Konzepte noch keine endgültige Form angenommen und verfügbare Implementierungen und Deployments eher prototypischen Charakter haben.

2.1.1. Identity & Access Management

Sicherheitsmanagement gehört zu den klassischen IT-Managementfunktionen und beinhaltet unter anderem die *Identifikation*, *Authentifizierung* und *Autorisierung* von Benutzern [HAN99]. Die historische Entwicklung zeigt, dass Softwaresysteme zur Erbringung eines Dienstes in der Regel mit einer eigenen, integrierten Benutzerverwaltung ausgestattet sind; die Möglichkeiten zum autarken Betrieb haben dabei häufig Vorrang vor der gemeinsamen Nutzung von Benutzerdatenbeständen.

Die Pflege von Benutzer- und Autorisierungsdaten wurde üblicherweise von den für den jeweiligen Dienst zuständigen Administratoren mit einem von der jeweiligen Software vorgegebenen Managementfrontend durchgeführt. Dieser Prozess wurde insbesondere auch beibehalten, als sich für viele andere Aspekte des Netz- und Systemmanagements bereits integrierte, zentrale Lösungsansätze etabliert hatten.

Durch die redundante Pflege derselben Daten an verschiedenen Stellen, die in diesem Zusammenhang auch als *Silos* bezeichnet werden, ergeben sich in der Praxis sehr schnell Inkonsistenzen. Werden beispielsweise die Kontaktinformationen eines Benutzers nur bei einigen, aber nicht bei allen Diensten aktualisiert, so erschwert sich die Kommunikation mit dem Betroffenen, beispielsweise im Fall eines Problems, das ein beidseitiges Eingreifen erfordert. Schwerwiegender sind Fälle, in denen Benutzern Berechtigungen nicht rechtzeitig, beispielsweise beim Ausscheiden eines Mitarbeiters, entzogen werden, so dass nachfolgende, aus organisatorischer Sicht unberechtigte Zugriffe technisch nicht verhindert werden.

Abbildung 2.2 illustriert die Bildung von Silos am Beispiel von Diensten für Studenten an einer Universität; das Beispiel wird in Szenario 1 (Abschnitt 2.1.1.8) vertieft.

2.1.1.1. Zentralisierter Datenbestand

Ein explizites Ziel von I&AM ist deshalb die Schaffung eines zentralen Datenbestandes, der für die an das I&AM-System angeschlossenen Dienste autoritativ ist, alle dienstübergreifend relevanten Benutzerdaten enthält und über den die Berechtigungen zur Benutzung der Dienste

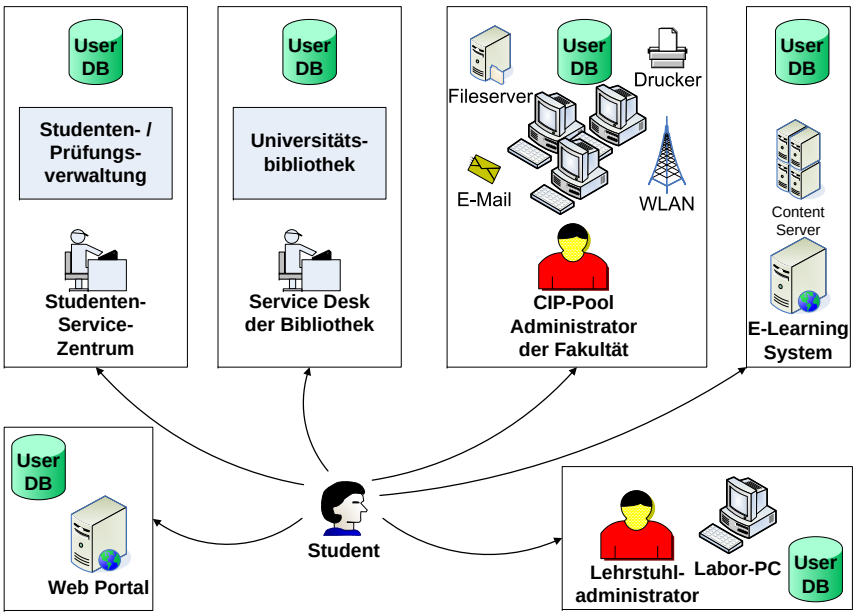


Abbildung 2.2.: Bildung von „Silos“ durch autarke Benutzerverwaltung pro Dienst

gesteuert werden können. Die Nutzung dieses Datenbestandes erstreckt sich neben von den Benutzern in Anspruch genommenen Diensten auch auf interne Systeme, die beispielsweise für das Rechnungswesen benötigt werden.

Der zentrale Datenbestand, der im Allgemeinen als **Identity Repository** bezeichnet wird, kann mit relationalen Datenbankmanagementsystemen oder Verzeichnisdiensten realisiert werden. In der Praxis haben sich zwischenzeitlich LDAP-basierte *Enterprise Directory Services* für diese Aufgabe durchgesetzt. Ausschlaggebend hierfür ist insbesondere, dass LDAP im Gegensatz zu der im Datenbankumfeld eingesetzten Sprache SQL nicht nur die Anfragesprache selbst, sondern auch das verwendete TCP/IP-basierte Request-Response-Protokoll für die Kommunikation zwischen Client und Server definiert; hierdurch wird eine durchgängige Interoperabilität zwischen LDAP-fähigen Komponenten erreicht, während bei relationalen Datenbankmanagementsystemen herstellerspezifische Programmierschnittstellen erforderlich sind, durch die die Kommunikation zwischen Systemen unterschiedlicher Hersteller deutlich aufwendiger zu realisieren ist.

Das Identity Repository umfasst zwar den gesamten Benutzerdatenbestand, es wird allerdings in der Regel nicht dazu verwendet, mittels Managementfrontend einzelne Einträge direkt darin anzulegen. Vielmehr werden *autoritative Datenquellen* definiert, die das Identity Repository speisen und in diesem Kontext auch als *führende Systeme* bezeichnet werden; Beispiele umfassen das in einer Organisation eingesetzte Personalverwaltungssystem und das Customer Relationship Management. Für die Zuweisung von Berechtigungen an erfasste Benutzer können optionale Administrationsoberflächen eingesetzt werden; im Allgemeinen wird jedoch angestrebt, die Berechtigungen explizit bereits in den autoritativen Datenquellen zu vergeben oder diese implizit daraus abzuleiten, aus welcher Datenquelle der Datensatz übermittelt wurde. Abbildung 2.3 verdeutlicht die logische Positionierung des Identity Repositories.

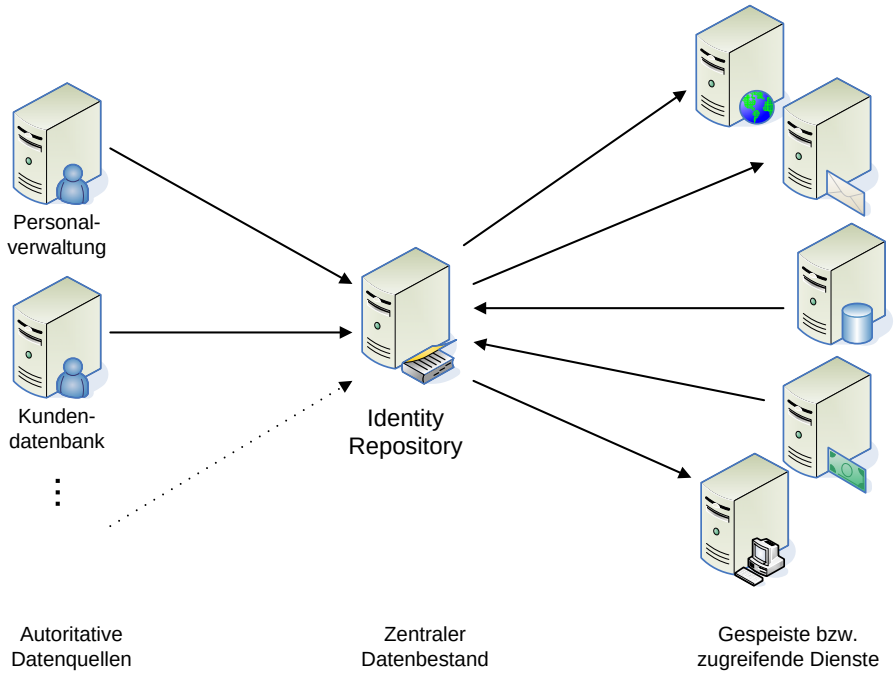


Abbildung 2.3.: Identity Repository als zentrale Datenbasis in I&AM-Systemen

2.1.1.2. Prozessübergreifende Identitätskorrelation

Die Datensätze werden im Identity Repository *aggregiert* und *korreliert*; die Korrelation ist immer dann erforderlich, wenn ein und dieselbe Person prinzipiell in verschiedenen führenden Systemen gepflegt werden könnte, z. B. weil sie sowohl Mitarbeiter als auch Kunde sein kann. In solchen Fällen ist es explizites Ziel von I&AM Systemen, dass diese Person im Identity Repository nur einmal und nicht mehrfach erfasst wird, aber durchaus alle ihren Rollen entsprechenden Berechtigungen erhält. Eine solche prozessübergreifende Identitätskorrelation kann insbesondere dadurch erschwert werden, dass die verschiedenen führenden Systeme keinen gemeinsamen Datensatzschlüssel wie beispielsweise eine Personalnummer verwenden. In solchen Fällen werden in der Praxis häufig Heuristiken, beispielsweise ein Abgleich auf Basis von Vor- und Nachname sowie Geburtsdatum, durchgeführt, die wiederum durch verminderte Datenqualität, beispielsweise durch Tippfehler bei der Erfassung der Person, erschwert werden können und eine Restfehlerrate aufweisen, die manuelle Eingriffe erfordert.

2.1.1.3. Konnektoren

Der Datenabgleich zwischen den führenden Systemen und dem Identity Repository wird mittels so genannter **Konnektoren** realisiert. Sie haben die Aufgabe, Daten aus dem Quellsystem auszulesen und in geeigneter Form im Zielsystem abzulegen; häufig sind hierbei Konvertierungen der eingesetzten Datenformate notwendig – beispielsweise muss ein Personeneintrag, der im Personalverwaltungssystem in einer relationalen Datenbank in normalisierter Form

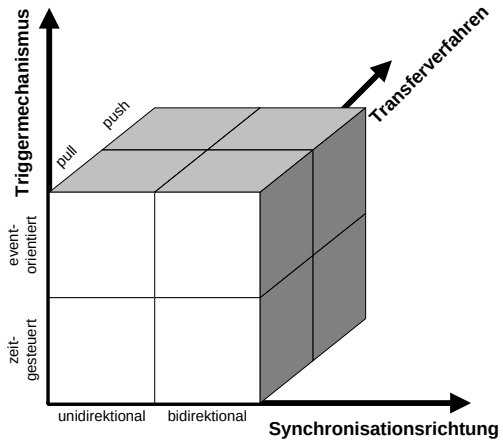


Abbildung 2.4.: Realisierungsvarianten von Konnektoren in I&AM-Systemen

auf mehrere Tabellen verteilt ist, in ein Verzeichnisdienstobjekt nach einem vorgegebenen LDAP-Datenschema umgewandelt werden. Die hierzu notwendigen Einzelschritte sind auch für FIM relevant und werden in Kapitel 4 näher erläutert.

Ein Konnektor kann, wie in Abbildung 2.4 dargestellt, *uni-* oder *bidirektional* realisiert werden; wenn Mitarbeiter beispielsweise nach geeigneter Authentifizierung in einem webbasierten Managementfrontend im Intranet ihre Anschrift ändern können sollen, muss sichergestellt werden, dass am Identity Repository durchgeführte Modifikationen auch zurück an die führenden Systeme propagiert werden.

Ferner ist die Häufigkeit, mit der die Datenbestände zweier Systeme über einen Konnektor abgeglichen werden, festzulegen. Hierbei wird zwischen *Intervallsteuerung* und *Eventorientierung* unterschieden. Bei intervallgesteuerten Konnektoren wird der Datenbestand zum Beispiel einmal pro Tag abgeglichen; bei Eventorientierung stößt jede Veränderung im Quellsystem einen Datenaustausch mit dem Zielsystem an, wodurch eine zeitnahe Propagation auf Kosten entsprechenden Overheads, z. B. erhöhten Netzwerkdatenverkehrs, realisiert werden kann.

Schließlich ist noch zu unterscheiden, ob die Daten aus dem Quellsystem abgerufen werden müssen (*Pull*-Verfahren) oder von diesem ins Zielsystem eingespeist werden (*Push*-Verfahren). Das Pull-Verfahren hat den systembedingten Nachteil, dass im Quellsystem erst nach synchronisationsrelevanten Datenbeständen gesucht werden muss, beispielsweise nach allen Einträgen, die seit der letzten Synchronisation modifiziert worden sind. Der Push-Ansatz setzt hingegen geeignete Unterstützung durch das Quellsystem voraus, die bei vielen heute üblichen Systemen allerdings noch nicht zur Verfügung steht oder erst durch die Installation zusätzlicher Softwarekomponenten nachgerüstet werden muss.

2.1.1.4. Anbindung von Diensten an ein I&AM-System

Bezüglich der Nutzung der im Identity Repository erfassten Daten durch die Dienstinstanzen, deren Benutzerverwaltung durch das I&AM-System möglichst weitgehend automatisiert

werden soll, existieren die folgenden Möglichkeiten:

1. Der Dienst ist beispielsweise LDAP-fähig und benötigt außer den im Identity Repository hinterlegten Daten keine weiteren benutzerspezifischen Informationen. In diesem Fall kann auf eine redundante lokale Benutzerverwaltung gänzlich verzichtet werden, sofern Quality-of-Service-(QoS-)Parameter wie die Performanz und Verfügbarkeit des Identity Repository ausreichend für den Dienstbetrieb sind.

2. Der Dienst kann auf die im Identity Repository hinterlegten Daten zugreifen, benötigt für das lokale Benutzerprofil aber noch weitere Informationen. Je nach eingesetzter Software auf Dienstseite kann es ausreichend sein, lediglich diese Zusatzinformationen lokal vorzuhalten, oder notwendig werden, den entsprechenden Datenbestand aus dem Identity Repository in die dienstlokale Benutzerverwaltung zu importieren und über diesen Mechanismus kontinuierlich aktuell zu halten.

3. Der Dienst ist auf seine lokale Benutzerverwaltung angewiesen und bietet keine Möglichkeit zum Import aus dem Identity Repository. In solchen Fällen ist wiederum auf Konnektoren zurückzugreifen, mit denen die Daten aus dem Identity Repository in das betroffene Zielsystem im dort benötigten Format eingespeist werden können – dieser Vorgang wird als **User Provisioning** bezeichnet.

Diese Varianten der Dienstanbindung werden in Abbildung 2.5 veranschaulicht.

Die Beibehaltung lokaler Benutzerverwaltungen kann auch dadurch erforderlich werden, dass die benötigten Daten zwar im Identity Repository vorliegen, aber nicht das vom Dienst benötigte Format aufweisen. Der Einsatz eines Provisioningverfahrens ist in der Regel kosteneffizienter umzusetzen als folgende Alternativen:

- Das Datenmodell des Identity Repository könnte an das vom Dienst benötigte angepasst werden. Während *Erweiterungen* des Datenmodells meist ohne großen Aufwand realisiert werden können, haben *Änderungen* in der Regel sehr weitreichende Konsequenzen, da beispielsweise *alle* bereits implementierten Konnektoren an das neue Datenmodell angepasst werden müssten. Insbesondere ist aufgrund der mangelnden Standardisierung von Datenmodellen (vgl. Abschnitt 3.8) jedoch davon auszugehen, dass konfliktäre Anforderungen von verschiedenen angeschlossenen Systemen vorliegen, die bereits syntaktisch nicht auf einen gemeinsamen Nenner gebracht werden können. Abschnitt 4.8 vertieft die Aspekte des Change Managements, deren Komplexität sich bei der Kombination mit organisationsübergreifendem Datenaustausch noch erhöht.

- Für den betroffenen Dienst kann beispielsweise ein dedizierter Verzeichnisdienst realisiert werden, der mit dem Identity Repository abgeglichen wird und in dem das benötigte Datenformat eingesetzt wird. Hierfür eignen sich insbesondere die in Abschnitt 2.1.1.5 erläuterten *virtuellen* Verzeichnisdienste. Sowohl der Implementierungsaufwand als auch die Kosten für den Betrieb eines zusätzlichen Repository (u. a. Lizenzen, Hardware, Wartung) sind jedoch häufig höher als bei einem Provisioningkonnektor, so dass diese Variante in der Praxis typischerweise nur eingesetzt wird, wenn damit verbundene Seiteneffekte wie Lastverteilung oder eine bessere Integration in die Securityinfrastruktur ausgenutzt werden sollen.

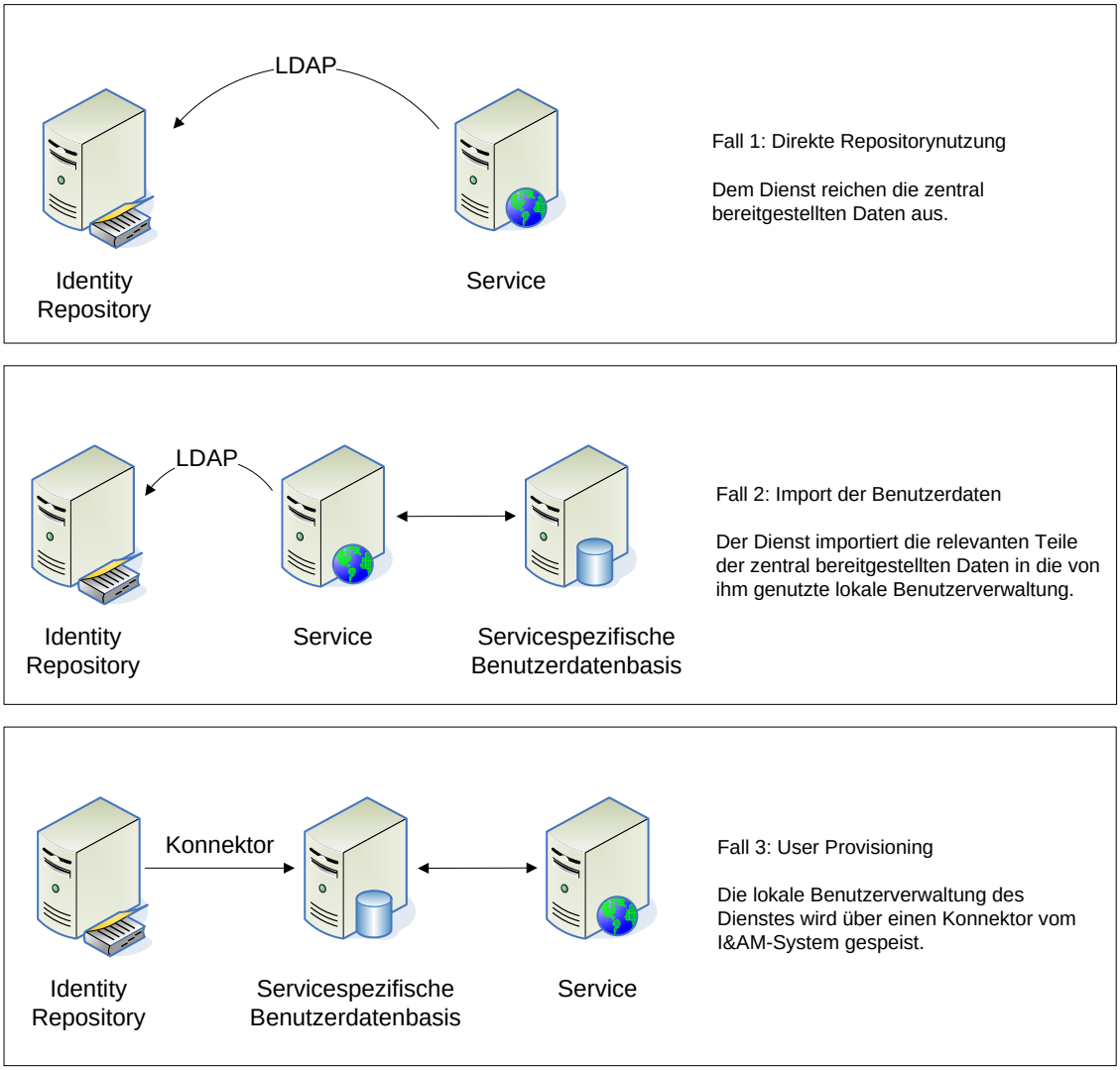


Abbildung 2.5.: Varianten zur Anbindung von Diensten an das Identity Repository

Sofern die angebundenen Dienste Veränderungen an den Datenbeständen des Identity Repository durchführen können sollen, sind den entsprechenden Systemen Schreibberechtigungen zuzuweisen beziehungsweise die Konnektoren bidirektional zu realisieren. Hierbei ist insbesondere darauf zu achten, dass nur die jeweils relevanten Teilmengen der entsprechenden Datensätze modifiziert werden können. Ebenso ist durch geeignete Backup-, Protokollierungs- und Auditingmechanismen sicherzustellen, dass unerwünschte Modifikationen, die beispielsweise von kompromittierten Diensten oder böswilligen Administratoren durchgeführt worden sind, erkannt und rückgängig gemacht werden können.

2.1.1.5. Meta-Directories, Provisioningsysteme und Virtuelle Verzeichnisdienste

Zur Implementierung der oben erläuterten Basisbestandteile von I&AM-Systemen stehen Softwarekomponenten zur Verfügung, die sich in die folgenden Kategorien einteilen lassen:

- Als **Meta-Directory** wird eine Kombination aus Identity Repository und Konnektoren bezeichnet. Eine Vielzahl von Herstellern bietet inzwischen LDAP-basierte Verzeichnisdienste zusammen mit eigenen Programmiersprachen oder Funktionsbibliotheken für weit verbreitete Programmier- und Skriptsprachen an, mit denen die Befüllung des Identity Repository und das User Provisioning für die Zielsysteme realisiert werden kann.

- So genannte **Provisioningsysteme** haben kein eigenes Identity Repository. Sie leiten Änderungen in den Quellsystemen über Konnektoren an die angeschlossenen Zielsysteme weiter, können aufgrund des fehlenden eigenen Datenbestands jedoch nicht für das in Abschnitt 2.1.1.3 beschriebene Pull-Verfahren eingesetzt werden; sie werden deshalb primär in Szenarien ohne LDAP-fähige Zielsysteme oder in Kombination mit anderen Komponenten eingesetzt.

- **Virtuelle Verzeichnisdienste** sind komplementär zu Provisioningsystemen: Sie haben Konnektoren zu den Quellsystemen, aber weder Konnektoren zu den Zielsystemen noch ein eigenes Identity Repository. Eingehende Anfragen können beantwortet werden, indem sie zur Laufzeit an die relevanten Quellsysteme weitergeleitet werden. Damit ist es beispielsweise möglich, eine Gesamtsicht sowohl auf Mitarbeiter- als auch auf Kundendaten, die in verschiedenen Datenbasen hinterlegt sind, zur Verfügung zu stellen, ohne dass die Daten redundant in einem Identity Repository gehalten werden müssen. Damit verbunden sind zwangsläufige Performanznachteile, da die benötigten Daten erst aus einem anderen System bezogen werden müssen; beim Ausfall eines Quellsystems kann es zu unvollständigen Antworten kommen, die nicht unmittelbar als Fehler erkennbar sind.

Abbildung 2.6 stellt diese Varianten graphisch dar. Die Auswahl der zu verwendenden Komponenten hängt vom zu realisierenden Szenario ab und wird in Abschnitt 4.9 vertieft.

2.1.1.6. Datenschutz in I&AM-Systemen

Die Erfassung und Verarbeitung personenbezogener Daten unterliegt gesetzlichen Auflagen und kann ausschlaggebend für die Akzeptanz von Diensten durch Benutzer sein. Diese Arbeit orientiert sich an den Grundsätzen der EU-Datenschutzrichtlinie [EU-DSR], die sich in den Bundes- und Landesdatenschutzgesetzen sowie servicespezifischen Regelungen wie dem Teledienste-Datenschutzgesetz widerspiegelt, ohne juristische Aspekte zu vertiefen. Auf Besonderheiten bei der Weitergabe von Daten an Dritte im FIM-Kontext wird in Abschnitt 2.1.2.6 eingegangen.

Aufgrund dieser Auflagen ergeben sich die folgenden datenschutzrelevanten Bedingungen, die auch durch geeignete technische Maßnahmen zu gewährleisten sind:

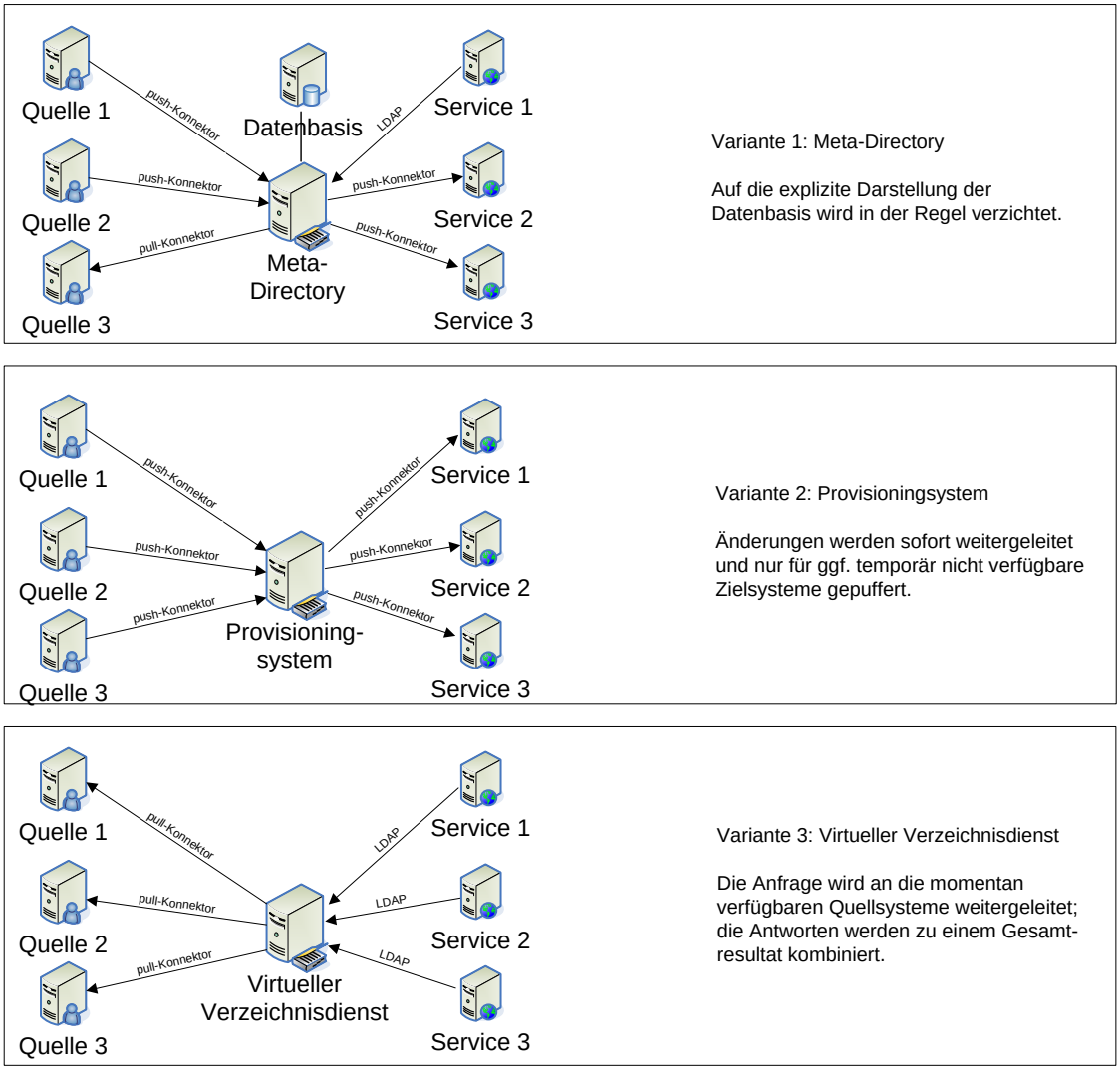


Abbildung 2.6.: Realisierungsvarianten: Meta-Directory, Provisioningsystem und virtueller Verzeichnisdienst

- Die Erfassung der Daten muss rechtmäßig erfolgen. Dies setzt voraus, dass entweder gesetzliche Grundlagen für die Datenakquisition vorliegen (z. B. im Behördenbereich) oder der Betroffene sein *Einverständnis* in geeigneter Form zum Ausdruck bringt. Letzteres ist beispielsweise zu beachten, wenn sich Benutzer über Webformulare selbst für einen Dienst registrieren können.

- Es gilt das Prinzip der *Datensparsamkeit*, nach dem nur solche Daten erfasst werden sollen, die für die Diensterbringung relevant sind. Ein zentrales Identity Repository, über das alle Dienste mit den benötigten Daten versorgt werden sollen, umfasst damit die entsprechende Vereinigungsmenge, die im Rahmen einer Anforderungsanalyse beim Aufbau des Identity Management Systems berücksichtigt werden muss.

Aus Datenschutzsicht ist die in einem Identity Repository durchgeführte Aggregation und Korrelation von Daten über ein und dieselbe Person aus mehreren Systemen eine nicht zu unterschätzende Gefahrenquelle, da ein Gesamtdatensatz unter Umständen mehr Informationen preisgibt als die reine „Summe seiner Einzelteile“. Der technischen Umsetzung der unten erläuterten zweckmäßigen Datenverarbeitung in Form eines *Privacy Policy Enforcements* kommt deshalb eine besondere Bedeutung zu.

- Die Betroffenen haben das Recht, über sie gespeicherte Daten einzusehen und über deren Verarbeitung durch die eingesetzten Systeme informiert zu werden. Das Einholen einer derartigen *Selbstauskunft* wird bei vielen Dienstleistern noch als seltene Ausnahme angesehen und manuell bearbeitet. Unter der Voraussetzung einer geeigneten Authentifizierungsmöglichkeit wird jedoch auch eine Online-Auskunft über eine Webseite attraktiv, da die relevanten Informationen aus dem Identity Repository entnommen und die Datenflüsse beispielsweise aus der Architektur des I&AM-Systems abgeleitet werden können.

- Die Betroffenen haben das Recht, falsche Daten korrigieren zu können. Analog zur Selbstauskunft kann die Möglichkeit geschaffen werden, Änderungen online per Webformular durchzuführen. Eine zentrale Fragestellung hierbei ist, wie die Echtheit der vom Benutzer gemachten Angaben verifiziert werden kann. Sowohl das Federated Identity Management als auch das User Centric Identity Management bieten Lösungsansätze, wie entsprechende Daten aus für den Dienstanbieter vertrauenswürdigen Quellen übernommen werden können. Im rein organisationsinternen Fall kann nach wie vor beispielsweise die Überprüfung amtlicher Dokumente oder anderer geeigneter Nachweise erforderlich sein.

- Das Einverständnis zur Erfassung und Verarbeitung der Daten kann widerrufen werden. Der Datensatz des Betroffenen ist in diesem Fall in angemessener Zeit aus den beteiligten Systemen zu entfernen, wodurch in der Regel auch das Vertragsverhältnis mit dem Dienstanbieter endet. Der Widerruf kann auch partiell, zum Beispiel für bestimmte Verarbeitungszwecke, erfolgen und ist geeignet auf die angeschlossenen Systeme abzubilden. Hieraus folgt, dass diese Zwecke bei der Implementierung der Konnektoren zwischen Identity Repository und Zielsystem bekannt sein und geeignet ausgewertet werden müssen.

- Die eingesetzten Datenverarbeitungsverfahren und die Maßnahmen zum Schutz der Daten sind zu dokumentieren. Üblicherweise werden sie dem zuständigen Datenschutzbeauftragten zur Genehmigung vorgelegt, der auch das offizielle Verfahrensverzeichnis pflegt. Darüber hinaus sind je nach Verfahren auch weitere Mitbestimmungsberechtigte, beispielsweise der Personalrat, mit einzubeziehen und entsprechende Rahmenvereinbarungen zu schließen, deren Auswirkungen technisch umzusetzen sind.

  Da die Datenflüsse über das Identity Management System gesteuert werden, liegt es nahe, dieses zu Dokumentationszwecken heranzuziehen. Im Idealfall kann eine Datenflussdokumentation automatisch erstellt und aktuell gehalten werden.

- Die Verarbeitung der Daten muss *zweckgemäß* erfolgen. Die Einhaltung dieser Auflage muss primär von den ans Identity Management System angeschlossenen Diensten sichergestellt werden. Durch geeignete Securitymechanismen ist jedoch zu gewährleisten, dass

das Identity Repository selbst nicht zweckentfremdet wird. Entsprechende Maßnahmen werden in Abschnitt 4.7 diskutiert.

Aktuelle Praktiken und Möglichkeiten zur Umsetzung dieser Datenschutzaspekte werden in Abschnitt 3.5 behandelt.

2.1.1.7. Einbindung in die organisationsinternen Geschäftsprozesse

Die Einführung eines Identity Management Systems hat offensichtlich nicht nur technische Konsequenzen für den Betrieb der einzelnen Dienste, sondern muss auch in den organisatorischen Abläufen entsprechend berücksichtigt werden. Durch die Automatisierung der Benutzerverwaltung in allen angeschlossenen Systemen sind insbesondere in folgenden Prozessen und Geschäftsfunktionen Änderungen notwendig:

- Bei der Einstellung neuer Mitarbeiter oder der Akquisition neuer Kunden ist nur noch eine einmalige Erfassung der relevanten Daten mit entsprechender Zuteilung von Rechten zur Nutzung von Diensten notwendig, so dass dezentrale, dienstspezifische Administrationsschritte weitgehend entfallen können. Insbesondere reduziert sich hierdurch die Wartezeit, bis die neuen Benutzer die Dienste produktiv verwenden können – man spricht vom **Zero-Day Start**, bei dem die Zielsysteme am ersten Tag des Vertragsbeginns mit den benötigten Daten beliefert bzw. der entsprechende Datensatz im Identity Repository zum Abruf freigeschaltet wird.
- Analoges gilt für die Prozesse, die zum Beispiel beim Ausscheiden eines Mitarbeiters durchlaufen werden. Beim Ablauf der Vertragslaufzeit bzw. nach einer pro Service frei wählbaren **Karenzzeit** werden die Berechtigungen des Benutzers bei allen Diensten automatisch entzogen, so dass auf herkömmliche Methoden wie Laufzettel – zumindest bei IT-Diensten – verzichtet werden kann und es beispielsweise nicht mehr zu urlaubsbedingten Verzögerungen kommt.
- Die dezentrale Pflege der Personendaten entfällt; da somit Datenpflege und Datennutzung in der Regel zeitlich, räumlich und organisatorisch getrennt erfolgen, werden Maßnahmen zur Sicherstellung der Datenqualität auf Quellsystemseite notwendig.
- Mit dem zentralen Identity Repository und geeigneten Managementfrontends steht dem Service Desk ein mächtiges Werkzeug zur Verfügung, über das nicht nur viele Informationen über Benutzer abgerufen werden können, sondern das beispielsweise auch ein einfaches Zurücksetzen von Passwörtern ermöglicht. Über standardisierte Schnittstellen wie LDAP wird zudem die direkte Anbindung eines Trouble Ticket Systems ermöglicht.
- Das *Security Management* muss einerseits auf die am Identity Management System beteiligten Komponenten ausgedehnt werden, kann andererseits jedoch vom zentralen Bestand an Authentifizierungs- und Autorisierungsdaten profitieren.
- Das *Change Management* muss die Existenz des Identity Management Systems geeignet berücksichtigen. Da durch die Einführung eines solchen Systems die bereits bestehenden Prozesse zur Verarbeitung von Benutzerdaten lediglich automatisiert und zum Teil vereinfacht werden, ergibt sich daraus nicht zwangsläufig eine höhere Komplexität des

Change Managements. Bedingt durch die Automatisierung kann es jedoch notwendig werden, Teile des Change Managements stärker zu formalisieren, da manuelle Eingriffsmöglichkeiten entfallen können.

- Auch an den übrigen Prozessen ergeben sich Änderungen, die hier am Beispiel der Klassifizierung nach ITIL nur skizziert werden:
  - Incident und Problem Management müssen die Abhängigkeiten der Dienste vom zentralen Identity Repository berücksichtigen.
  - Configuration und Release Management müssen an die Nutzung des I&AM-Systems angepasst werden; beispielsweise könnte die technische Möglichkeit zur nahtlosen Anbindung an das I&AM-System ein ausschlaggebendes Kriterium für die Anschaffung neuer Softwaresysteme werden.
  - Die zeitnahe Freischaltung von Benutzern für Dienste kann sich in besseren QoS-Parametern im Rahmen des Service Level Managements niederschlagen.
  - Eine statistische Auswertung der Benutzerdaten kann im Rahmen des Capacity Managements herangezogen werden, da aus dem zentralen I&AM-System auch dienstübergreifende Abhängigkeiten ersichtlich sind.

2.1.1.8. Szenario 1: Projekt IntegraTUM

Im Rahmen des DFG-geförderten Projekts IntegraTUM wird unter anderem ein Identity & Access Management System für die Technische Universität München (TUM) mit campusweitem Abdeckungsgrad aufgebaut. Dieses Szenario dient einerseits der Veranschaulichung der in den vorangegangenen Abschnitten eingeführten I&AM-Komponenten, andererseits zur Ableitung erster allgemeiner Anforderungen im Hinblick auf eine Erweiterung um FIM-Komponenten.

Ausgangssituation Vor der Einführung eines I&AM-Systems zeichnete sich an der TUM ein hoher Grad an Redundanz im Bezug auf die Erfassung und Pflege von Personendaten ab, da es beispielsweise keinen automatisierten Datenabgleich zwischen den technischen Systemen der Verwaltung, der Bibliothek, den Fakultäten und zentralen IT-Diensten wie dem TUM-Webportal und der E-Learningsoftware gab.

Ein Austausch von Daten zwischen der Verwaltung und den Dienstbetreibern wurde in der Regel einmal pro Semester manuell angestoßen und erfolgte in Dateiformaten, die eine aufwendige manuelle Nachbearbeitung mit sich brachten. Als Konsequenz wurde an vielen Stellen die manuelle Neuerfassung und Pflege von Benutzerdaten bevorzugt, da dadurch eine höhere Datenaktualität bei geringerer Prozesskomplexität realisiert werden konnte.

Auf die damit verbundenen Nachteile für Benutzer, beispielsweise sich für viele Dienste separat registrieren und ihre Daten an vielen Stellen parallel pflegen zu müssen, konnte keine Rücksicht genommen werden. Abbildung 2.7 gibt einen vereinfachten Überblick über die relativ unstrukturierten Flüsse personenbezogener Daten vor der Einführung des I&AM-Systems; einige der offensichtlichen Defizite werden hier nur knapp skizziert:

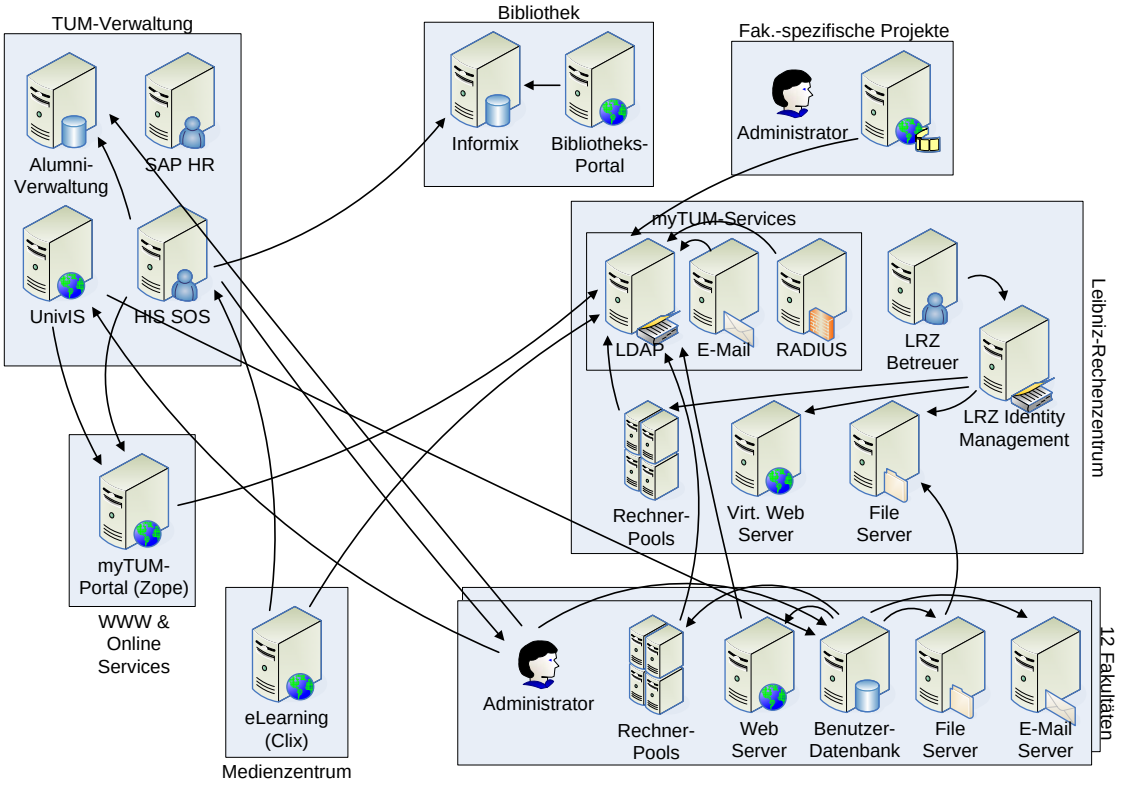


Abbildung 2.7.: Szenario 1: Flüsse von Benutzerdaten vor der Einführung des I&AM-Systems

- Die ins zentrale Personalverwaltungssystem SAP HR eingepflegten Daten werden von keinem anderen Dienst genutzt. Die Bibliothek erhält zwar einen Auszug aus dem Studentenverwaltungssystem HIS SOS, muss Mitarbeiterdaten jedoch wie viele andere TUM-interne Dienstleister selbständig erfassen.
- Durch die Vielzahl eigenständiger Benutzerdatenbasen kommt es zu Inkonsistenzen, da Benutzer ihre Daten häufig nur bei einigen, aber nicht bei allen Diensten zeitnah aktualisieren; durch den nur einmal pro Semester stattfindenden Abgleich von Studentendaten arbeiten mehrere Systeme mit bereits veralteten Daten, obwohl die Aktualisierung in der Verwaltung inzwischen durchgeführt wurde.
- Die Benutzerfreundlichkeit leidet darunter, dass Personen den Zugang zu jedem Dienst separat beantragen und Änderungen an ihren Daten nicht nur einer zentralen, sondern mehreren Stellen kommunizieren müssen.
- Die Skalierbarkeit des Gesamtsystems ist stark begrenzt, da die Einführung weiterer Dienste die Komplexität der Datenflüsse noch weiter erhöhen würde.
- Für das myTUM-Webportal wird bereits ein am LRZ gehosteter LDAP-Server betrieben, der jedoch ein für das Portal optimiertes Datenschema einsetzt. Die Nutzung dieses Datenbestandes durch andere Dienste ist deshalb technisch schwierig und unter dem

Datenschutzaspekt der zweckgemäßen Datennutzung suboptimal.

- Es liegen Abhängigkeiten vor, die sich über mehrere Systeme hinweg erstrecken, wodurch das Change Management deutlich erschwert wird.

Das Projekt IntegraTUM schafft deshalb die organisatorischen und personellen Voraussetzungen, um dienstübergreifend gemeinsam an einer Modernisierung der Informations- und Kommunikationsinfrastruktur zu arbeiten.

Zielsetzung Das IntegraTUM I&AM-System hat die primäre Aufgabe, alle benutzerrelevanten Daten aus den dafür autoritativen Quellen zu aggregieren, zu korrelieren und an die beteiligten Zielsysteme weiterzuleiten. Zu diesem Zweck werden alle Personen erfasst, die im weiteren Sinn als Angehörige der TUM bezeichnet werden können; neben Studenten und Mitarbeitern umfasst dies insbesondere auch Alumni und Gäste. Dabei sind folgende Besonderheiten zu beachten, die Konsequenzen für die Gestaltung des I&AM-Systems haben:

- Die Einteilung in Studenten, Mitarbeiter, Alumni und Gäste ist nicht disjunkt. Beispielsweise sind viele Studenten als Hilfskräfte tätig und werden somit auch als Mitarbeiter geführt. Das I&AM-System muss somit Datensätze aus verschiedenen Datenquellen wie der Studenten- und Personalverwaltung korrelieren können.
- Personen können mehrere Anstellungsverhältnisse an der TUM haben (z. B. zwei Halbtagsstellen in unterschiedlichen Einrichtungen), mehrere Studiengänge belegen oder Gäste mehrerer Einrichtungen sein, woraus sich unterschiedliche Berechtigungen ergeben. Beispielsweise bei der Gästeverwaltung, die naturgemäß dezentral erfolgt, ergeben sich hieraus auch Randbedingungen an die Berechtigungen dezentraler Administratoren, insbesondere im Hinblick auf den Datenschutz.

Abbildung 2.8 verdeutlicht die Anforderungen an das IntegraTUM I&AM-System abstrakt: Das zentrale Identity Repository wird von den autoritativen Datenquellen gespeist und stellt den angebundenen Zielsystemen die korrelierten Daten zur Verfügung. Im Folgenden wird die konkrete Realisierungsarchitektur diskutiert.

Architektur und technische Komponenten Abbildung 2.9 zeigt die Architektur des I&AM-Systems, die vom Autor dieser Arbeit im Rahmen des Projekts IntegraTUM mitgestaltet wurde, mit den daran angeschlossenen Systemen; die in der Abbildung eingekreisten Ziffern korrespondieren mit den in der folgenden Aufzählung angegebenen:

Datenquellen ① Für die Verwaltung von Studenten und Mitarbeitern werden die kommerziellen Systeme HIS SOS und SAP HR eingesetzt, die auf jeweils proprietären Informationsmodellen basieren. Insbesondere fehlt durch Verwendung von Matrikelnummern einerseits und Personalnummern andererseits ein gemeinsames Schlüsselattribut, das zur systemübergreifenden Korrelation der Datensätze herangezogen werden könnte.

Für die Erfassung von Gästen existiert ein dediziertes webbasiertes Managementfrontend, das ins myTUM-Portal integriert ist und von mit der Gästeverwaltung beauftragten

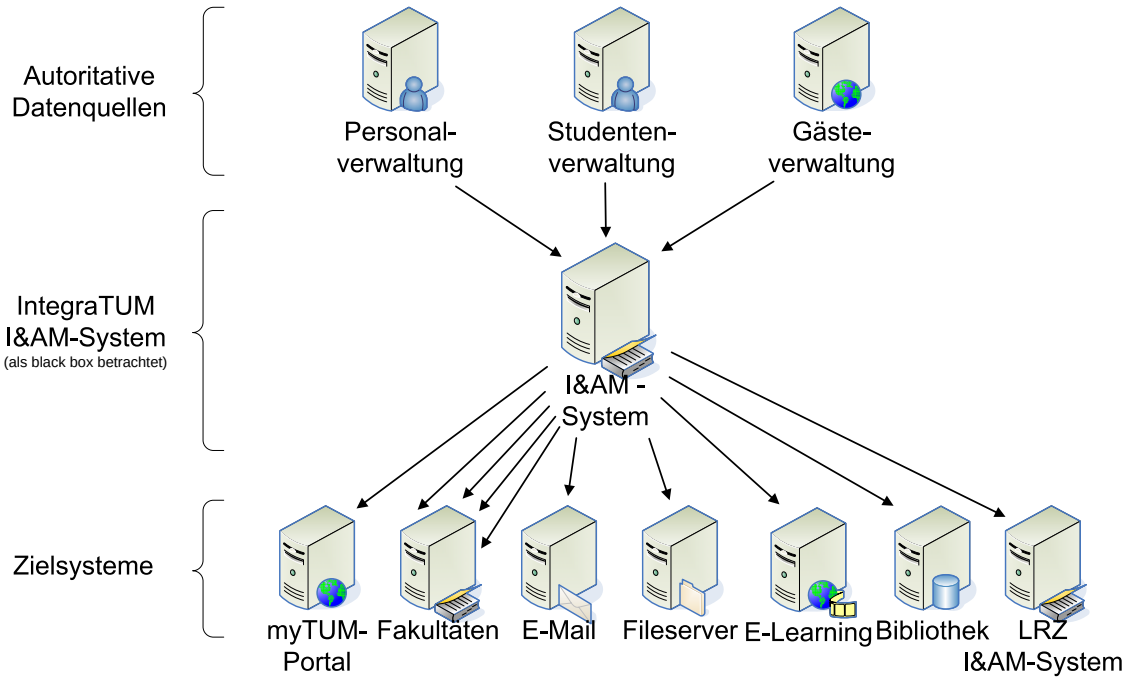


Abbildung 2.8.: Szenario 1: Abstrakte Sicht auf die Benutzerdatenflüsse bei Einführung des I&AM-Systems

Mitarbeitern der Fakultäten genutzt werden kann. In einer späteren Projektphase sollen darüber hinaus Daten externer Bibliotheksnutzer und Gastdozenten von der Bibliothek bzw. über das E-Learning-System eingespeist werden können.

Die Komplexität des Gesamtsystems wird durch die Vielzahl an Datenquellen höher als bei vielen anderen I&AM-Realisierungen, mit denen lediglich Mitarbeiter sowie Kunden und Anwender verwaltet werden (vgl. Szenario 3 in Abschnitt 2.2.1).

Konnektoren ② Zur Anbindung der Quell- und Zielsysteme sowie zum Datenabgleich zwischen den eingesetzten I&AM-Komponenten werden Konnektoren verwendet. Da die technischen Möglichkeiten der angebundenen Systeme und die jeweiligen Anforderungen an die Frequenz des Datenabgleichs variieren, kommen sämtliche Ausprägungen von Konnektoren zum Einsatz (vgl. Abschnitt 2.1.1.3).

Meta-Directory ③ Den Kern des I&AM-Systems bildet ein zentrales Meta-Directory, in dessen Identity Repository alle Hochschulangehörigen mit ihren jeweiligen Berechtigungen erfasst sind. Wie untenstehend erläutert wird, erfolgt der Datenabgleich aus Skalierbarkeits- und Securitygründen nicht direkt mit allen Quell- und Zielsystemen, sondern mit dafür dedizierten Verzeichnisdiensten bzw. einem Provisioningsystem.

Provisioningsystem ④ Mehrere Zielsysteme sind aus Sicht des I&AM-Systems reine Datenkonsumenten, d. h. sie speisen – abgesehen von ggf. notwendigen Initialabgleichen – keine eigenen Daten ins I&AM-System ein. Ihre Anbindung erfolgt deshalb über ein Provisioningsystem.

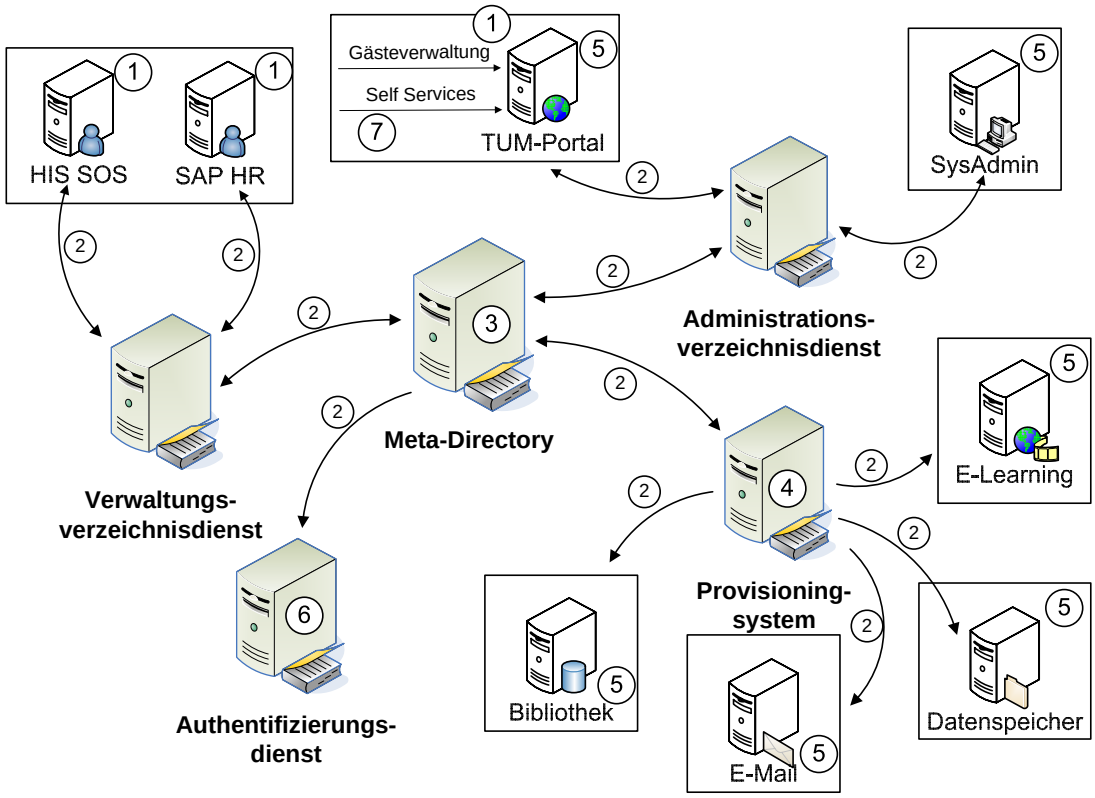


Abbildung 2.9.: Szenario 1: Realisierungsarchitektur des IntegraTUM I&AM-Systems

Zielsysteme ⑤ Im Unterschied zu überschaubaren, zentral verwalteten IT-Landschaften ist es im universitären Umfeld nicht möglich, die zum Einsatz kommenden Zielsysteme strikt vorzugeben oder ihre Beschaffung von der Kompatibilität mit schon vorhandenen Systemen abhängig zu machen. Aus diesem Grund müssen proprietäre Systeme, die zum Teil nicht auf die Integration mit zentralen Benutzerverwaltungen ausgelegt sind, durch die Implementierung neuer Konnektoren an das I&AM-System angebunden werden.

Authentifizierungsdienst ⑥ Um eine durchgängige Benutzung aller IT-Dienste mit demselben Benutzernamen und Passwort im Sinne eines **Unified Login** zu ermöglichen, kommt ein auf die Authentifizierung von Benutzern spezialisierter Verzeichnisdienst zum Einsatz. Er wird insbesondere auch von Systemen genutzt, die nicht direkt mit dem I&AM-System gekoppelt sind; hierzu gehören beispielsweise Webserver von Lehrstühlen und Fachschaften, für die aufgrund ihrer Vielzahl und des eingeschränkten Anwenderkreises eine Anbindung über dedizierte Konnektoren unverhältnismäßig aufwendig wäre. Das **Password Management** sieht vor, dass das für alle angebundenen Dienste zu verwendende Benutzerpasswort ausschließlich über das myTUM-Portal geändert werden kann und über das I&AM-System an alle Dienste, die eine lokale Benutzerauthentifizierung durchführen, sowie den Authentifizierungsdienst propagiert wird; die Verwendung möglichst sicherer Passwörter wird dabei über eine verbindliche **Password Policy** erzwungen, so dass erfolgreichen Brute-Force-Angriffen, bei denen ein Angreifer alle möglichen Zeichenkombinationen ausprobiert, um ein Passwort zu erraten, durch die vorgeschrie-

bene Verwendung von Sonderzeichen und regelmäßige Passwortänderungen vorgebeugt wird.

Self Services ⑦ Eine Sonderrolle unter den Zielsystemen nimmt das TUM-Webportal ein, da es als Managementschnittstelle zu Anwendern und Administratoren dient. Es bietet beispielsweise die als *Self Service* bezeichnete Funktionalität, dass Anwender ihre E-Mail-Adresse konfigurieren und ihre Stammdaten einsehen und partiell ändern können. Somit fungiert das Webportal als Quelle für selektive Datenmodifikationen, die insbesondere an die führenden Systeme der Studenten- und Personalverwaltung zu propagieren sind.

Replikate (nicht eingezeichnet) Die Hochverfügbarkeit des I&AM-Systems wird durch die redundante Bereitstellung seiner Komponenten in Form von Replikaten erreicht. Sie kommen bei unvorhergesehenen Problemen wie Hardwaredefekten und bei Wartungsarbeiten wie Software-Updates zum Einsatz, da längere Ausfallzeiten aufgrund der Vielzahl von Geschäftsprozessen, die sich auf das I&AM-System abstützen, unbedingt vermieden werden müssen und die Koordination geplanter Ausfallzeiten aufgrund der Vielzahl beteiligter Systeme im Allgemeinen zu aufwendig ist.

Interne Dienste (nicht eingezeichnet) Zu Administration der Komponenten des I&AM-Systems kommt ein herstellerspezifisches, webbasiertes Managementfrontend zum Einsatz. Verschiedene Funktionen wie das Erzeugen von Benutzernamen und Initialpasswörten werden durch eigene Implementierungen realisiert, die in Form von Web Services zur Verfügung stehen und auf einem dedizierten Server (nicht eingezeichnet) betrieben werden.

Darüber hinaus existieren Schnittstellen zu nicht I&AM-spezifischen Systemen, beispielsweise zum System- und Servicemonitoring, Accounting und Service Desk; auf sie wird in Kapitel 4 näher eingegangen.

Technische Kernaspekte Dadurch, dass das I&AM-System Kennungen in den Zielsystemen anlegen, aktualisieren, sperren und löschen kann, reduziert sich die lokale Benutzerverwaltung auf die Vergabe applikationsspezifischer Berechtigungen. Bei der zentralen Verwaltung der Benutzer und ihrer Rechte können jedoch nach wie vor manuelle administrative Eingriffe notwendig werden:

- Die Korrelation der in den Quell- und Zielsystemen schon vor der Einführung des I&AM-Systems vorhandenen Datensätze muss aufgrund des Fehlens eines gemeinsamen Schlüsselattributs auf Basis von Heuristiken wie übereinstimmenden Vor- und Nachnamen sowie Geburtsdaten durchgeführt werden.

  Da die **Datenqualität** in der Praxis, z.B. aufgrund von Tippfehlern, nicht perfekt ist, und da es nicht ausgeschlossen ist, dass zwei unterschiedliche Personen denselben Vor- und Nachnamen sowie dasselbe Geburtsdatum haben, sind jedoch manuelle Eingriffe, mindestens in Form von Bestätigungen, zum Teil auch in Form von Korrekturen notwendig.

  Ein zentraler organisatorischer Aspekt des Projekts IntegraTUM ist deshalb die systemübergreifende Einführung eines künstlichen Schlüsselattributs für erfasste Personen,

das insbesondere bei der Neuerfassung von Personen in den Datenquellen berücksichtigt wird, um Mehrfacheinträge derselben Person zu vermeiden.

Da prinzipiell nicht ausgeschlossen werden kann, dass die Korrelation trotz dieser technischen Maßnahmen fehlschlägt und eine Person doppelt eingetragen wird, wird im Rahmen der Self Services die Möglichkeit zur Zusammenführung mehrerer Datensätze derselben Person angeboten.

- Die Vergabe von Rechten an Benutzer erfolgt rollenbasiert; beispielsweise ist für Mitarbeiter und Studenten in Form von **Rollen** festgelegt, welche Systeme sie mit welchen Einschränkungen nutzen können. Die Zuordnung zu einer Rolle erfolgt dabei in Abhängigkeit von dem Quellsystem und ausgewählten Teilen der Datensätze, beispielsweise der Fakultätszugehörigkeit eines Mitarbeiters. Sofern die Rechte individuell erweitert werden sollen, muss ein entsprechender Workflow durchlaufen werden, der beispielsweise die Schritte „Beantragung durch den Benutzer“ und „Genehmigung durch einen Administrator“ umfasst.

- Neben einer Zuweisung von Rollen ist auch die Einteilung in **Gruppen** notwendig, um beispielsweise zielgerichtete E-Mail-Verteiler und Dateiablagebereiche erstellen zu können. Die Zugehörigkeit zu Gruppen kann entweder automatisch aus den Daten einer Person (z. B. „alle Studenten im ersten Semester“) abgeleitet oder muss manuell spezifiziert werden (z. B. „alle Teilnehmer an einem Projekt“). Es ist deshalb notwendig, dass neben Personen- auch Gruppeninformationen abgerufen werden können.

Der Einsatz des Verbundes mehrerer I&AM-Komponenten, insbesondere der Verzeichnisdienste, dient folgenden Zwecken:

- Aufgrund der Heterogenität und Inflexibilität der anzubindenden proprietären Systeme kann kein Datenmodell konstruiert werden, das für alle Systeme eingesetzt werden könnte. Vielmehr sind durch die Konnektoren umfassende Datenkonvertierungen vorzunehmen; in den beteiligten Verzeichnisdiensten können die Daten zum Abruf in verschiedenen Formaten bereitgestellt werden.

- Die Vielzahl sowohl darauf zugreifender Client-Systeme als auch eingesetzter Konnektoren resultiert in der Notwendigkeit zur **Lastverteilung**, die auch durch die geeignete Platzierung der Verzeichnisdienste in der Netzwerkinfrastruktur und den Einsatz zusätzlicher Replikate weiter unterstützt werden kann.

- Es erfolgt eine Integration in das unten beschriebene Sicherheitskonzept, so dass pro Verzeichnisdienst nur diejenigen Daten vorgehalten werden müssen, die von daran angeschlossenen Systemen benötigt werden; somit kann der Schaden im unwahrscheinlichen, aber nicht auszuschließenden Fall, dass beispielsweise aufgrund eines Softwarefehlers ein Verzeichnisdienst kompromittiert wird, begrenzt werden.

Datenschutz Die Berechtigung zur Erfassung und Verarbeitung personenbezogener Daten von Studenten ergibt sich aus dem bayerischen Hochschulgesetz, so dass für diesen Anwenderkreis kein explizites Einverständnis einzuholen wäre. Um die datenschutzrechtlich relevanten Prozesse jedoch für alle Benutzer transparent zu gestalten, werden Studenten wie auch

Mitarbeiter und Gäste über die Benutzerrichtlinien der TUM und damit der elektronischen Verarbeitung ihrer Daten informiert und müssen dieser zustimmen.

Über Self Services im TUM-Webportal kann jede erfasste Person konfigurieren, welche Teilmengen ihrer personenbezogenen Daten von anderen Mitarbeitern, Studenten bzw. allen Personen eingesehen werden dürfen. Darüber hinaus besteht in den angeschlossenen Diensten die Möglichkeit zur Verfeinerung dieser Konfiguration; beispielsweise kann im Rahmen des E-Learning-Systems festgelegt werden, dass Kontaktinformationen nur denjenigen anderen Studenten angezeigt werden, die mit der betroffenen Person an einer gemeinsamen Vorlesung teilnehmen.

Um die Sicherheit der Daten zu gewährleisten, wird das I&AM-System wie folgt in eine gesamtheitliche **Sicherheitsinfrastruktur** integriert:

- Der Zugang zu den Systemen und der Zugriff auf die Daten werden auf mehreren Ebenen geschützt:
  - Die Hardware, auf der die Dienste betrieben werden, wird in einem Serverraum betrieben, zu dem ein physischer Zugang nur ausgewählten Personen möglich ist.
  - Der Zugang zu den Diensten über Netzwerk ist mittels Firewalls, Zertifikaten und Passwörtern auf ausgewählte Maschinen und Personen beschränkt.
  - Der Abruf von Daten wird über **Access Control Lists (ACLs)** gesteuert, so dass authentifizierte Benutzer nur auf diejenigen Daten zugreifen können, für die sie explizit autorisiert wurden.
  - In jedem Verzeichnisdienst werden nur die von den daran angeschlossenen Systemen benötigten Informationen gespeichert.
- Die Übertragung der Daten erfolgt ausschließlich verschlüsselt. Die dazu eingesetzten Verfahren *Secure Socket Layer* (SSLv3) bzw. *Transport Layer Security* (TLSv1) dienen darüber hinaus der starken Authentifizierung und der Sicherstellung der Integrität der übertragenen Daten.
- Schreibender Zugriff auf den Datenbestand unterliegt **Plausibilitätsprüfungen**, die ein versehentliches oder absichtliches Modifizieren der Daten mit schlechter Datenqualität bzw. Falschinformationen zwar nicht vollständig verhindern, aber deutlich erschweren können.
- Ausgewählte lesende und schreibende Zugriffe werden protokolliert; die dabei anfallenden Logfiles werden im Rahmen von regelmäßigen **Audits** auf Auffälligkeiten untersucht und unterstützen die IT-forensische Analyse beim Bekanntwerden sicherheitsrelevanter Vorfälle.
- Die Serversysteme und das lokale Netzwerk, in dem sie betrieben werden, sind an Monitoring- bzw. Intrusion-Detection-Systeme angebunden, die auffällige Zugriffe auf Basis von Signaturen bzw. Heuristiken erkennen können.
- Alle beteiligten Systeme werden größtenteils automatisiert mit Betriebssystem- und Softwareaktualisierungen versorgt. Sofern das Einspielen eines Updates mit einem temporären Ausfall des Dienstes verbunden ist, wird es manuell zu einem geeigneten Zeit-

punkt durchgeführt; die Redundanz der Hardware ermöglicht dabei ein für die angeschlossenen Systeme und Anwender transparentes Vorgehen.

Eine Auskunft über die gespeicherten Daten im Rahmen der informationellen Selbstbestimmung ist über schriftliche Anfragen, persönliches Erscheinen am Service Desk bei Vorlage eines Lichtbildausweises und über das Webportal nach Authentifizierung möglich.

Die Prozesse und Implementierungen werden mit dem Datenschutzbeauftragten der TUM abgesprochen und von diesem in das offizielle Verfahrensverzeichnis aufgenommen; ebenso wird der Einbeziehung der Personalvertreter Folge geleistet. Neue Systeme werden an das I&AM-System nur angebunden, wenn auch für sie eine entsprechende Datenschutzfreigabe vorliegt, in der auch die Übernahme von Daten aus den zentralen Beständen spezifiziert wird.

Organisatorische Aspekte Mit der Einführung eines I&AM-Systems an der TUM ist eine umfassende Optimierung der von ihm unterstützten Geschäftsprozesse verbunden, die auf die Nutzung der neu geschaffenen technischen Möglichkeiten abzielt. Im Folgenden werden drei ausgewählte Aspekte skizziert, die auch andere Organisationen bei der Einführung eines I&AM-Systems betreffen würden:

1. Anpassung von Verwaltungsprozessen: Durch den Aufbau eines zentralen Datenbestandes erhöhen sich die Anforderungen an die Datenqualität in den Quellsystemen, während sich der Aufwand zur Akquisition und Pflege von Daten in den Zielsystemen reduziert:

   - Über die Quellsysteme sind nach Möglichkeit *alle* für die Zielsysteme relevanten Daten zu erfassen. Ausgenommen hiervon sind lediglich servicespezifische Daten, die erst bei der Nutzung der Dienste und nicht bereits bei ihrer Bereitstellung anfallen bzw. für die durch Konnektoren eingetragene Voreinstellungen nicht ausreichen (vgl. Profildaten in Abschnitt 2.1.2.2).
   - Die Qualität der in den Quellsystemen erfassten Daten muss beispielsweise hinsichtlich Aktualität und Fehlerrate (z. B. Tippfehler) den Zielsystemen genügen.
   - Die Quellsysteme müssen eine prozessübergreifende Personenkorrelation so weit unterstützen, dass eine in mehreren Quellsystemen geführte Person zu einem einzigen und nicht zu mehreren Einträgen im I&AM-System führt. Dies kann in der Regel durch geeignete Schnittstellen zu den I&AM-Komponenten gewährleistet werden, die entsprechende Such- und Korrelationsfunktionalität bieten.
   - Der bisherige Prozess zum Einspielen und Pflegen der Daten im Zielsystem ist durch die Anbindung an das I&AM-System zu ersetzen. Sofern der Konnektor zwischen I&AM-System und Zielsystem nicht bidirektional arbeitet, also Datenänderungen, die im Zielsystem durchgeführt werden, in den zentralen Bestand übernimmt, sind eventuell im Zielsystem angebotene Möglichkeiten zur Pflege der eigenen Daten zu deaktivieren. In diesem Fall sind die Dienstnutzer geeignet darüber zu informieren, dass sie ihre Daten z. B. nur noch über das zentrale Webportal aktualisieren können. In der Praxis trifft dies bei fast allen Diensten auf Passwortänderungen zu, die im Dienst unterbunden und über einen zentralen Self Service durchgeführt werden müssen; der technische Grund dafür ist, dass lokale Passwortänderungen in den Diensten häufig nicht „abgefangen“ werden können, um das neue Passwort dienstübergreifend synchronisieren zu können.

- Da mit der Einführung des I&AM-Systems beispielsweise bei der Universitätsbibliothek keine explizite manuelle Registrierung mehr notwendig ist, kann die Ausgabe des Bibliotheksausweises mit der Erstimmatrikulation von Studenten zusammengelegt werden und somit den beidseitigen Aufwand reduzieren. Das I&AM-System bildet damit auch die Grundlage für die Optimierung von Prozessen, die keinen unmittelbaren technischen Bezug zu ihm haben.

2. Integration in den Service Desk: Durch die Bereitstellung eines zentralen Systems, über das die für alle Dienste relevanten Benutzerdaten und die individuellen Berechtigungen der Benutzer abgerufen werden können, kann die Funktionalität, die dem First Level Support zur Verfügung gestellt wird, deutlich erweitert werden.

   Insbesondere können Routineaufgaben wie das Zurücksetzen von vergessenen Passwörtern effizienter zentral durchgeführt werden, ohne den Second Level bzw. einen dienstespezifischen Support involvieren zu müssen. Voraussetzung hierfür ist die Schaffung geeigneter Managementschnittstellen, die insbesondere auch das Abrufen von Monitoringinformationen umfasst, da sich beispielsweise durch die Einführung eines zentralen Authentifizierungsdienstes neue Abhängigkeiten und potentielle Fehlerquellen ergeben.

3. Neben dem nach ITIL als Funktion klassifizierten Service Desk ergeben sich auch Änderungen für Querschnittsprozesse wie das Security Management. Die Übernahme von Benutzerdaten aus dem I&AM-System und die Delegation von Aufgaben wie der Authentifizierung ist nicht nur sicherheitsrelevant, sondern muss beispielsweise auch vom Change Management geeignet berücksichtigt werden.

Die Auswirkungen auf das IT Service Management werden in Kapitel 4 näher betrachtet.

2.1.1.9. Anforderungen an FIM bei gegebenem I&AM-System

Im Folgenden werden auf Basis des im vorhergehenden Abschnitt erläuterten Szenarios allgemeine Anforderungen an I&AM-Systeme und FIM-Komponenten abgeleitet, wenn ein bereits bestehendes I&AM-System um organisationsübergreifenden Personendatenaustausch erweitert werden soll. Die hier erarbeiteten generellen Anforderungen werden auf Basis der weiteren Szenarien verfeinert und in Abschnitt 2.3 zusammengefasst und katalogisiert.

Die Anforderungen werden hier und in allen nachfolgenden Szenarien in die Kategorien *funktional*, *nichtfunktional technisch*, *sicherheitsspezifisch*, *organisatorisch* und *datenschutzspezifisch* eingeteilt. Diese Form der Anforderungsgruppierung wurde gewählt, da eine Analyse dieser fünf Aspekte auch bei einer anderen Kategorisierung notwendig wäre. In einigen Fällen treten verschiedene Aspekte eines Kriteriums in mehreren Kategorien auf; beispielsweise ist die Kontrolle, welche Daten an welche Zielsysteme übermittelt werden dürfen, einerseits sicherheitsrelevant, z. B. zur Verhinderung von Industriespionage in Business-to-Business-Szenarien, andererseits datenschutzrelevant in nahezu allen Szenarien. Diese Nuancen sind für die Bewertung von FIM-Konzepten relevant und werden deshalb explizit als separate Anforderungen festgehalten.

In eckigen Klammern werden jeweils Kurzbezeichnungen für die Anforderung angegeben, um diese im Rahmen der weiteren Szenarien referenzieren zu können. Auf die explizite Nennung sehr grundlegender Anforderungen, die von allen FIM-Ansätzen bereits erfüllt werden, wird bewusst verzichtet, da sie für die weitere Analyse nicht relevant sind.

Funktionale Anforderungen Die folgenden funktionalen Anforderungen ergeben sich aus der abstrakten Betrachtung einer externen Organisation als zusätzliche Datenquelle bzw. als weiteres Zielsystem für ein bereits vorhandenes I&AM-System:

- Es müssen Mechanismen zur Datensatzkorrelation unterstützt werden, um einen Benutzer, der bereits erfasst wurde oder im Zielsystem bereits eingetragen ist, nicht mehrfach in den jeweiligen Datenbestand aufzunehmen [FA-Korrelation].
- Die Daten müssen zwischen dem fremden und dem lokal benötigten Format umgewandelt werden können, das beispielsweise durch ein LDAP-Schema spezifiziert wird; hierzu sind ggf. wie in I&AM-Konnektoren Datenkonversionen durchzuführen und die Verfügbarkeit von Pflichtangaben sicherzustellen (vgl. als *mandatory* gekennzeichnete Datenfelder in Abschnitt 2.1.2.4) [FA-Schema].
- Änderungen an den Datenbeständen müssen zeitnah an alle anderen Organisationen, denen Informationen über den Benutzer zur Verfügung gestellt worden sind, propagiert werden, um Inkonsistenzen zu vermeiden [FA-Updates].
- Modifikationen, die eine andere Organisation an den Daten eines Benutzers durchgeführt hat, sollen selektiv in den lokalen Datenbestand übernommen werden können [FA-Schreibzugriff].

Nichtfunktionale technische Anforderungen Die folgenden Anforderungen betreffen Anforderungen an zu integrierende FIM-Komponenten, die zwar technische Aspekte betreffen, jedoch nicht direkt mit deren Funktionalität zusammenhängen.

- Das eingesetzte Verfahren muss ausreichend skalierbar sein, um effizient mit anderen Organisationen Personendaten austauschen zu können; dies umfasst die Unterstützung von
  - potentiell beliebig vielen externen Datenquellen bzw. -abnehmern.
  - einer beliebigen Anzahl lokaler Dienste, die anderen Einrichtungen zur Verfügung gestellt werden sollen.
  - langlebigen, fixierten Schnittstellen zwischen I&AM- und FIM-Komponenten, um über eine Entkopplung das Change Management zu erleichtern.
  - Hochverfügbarkeits- und Lastverteilungsverfahren.

  Diese Aspekte werden in Kapitel 4 vertieft; für die Analyse werden sie zu einer Anforderung zusammengefasst [NFA-Skalierbarkeit].
- Existierende Managementfrontends und -werkzeuge sollen beibehalten werden und auf den Gesamtbenutzerbestand angewendet werden können, beispielsweise im Bezug auf Rechteverwaltung und Accounting [NFA-Management].
- Die FIM-Komponenten sollen plattform- und betriebssystemunabhängig sein, um flexibel mit verschiedenen I&AM-System zusammenarbeiten zu können [NFA-Portabilität].

Sicherheitsanforderungen Die folgenden Anforderungen zielen auf eine grundlegende Integration in bereits vorhandene Sicherheitsinfrastrukturen ab:

- Das Anlegen von Benutzern durch andere Organisationen muss an Genehmigungsprozesse gekoppelt oder zumindest selektiv unterbunden werden können, um beispielsweise aufgrund von Missbrauchsfällen gesperrten Benutzern den Zugriff auf lokale Dienste verbieten zu können [SEC-Genehmigung].
- Der Datentransfer muss *sicher* erfolgen; dies umfasst insbesondere:
  - Die Gegenstelle muss identifiziert und authentifiziert werden, beispielsweise über Serverzertifikate.
  - Die Integrität der übertragenen Daten muss gewährleistet werden, z. B. durch kryptographische Prüfsummen.
  - Die Vertraulichkeit der Daten muss beispielsweise durch Verschlüsselung gewährleistet werden.

  Darüber hinaus sind FIM-Datenaustauschprotokolle so zu konstruieren, dass sie keine grundlegende Designschwäche haben, die solche technischen Schutzmaßnahmen außer Kraft setzen würden [SEC-Datenübertragung].
- Die tatsächliche Nutzung von Diensten über FIM darf vom Benutzer nicht erfolgreich abgestritten werden können (engl. *non-repudiation*) [SEC-Unleugbarkeit].
- Die FIM-Komponenten müssen nahtlos in die bestehenden Netzwerk- und Systemsicherheitsprozesse integrierbar sein. Dies umfasst insbesondere
  - das Verbot direkter Schreibzugriffe auf den lokalen Benutzerdatenbestand.
  - das Vermeiden eines Lockern von Restriktionen, z. B. an Firewalls, um einen direkten Zugriff auf den lokalen Datenbestand zu ermöglichen, wenn dieser vorher bewusst von externen Zugriffen abgeschottet war.
  - das Verhindern, dass bereits eingerichtete Zugriffskontrollbeschränkungen, beispielsweise LDAP Access Control Lists, umgangen werden können.
  - den Schutz vor Angriffen auf die Verfügbarkeit des I&AM-Systems, z. B. in Form von (distributed) Denial of Service Attacken.
  - die Anwendbarkeit von Werkzeugen wie Intrusion Detection Systemen.

  Diese Aspekte werden wiederum in Kapitel 4 näher diskutiert, für die Analyse jedoch zu einer Anforderung zusammengefasst [SEC-Integration].

Organisatorische Anforderungen Die auf organisatorischer Ebene durchzuführenden Vorbereitungen für FIM-basierten Datenaustausch stellen wie auch die technischen Anforderungen komplexe Herausforderungen dar, die in Abschnitt 2.1.2 vertieft werden; grundlegend sind folgende Randbedingungen zu berücksichtigen:

- Die Datenquellen müssen frei gewählt werden können; insbesondere muss eine Einschränkung auf vertrauenswürdige Datenquellen realisierbar sein [ORG-Trust].

- Die Datenqualität und andere im Rahmen von Service Level Agreements vereinbarte Gütemerkmale müssen in Form von Policies spezifiziert werden können, deren Einhaltung automatisiert überwacht werden kann [ORG-SLAs].
- Je nach Szenario kann über den reinen Austausch von Personendaten auch der Aufbau eines verteilten Autorisierungssystems erforderlich sein, bei dem die Datenquelle mitbestimmt, welche Dienste ein Benutzer beim Empfänger der Daten nutzen darf. Hierfür muss ein geeigneter Autorisierungsprozess definiert werden, der durch die FIM-Lösung abgebildet werden kann [ORG-Autorisierung].

Datenschutzanforderungen Durch die Weitergabe bzw. den Bezug personenbezogener Daten an bzw. von Dritten werden die datenschutzrechtlichen Anforderungen nochmals verschärft. Eine vertiefende Diskussion erfolgt in Abschnitt 2.1.2.6 und den Szenarien 3–5. Grundlegend sind folgende Anforderungen festzuhalten:

- Seitens der Datenquelle muss es möglich sein, die Menge der über erfasste Personen ausgetauschten Daten einschränken zu können. Die Steuerung erfolgt dabei über so genannte Attribute Release Policies (vgl. Abschnitt 3.5) [DSA-ARPs].
- Häufig ist es erforderlich, dass die betroffenen Personen selbst diese selektive Freigabe ihrer Daten konfigurieren können; dies impliziert, dass die Betroffenen über die Weitergabe ihrer Daten an Dritte informiert werden und dieser zustimmen [DSA-Zustimmung].

Die genannten Anforderungen werden aus Sicht *einer* an einem FIM-Prozess beteiligten Organisation gestellt; die weiteren Szenarien gehen darüber hinaus auch auf die Benutzer- sowie die Föderationsperspektive ein.

2.1.2. Federated Identity Management

In diesem Abschnitt werden die Prozesse und Workflows von Federated Identity Management (FIM) vertieft. Nach einer kurzen Skizzierung der grundlegenden Motivation für den Einsatz von FIM wird in Abschnitt 2.1.2.2 beschrieben, welche Daten mittels FIM prinzipiell zwischen den beteiligten Organisationen ausgetauscht werden können. Dies führt zu der Definition eines FIM-Rollenmodells für Organisationen in Abschnitt 2.1.2.3.

In Abschnitt 2.1.2.4 wird anschließend näher auf die Modellierung von *allgemeinen Identitätsdaten eingegangen*, die eine von drei Datenkategorien darstellen, die mittels FIM ausgetauscht werden können; diese Beschreibung gilt prinzipiell auch für I&AM-Systeme sowie für das User Centric Identity Management (UCIM), spielt jedoch im Hinblick auf die Interoperabilität von FIM-Systemen eine so wesentliche Rolle, dass sie hier in den FIM-Kontext eingegliedert wurde.

Der organisationsübergreifende Datenaustausch stellt besondere Anforderungen an die Beziehungen zwischen den beteiligten Organisationen sowie zwischen den Benutzern und den involvierten Dienstleistern. In den Abschnitten 2.1.2.5 und 2.1.2.6 wird deshalb auf die Aufgaben des Trust Managements im FIM-Umfeld sowie auf die grundlegenden Datenschutzanforderungen eingegangen.

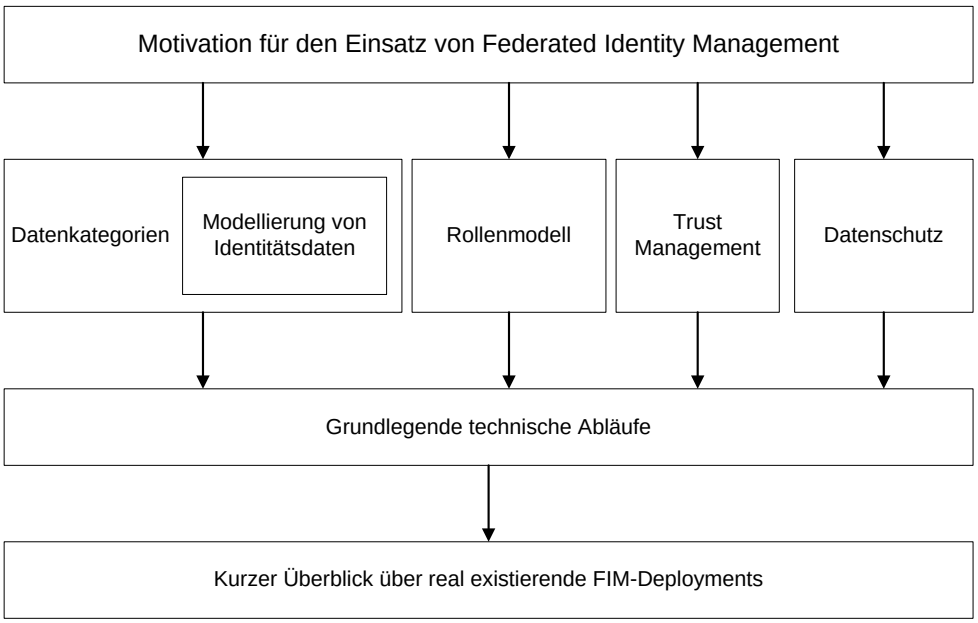


Abbildung 2.10.: Vorgehensmodell für die grundlegende Diskussion von FIM

Die prinzipiellen technischen Abläufe werden in Abschnitt 2.1.2.7 diskutiert; den Abschluss bildet eine Übersicht über real existierende FIM-Deployments, die für eine erste Einschätzung des Reifegrads von FIM herangezogen werden kann. Szenarien und Anforderungen werden in Abschnitt 2.2 diskutiert, um auch die in Abschnitt 2.1.3 erläuterten UCIM-Aspekte, die für FIM relevant sind, berücksichtigen zu können.

Abbildung 2.10 zeigt das für diesen Abschnitt gewählte Vorgehensmodell.

2.1.2.1. Motivation für FIM

Das elementare Ziel von FIM ist die organisationsübergreifende Übermittlung von personenbezogenen Daten, von der sowohl die beteiligten Organisationen als auch die Benutzer profitieren sollen. Die wichtigsten Mehrwerte ergeben sich für den Empfänger dieser Daten:

- Der manuelle Aufwand zur initialen Eintragung der Daten wird weitestgehend eliminiert bzw. auf diejenigen Informationen reduziert, die für den Dienstleister spezifisch sind. Dies resultiert in einer unmittelbaren Zeitersparnis und **Effizienzsteigerung**.
- Die **Datenqualität** kann dadurch erhöht werden, dass Informationen über eine Person nur von vertrauenswürdigen Datenquellen akzeptiert werden. Dadurch kann auch der Aufwand zur Überprüfung der gemachten Angaben reduziert werden.

Die **Benutzerfreundlichkeit** wird gesteigert, da die Pflege der Daten im Idealfall nur noch an einer zentralen Stelle erfolgen muss und Änderungen an diejenigen Dienstleister, die diese Daten übernommen haben, automatisch propagiert werden. Ein Benutzer kann somit beispielsweise nicht mehr versäumen, dass er seine Adressänderung noch anderen Dienstleistern

mitteilen muss, so dass Inkonsistenzen verhindert werden. Allgemein wird ein Anstieg der Datenqualität auch davon erwartet, dass Benutzer von der häufig als lästig empfundenen Aufgabe, bei jedem Dienstanbieter ihre persönlichen Daten manuell eintragen zu müssen, entbunden werden.

Für die als Datenquellen fungierenden Identity Provider ergibt sich der aus Datenschutzperspektive nicht unkritische Vorteil, dass sie wissen, welche Daten von welchem Dienstleister über welche Benutzer abgerufen werden. In Business-to-Business-Szenarien kann somit die unbedachte manuelle Herausgabe zu vieler Informationen über die eigenen Mitarbeiter technisch unterbunden werden. In anderen Fällen kann es unerwünscht sein, dass als Identity Provider agierende Organisationen diese Möglichkeit zur Profilbildung über ihre Benutzer haben, wodurch der Einsatz von UCIM motiviert wird, bei der jeder Benutzer als sein eigener Identity Provider auftreten kann (vgl. Abschnitt 2.1.3). In der Praxis muss deshalb häufig ein Kompromiss aus Datenqualität sowie möglichst weitgehender Automatisierung und den Schutzinteressen der Benutzer gefunden werden.

2.1.2.2. Datenkategorisierung

Die Klassifikation der im Rahmen von FIM übertragenen Daten erfolgt hier in Anlehnung an SAML (siehe Abschnitt 3.2.1 auf Seite 116) und hat sich inzwischen weitgehend durchgesetzt. Demnach lassen sich die folgenden drei Hauptkategorien unterscheiden:

1. **Authentifizerungsbestätigungen** (engl. *authentication assertion*), in denen festgehalten wird, dass sich der Benutzer beim Aussteller der Bestätigung erfolgreich authentifiziert hat. Sofern der Empfänger dieser Bestätigung dem Aussteller vertraut und eine Fälschung der Bestätigung ausgeschlossen werden kann, kann eine erneute Authentifizierung des Benutzers beim Empfänger entfallen.

   Konkret kann dadurch ein *organisationsübergreifendes* ***Single Sign-On*** erreicht werden, das bedeutet, dass der Benutzer beispielsweise nach einmaliger Eingabe seines Passworts für den Dienst einer Organisation auch die Dienste anderer Organisationen benutzen kann, ohne das Passwort erneut eingeben zu müssen. Neben einer Steigerung der Benutzerfreundlichkeit wird dadurch erreicht, dass verschiedenen Problemen bei dezentraler Passworteingabe vorgebeugt wird: Beispielsweise kann dadurch beim Empfänger der Daten auf Prozesse für vergessene und zurückzusetzende Passwörter verzichtet werden und das Risiko, dass Benutzer aus praktischen Gründen für verschiedene Dienste dasselbe Passwort verwenden, wird eliminiert.

2. **Autorisierungsbestätigungen** (engl. *authorization assertion*), anhand derer der Aussteller der Bestätigung positive und ggf. auch negative Autorisierungsentscheidungen zur Nutzung von Diensten des Empfängers der Bestätigung kommunizieren kann.

   Sofern der Empfänger dem Aussteller vollständig vertraut, kann somit auf die Speicherung von Autorisierungsinformationen lokal beim Empfänger verzichtet werden; dies lässt sich insbesondere in Outsourcingszenarien effizient einsetzen. Praktisch relevant ist ferner eine Kombination lokaler und verteilter Autorisierung, bei der die Dienstnutzung nur gestattet wird, nachdem sie sowohl vom Aussteller als auch vom Empfänger einer solchen Bestätigung autorisiert wurde.

3. Allgemeine Benutzerinformationen. In diese Kategorie fallen alle Daten, die weder Authentifizierungs- noch Autorisierungsbestätigungen sind. Da Identitäten häufig objektorientiert modelliert werden, entsprechen die atomaren übertragbaren Daten den Attributen dieser Objekte, so dass diese Kategorie technisch als **allgemeine Attributsauskunft** (engl. *attribute assertion*) bezeichnet wird.

   Dabei sind folgende Aspekte zu berücksichtigen:

   - Aus den übermittelten Attributen können empfängerseitig durchaus Autorisierungen abgeleitet werden, ohne dass eine explizite Autorisierungsbestätigung vorliegen muss; die Übertragung erfolgt jedoch ohne diese Semantik.
   - Die so übermittelten Daten können in beliebige Subkategorien untergliedert werden. Häufig wird zwischen **Identitäts-** und **Profildaten** unterschieden [PESA]. Identitätsdaten umfassen dabei alle stark personenbezogenen Daten wie Namen und Anschriften; in Profildaten werden hingegen beispielsweise Customizing-Optionen für Applikationen hinterlegt. Da die Semantik eines Attributs jedoch nicht ohne weitere Angaben bestimmt werden kann, erfolgt eine derartige Subkategorisierung nicht automatisch.

   Offensichtlich wird über diese dritte Datenkategorie ein sehr flexibler Austausch nahezu beliebiger Informationen ermöglicht, so dass ein gemeinsames Verständnis von Syntax und Semantik auf Absender- und Empfängerseite vorausgesetzt werden muss.

Alle übertragenen Daten sind üblicherweise mit **Metadaten**, z. B. einem Zeitstempel sowie einer Gültigkeitsdauer, versehen, um Missbrauch vorzubeugen. Die Integrität, Authentizität und Vertraulichkeit der Daten kann durch kryptographische Maßnahmen wie Prüfsummen, digitale Signaturen und Verschlüsselung gewährleistet werden. Die dazu in der Regel notwendige **Public Key Infrastruktur** (PKI) stellt jedoch eine nicht triviale Randbedingung dar, deren Auswirkungen in Kapitel 3 vertieft dargestellt werden.

2.1.2.3. FIM-Rollenmodell

Im Umfeld des Federated Identity Managements können Organisationen in verschiedenen Rollen agieren, die nachfolgend skizziert werden:

- **Identity Provider (IDP)**: Ein IDP ist eine autoritative Datenquelle für die im vorhergehenden Abschnitt erläuterten Authentifizierungsbestätigungen und in der Regel die primäre Datenquelle für Autorisierungsbestätigungen sowie allgemeine Attributsauskünfte. In den meisten Fällen entspricht der IDP der Heimateinrichtung des Benutzers, in Business-to-Business (B2B) Outsourcingszenarien also beispielsweise dem Arbeitgeber eines Benutzers.

  Charakteristisch für alle FIM-Ansätze ist, dass jede Identität *genau einem* IDP zugeordnet sein muss; hierbei existieren die folgenden Sonderfälle:

  1. Der Benutzer kann mehrere digitale Identitäten haben oder verschiedene Rollen einnehmen, die mit unterschiedlichen IDPs verknüpft sind. Beispielsweise könnte

eine Person eine berufliche und eine private Identität definieren und dafür unterschiedliche IDPs verwenden. In jeder FIM-basierten Transaktion kommt jedoch nur genau ein IDP zum Einsatz.

2. Im Extremfall agiert jeder Benutzer als sein eigener IDP, indem er die entsprechende IDP-Softwarekomponente auf seiner eigenen Maschine betreibt. Diese Vorgehensweise wurde zuerst unter dem Namen *local wallet approach* diskutiert [OWNCTL, SSOTAX]; inzwischen hat sich daraus das in Abschnitt 2.1.3 diskutierte User Centric Identity Management entwickelt. Es ist zu bedenken, dass ein so betriebener IDP nicht ohne Weiteres als besonders zuverlässige Datenquelle einzustufen ist.

FIM-Ansätze werden als *zentralisiert* bezeichnet, wenn es nur einen IDP für alle Benutzer gibt, bzw. als *dezentralisiert*, wenn es mehrere IDPs geben kann. Bei einem dezentralisierten Ansatz ist ferner zu unterscheiden, ob ein Benutzer seinen IDP unter mehreren verfügbaren frei auswählen kann oder ob ihm ein IDP anhand vorgegebener Kriterien fest zugeordnet wird, wie es in B2B-Szenarien häufig der Fall ist.

- **Service Provider (SP)**: SPs bieten Dienste an, für deren Erbringung Informationen über den jeweiligen Benutzer erforderlich sind. Anbieter ausschließlich vollständig anonym nutzbarer Dienste erfordern kein FIM und werden an dieser Stelle zur Vereinfachung bewusst ausgeschlossen, obwohl sie im Allgemeinen durchaus auch als SPs bezeichnet werden können.

  Im FIM-Kontext werden die benötigten Informationen so weit wie möglich vom für den Benutzer zuständigen IDP und optional von den nachfolgend erläuterten Attribute Authorities bezogen; SPs werden deshalb manchmal auch als *identity data consumers* bezeichnet.

  Die Akzeptanz der über FIM bezogenen Daten hängt neben den Kriterien, die auch für eine lokale Datenakquisition gelten würden, zusätzlich vom Grad des Vertrauens in die jeweilige Datenquelle ab. Die elementaren Aspekte des Trust Managements in FIM werden in Abschnitt 2.1.2.5 erläutert.

  Wie zu verfahren ist, wenn nicht alle benötigten Daten über FIM akquiriert werden können, wird von der zur Verfügung stehenden Technik beeinflusst: Im primitivsten Fall schlägt die Dienstnutzung fehl; alternativ bestehen die beiden Möglichkeiten, dass der Benutzer die Daten entweder beim SP oder seinem IDP bzw. einer Attribute Authority nachträgt. Die FIM-protokollspezifischen Interaktionsmöglichkeiten werden in Kapitel 3 erläutert.

  Zur Erbringung eines Dienstes kann ein SP von anderen Diensten abhängig sein, die er entweder selbst anbietet oder die von externen SPs zur Verfügung gestellt werden. Wenn die eingesetzte FIM-Technik das Konzept der **Delegation** unterstützt, kann sich der SP gegenüber dem Anbieter des zusätzlich benötigten Dienstes als der eigentliche Benutzer ausgeben; in diesem Fall sind besondere Schutzmechanismen notwendig, die Missbrauch durch betrügerisches Auftreten („*Impersonation*“) verhindern.

- **Attribute Authority (AA)**: AAs können wie IDPs allgemeine Attributsauskünfte erteilen; sie werden benötigt, wenn Informationen über einen Benutzer auf mehrere Organisationen verteilt sind.

Der wesentliche technische Unterschied zu IDPs besteht darin, dass AAs nicht für die Authentifizierung von Benutzern eingesetzt werden. Darüber hinaus sind Benutzer in der Regel organisatorisch stärker an ihren IDP gebunden als an eine der für sie relevanten AAs. Obwohl es theoretisch möglich wäre, dass ein IDP nur für die Authentifizierung eingesetzt wird und der übrige Datenaustausch ausschließlich mit AAs erfolgt, ist diese Vorgehensweise derzeit praktisch irrelevant; dies ist insbesondere damit zu begründen, dass es häufig bereits aufwendig ist, den für einen Benutzer zuständigen IDP dynamisch zu ermitteln (siehe Abschnitt 2.1.2.7); eine Fragmentierung der Daten über mehrere AAs erhöht die Komplexität noch weiter.

Obwohl es aus dem Namen *Attribute* Authority nicht hervorgeht, kann eine AA prinzipiell auch Autorisierungsbestätigungen ausstellen (vgl. Abschnitt 2.1.2.2). Sofern bei den von einer Organisation übermittelten Daten eine klare Trennung zwischen Attributsauskünften und Autorisierungsbestätigungen vorliegt, wird im Rahmen dieser Arbeit deshalb der Begriff **Authorization Provider (AP)** verwendet.[1] Die Möglichkeit zur Verteilung von Autorisierungsentscheidungen auf weitere Organisationen neben IDP und SP hat jedoch aufgrund der damit verbundenen Komplexität und den Randbedingungen an die Verfügbarkeit der involvierten Systeme derzeit eine nur geringe praktische Bedeutung.

- **Trusted Third Party (TTP)**: TTPs bieten FIM-spezifische Dienste für AAs, IDPs und SPs, aber nicht für einzelne Benutzer an. Hierzu gehören beispielsweise:
  - Bestätigung oder Garantie der Echtheit und Korrektheit von Benutzerattributen.
  - Ermittlung des zu einem Benutzer gehörenden IDP bzw. relevanter AAs.
  - Verwaltung von Metadaten, beispielsweise Listen vertrauenswürdiger AAs, IDPs und SPs sowie deren Public Keys bzw. PKI-Zertifikate.
  - Hinterlegung personenbezogener Daten, die einem SP im Rahmen einer anonymen oder pseudonymen Transaktion bewusst vorenthalten werden, anhand derer im Missbrauchsfall jedoch dennoch der Verursacher ermittelt werden kann („*revocable anonymity*“) [TERMPR, REIDEN].

  Wie aus dem Namen *Trusted Third Party* bereits hervorgeht, handelt es sich dabei vorwiegend um sicherheitskritische Dienste, so dass eine geeignete Vertrauensbeziehung zwischen der TTP und deren Kunden gegeben sein muss (vgl. Abschnitt 2.1.2.5).

Diese Rollen schließen sich gegenseitig nicht aus; häufig sind Organisationen beispielsweise sowohl IDP als auch SP. Mit Ausnahme von AAs, die funktional eine Teilmenge von IDPs bereitstellen, sind jedoch je nach Rolle deutlich unterschiedliche FIM-Komponenten einzusetzen, die in die jeweilige IT-Infrastruktur integriert werden müssen.

2.1.2.4. Modellierung von Identitäten

Im Gegensatz zu I&AM-Systemen, die aufgrund ihres organisationsinternen Charakters jede *Person* nur genau einmal erfassen wollen, ist es in FIM-Szenarien mit potentiell globalem

[1] Die begrifflich näher an Attribute Authorities liegende Bezeichnung „Authorization Authority“ wird nicht verwendet, da extern eingeholte Autorisierungen nicht zwangsweise autoritativ für einen SP sein müssen.

Abdeckungsgrad durchaus erlaubt und unter Umständen aus Datenschutzgründen (vgl. Abschnitt 2.1.2.6) sogar erwünscht, dass eine Person mehrere Identitäten hat, die sie *unabhängig voneinander* einsetzen kann; wichtig ist dabei, dass jede *Identität* nur einmal und nicht mehrfach erfasst wird. Für die Modellierung dieses Sachverhalts gelten folgende Regeln:

- Jede reale Person existiert genau einmal und ist eine Entität vom Typ Person, die eineindeutig identifiziert werden kann.
- Für Identity Management relevante Personen werden in Form von **digitalen Identitäten** erfasst; jede erfasste Person hat somit mindestens eine Identität. Auf Basis der erfassten Daten *kann* es möglich sein, eindeutig auf die hinter einer Identität steckende reale Person zu schließen; dies ist, wie unten erläutert wird, im Rahmen von anonym oder pseudonym nutzbaren Diensten jedoch keine zwingende Voraussetzung.

  Es hat sich durchgesetzt, dass Identitäten objektorientiert modelliert werden, unabhängig davon, in welchen technischen Systemen (z. B. relationale Datenbanken, die keine Objektorientierung unterstützen) sie letztendlich gespeichert werden. Daten und Eigenschaften einer Identität werden deshalb in Form von **Attributen** erfasst:

  - Attribute sind Tupel, jeweils bestehend aus einem **Attributsnamen** und einer *ungeordneten* **Wertemenge**. Im Folgenden verwendete Beispiele für Attributsnamen sind `Erster_Vorname`, `Zweiter_Vorname` und `Telefonnummer`.
  - Die Wertemenge ist leer, wenn die Eigenschaft der Person nicht erfasst worden ist oder nicht zutrifft; beispielsweise ist die Wertemenge des Attributs `Zweiter_Vorname` bei Personen, die nur einen Vornamen haben, leer.
  - Attribute, deren Wertemenge nicht leer sein darf, um eine Identität anlegen zu können, werden als **mandatory** bezeichnet; die übrigen Attribute sind **optional**.
  - Ein Attribut oder eine Kombination aus Attributen, anhand derer eine Identität eindeutig innerhalb des betrachteten Datenbestands bestimmt werden kann, wird als *Schlüssel* bezeichnet. Jede Identität muss über einen Schlüssel verfügen; gegebenenfalls wird hierfür ein künstliches Schlüsselattribut, z. B. `Personalnummer`, eingeführt.
  - Attribute mit einelementiger Wertemenge werden als *single-value* Attribute bezeichnet; ein typisches Beispiel hierfür ist `Erster_Vorname`.
  - Attribute mit mehrelementiger Wertemenge sind so genannte *multi-valued* Attribute; ein Beispiel hierfür ist `Telefonnummer`, sofern für verschiedene Arten von Telefonnummern (z.B. dienstlich, privat, Festnetz, Mobiltelefon) keine dedizierten Attribute vorgesehen sind.

  Das somit verwendete Datenmodell ist *flach*, da innerhalb der Attribute keine weiteren Strukturierungsmöglichkeiten wie beispielsweise Hierarchien oder Relationen zur Verfügung stehen (engl. *flat name/value pairs*). Diese Vorgehensweise ist die in der Praxis am Weitesten verbreitete. Sie stößt jedoch aufgrund der Eigenschaft, dass die Wertemengen ungeordnet sind und somit keine deterministische Reihenfolge für den Abruf einzelner Werte existiert, schnell an ihre Grenzen; beispielsweise kann der attributsübergreifende semantische Zusammenhang mehrerer Werte für die Attribute `Postleitzahl` und `Ort`

```
Erster_Vorname = Max
Nachname       = Mustermann
Adresse        = {
 <Adressen>
  <Adresse Id=1>
   <Typ>Geschäftsadresse</Typ>
   <Strasse>Musterstraße 1</Strasse>
   <PLZ>12345</PLZ>
   <Ort>Musterhausen</Ort>
  </Adresse>
  <Adresse Id=2>
   <Typ>Privatadresse</Typ>
   ...
   </Adresse>
   ...
  </Adressen>
}
Telefonnummer  = {
  <Telefonnummern>
   <Telefonnummer Id=1>
    <Typ>geschäftlich</Typ>
    <Land>+49</Land>
    <Vorwahl>01234</Vorwahl>
    <Durchwahl>567-89012</Durchwahl>
   </Telefonnummer>
   ...
  </Telefonnummern>
}
```

Objektorientierte Modellierung, umgesetzt in XML

```
Erster_Vorname = Max
Nachname       = Mustermann

Adresse1.Typ     = Geschäftsadresse
Adresse1.Strasse = Musterstraße 1
Adresse1.PLZ     = 12345
Adresse1.Ort     = Musterhausen
Adresse2.Typ     = Privatadresse
Adresse2.Strasse = ...
Adresse2.PLZ     = ...
Adresse2.Ort     = ...

Telefonnummer1.Typ       = geschäftlich
Telefonnummer1.Land      = +49
Telefonnummer1.Vorwahl   = 01234
Telefonnummer1.Durchwahl = 567-89012
Telefonnummer2.Typ       = ...
...
```

„Flache“ Attributswerte mit Strukturierung der Attributsnamen

Abbildung 2.11.: Identitätsmodellierung: Strukturierung von Attributswerten bzw. -namen

nicht abgebildet werden: Die zur Korrelation notwendige Information, welche Postleitzahl zu welchem Ort gehört, geht verloren. Zur Umgehung dieser Beschränkung haben zwei Verfahren praktische Bedeutung erlangt, die in Abbildung 2.11 veranschaulicht werden:

1. In den Werten der Attribute werden strukturierte Daten abgelegt, beispielsweise in Form von XML-Dokumenten; diese müssen vom Empfänger der Daten geeignet interpretiert werden können.
2. Die Attributsnamen werden mit einer Semantik belegt, die eine hierarchische Strukturierung ermöglicht, beispielsweise `Adresse1.Ort`, `Adresse1.PLZ`, `Adresse2.Ort` und `Adresse2.PLZ`. Wie in diesem Beispiel bereits angedeutet wird, werden häufig Trennzeichen wie Punkte oder Schrägstriche verwendet, um die Attributsnamen zu segmentieren; zusammengehörende Attribute können dann anhand des längsten gemeinsamen aus ganzen Segmenten bestehenden Präfixes ermittelt werden.

Offensichtlich handelt es sich dabei um pragmatische Ansätze, die das zugrunde liegende Problem der flachen Zuordnung von Attributswerten zu -namen nicht lösen; aufgrund ihrer Verbreitung und der Verwendung in einigen der in Kapitel 3 diskutierten Standards müssen sie jedoch mindestens aus Kompatibilitätsgründen unterstützt werden.

Innerhalb eines FIM-basierten Datenaustauschvorgangs können bei allen existierenden

Ansätzen nur Daten von genau einer Identität der Person abgerufen werden. In der Regel ist die Vermischung verschiedener Identitäten unerwünscht; soll sie erzwungen werden, sind mehrere FIM-Transaktionen erforderlich.

- Jede Identität kann mehrere **Rollen** haben. Beispielsweise könnte die berufliche Identität einer Person die Rollen *Angestellter*, *Ersthelfer* und *Personalratsmitglied* haben.

  Rollen können parametrisiert werden, so dass zusätzliche Attribute zur Verfügung stehen, wenn eine Identität eine bestimmte Rolle innehat. Beispielsweise könnte bei der Rolle *Angestellter* der Name oder der Schlüssel derjenigen Abteilung, in der die Person tätig ist, festgehalten werden.

  Aus den verschiedenen Rollen können unterschiedliche Autorisierungen beim Service Provider abgeleitet werden. Prinzipiell können im Rahmen einer FIM-Transaktion mehrere Rollen miteinander kombiniert werden; hierbei liegt es jedoch im Verantwortungsbereich des SP, die Kombination einander gegenseitig ausschließender Rollen zu verhindern. Dieser Vorgang wird als *separation of duties* bezeichnet und wird anhand des einfachen, nicht FIM-spezifischen Beispiels klar, dass Antragsteller und Genehmiger eines Bankkredites nicht dieselbe Person sein dürfen [TM03, WEK05].

  Die Definition verschiedener Rollen stellt bei einigen Ansätzen eine Möglichkeit zur Bildung von Sub-Identitäten dar, d. h. der Benutzer muss sich vor der Nutzung eines Dienstes entscheiden, im Kontext welcher Rolle er agieren möchte. Die parallele Nutzung mehrerer Rollen unterliegt dann denselben Beschränkungen wie die Nutzung mehrerer Identitäten. Im Rahmen dieser Arbeit wird eine klare Trennung zwischen *separaten* Identitäten und *kombinierbaren* Rollen angestrebt.

In Abhängigkeit von Art und Umfang der einem SP zur Verfügung gestellten Identitäts- und Rollendaten sind unterschiedlich starke Rückschlüsse auf die reale Person möglich. Aufgrund des gemeinsamen Suffixes der nachfolgend erläuterten englischen Begriffe spricht man diesbezüglich von **Nymity Levels** [NYMITY, PESA]:

- **Anonymity**: Dem SP liegen nicht genügend Informationen vor, um die verschiedenen Transaktionen eines Benutzers miteinander korrelieren zu können. Dies setzt voraus, dass der Benutzer nicht von anderen Benutzern in einer ausreichend großen Benutzermenge, dem so genannten *Anonymity Set*, unterschieden werden kann [TERMPR].
- **Pseudonymity**: Der SP kann anhand der vorliegenden Informationen zwar nicht auf die reale Person schließen, aber die Transaktionen desselben Benutzers miteinander korrelieren. Es werden folgende Arten pseudonymer Dienstnutzung unterschieden [SECUPS]:
  - *Person pseudonyms*: Der Realname der Person wird durch ein Pseudonym substituiert, das in allen Transaktionen mit allen SPs verwendet wird.
  - *Relationship pseudonyms*: Der Benutzer wählt für jeden SP ein individuelles Pseudonym, das er für alle Transaktionen mit dem jeweiligen SP verwendet.
  - *Role pseudonyms*: Der Benutzer wählt für jede seiner Rollen ein eigenes Pseudonym, das er SP-übergreifend in der jeweiligen Rolle verwendet.
- **Veronymity**: Der Benutzer ist dem SP als reale Person bekannt und verwendet eine Identität, die ihm eindeutig zugeordnet werden kann.

Service Provider sind aus ökonomischen Gesichtspunkten meist daran interessiert, möglichst viele Informationen über ihre Benutzer in Erfahrung zu bringen und beispielsweise mit Data Mining Verfahren auszuwerten: Je detaillierter das über einen Benutzer erstellte Profil ist, desto gezieltere Angebote können gemacht werden. Aus diesem Grund spielt der Datenschutz bei FIM eine zentrale Rolle; die grundlegenden Aspekte werden in Abschnitt 2.1.2.6 erläutert.

2.1.2.5. Föderationsmodelle und FIM-spezifisches Trust Management

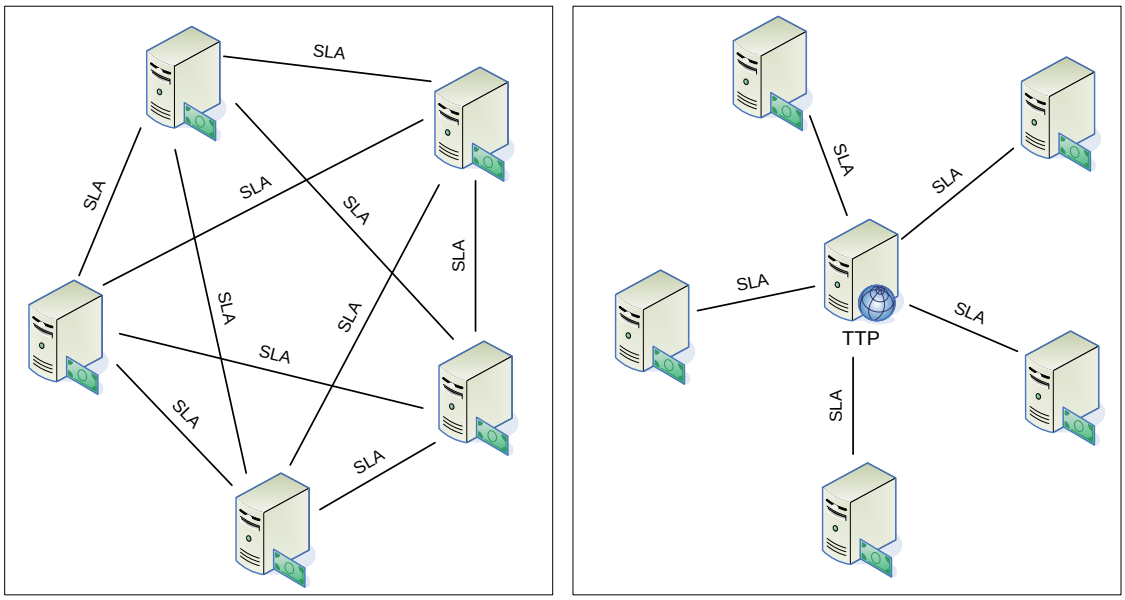
Der organisationübergreifende Austausch personenbezogener Daten setzt verschiedene Vertrauensbeziehungen voraus, die entweder a priori oder dynamisch bei Bedarf geschaffen werden müssen:

- SPs sind daran interessiert, Daten nur aus zuverlässigen Datenquellen zu beziehen, die über eine hohe Datenqualität verfügen. Konkret bedeutet dies, dass ein SP Daten nur von ausgewählten IDPs und AAs akzeptieren wird. Es muss also eine mindestens unidirektionale Vertrauensbeziehung vom SP zu diesen Datenquellen ausgehen.
- Komplementär dazu sind IDPs und AAs angehalten, Daten über Benutzer nur an zuverlässige SPs auszuhändigen. Insbesondere ist es hierzu notwendig, dass ein SP nachweisen kann, dass er auch wirklich derjenige ist, für den er sich ausgibt. Eine starke Authentifizierung des SP gegenüber einer Datenquelle ist somit Voraussetzung für eine mindestens unidirektionale Vertrauensbeziehung zum SP.
- Benutzer müssen ein besonderes Vertrauensverhältnis zu ihrem IDP haben, da sie diesem ihre Identitätsinformationen anvertrauen. Analoges gilt für AAs, die der Benutzer frei wählen kann. Andere AAs können dem Benutzer unbekannt sein bzw. setzen keine Vertrauensbeziehung voraus; hierzu gehören im E-Commerce-Umfeld beispielsweise *Scoring-Services*, die die Zahlungsfähigkeit einer Person auf Basis statistischer Daten über ihr soziales Umfeld abschätzen.
- Die meisten Benutzer haben Interesse daran, dass ihre personenbezogenen Daten nicht an unseriöse SPs herausgegeben werden. Vor der Datenübertragung muss also ein Vertrauensverhältnis vom Benutzer zum SP hergestellt worden sein.
- Trusted Third Parties (erläutert in Abschnitt 2.1.2.3) sind geeignet zu berücksichtigen.

Eine Menge von Organisationen, die zum Zweck des FIM-basierten Datenaustausches untereinander geeignete Vertrauensbeziehungen aufgebaut hat, wird als **Föderation** (engl. *identity federation*) bezeichnet.

Zur Formalisierung der Vertrauensbeziehungen können **Service Level Agreements** (SLAs) eingesetzt werden, die unter anderem die zu übermittelnden Daten sowie Bedingungen an deren Qualität und Verfügbarkeit spezifizieren. SLAs werden derzeit typischerweise in einer dedizierten Verhandlungsphase zeitlich deutlich vor der Dienstnutzung abgeschlossen, so dass zwei Organisationen, die bislang noch keine Berührungspunkte hatten, nicht ohne Weiteres über FIM Daten miteinander austauschen können.

Im primitivsten, als **Circle of Trust** bezeichneten Fall schließen alle Föderationsteilnehmer untereinander bilaterale SLAs ab. Diese Vorgehensweise skaliert aufgrund des damit verbundenen hohen Initial- und Pflegeaufwands ($\frac{n \cdot (n-1)}{2} = O(n^2)$ SLAs bei n Organisationen) bei



Föderation mit fünf Teilnehmern als *Circle of Trust*

Föderation mit fünf Teilnehmern mittels *brokered trust*

Abbildung 2.12.: SLA-basiertes Trust Management in einfachen Föderationsmodellen

größeren Föderationen nicht ausreichend. Deshalb haben sich einige effizientere Föderationsmodelle gebildet, die in Abschnitt 3.2.2.3 näher vorgestellt werden. Die derzeit in der Praxis höchste Relevanz hat die Realisierungsvariante über einen Trusted Third Party Service, die als **brokered trust** bezeichnet wird. Dabei schließt jede Organisation ein SLA mit der TTP ab und vertraut jeder anderen Organisation, die mit der TTP einen analogen Vertrag abgeschlossen hat; der Aufwand für das SLA-Management reduziert sich damit auf $O(n)$. Abbildung 2.12 stellt beide Varianten graphisch dar.

Protokolle, die eine Vereinbarung von Vertrauensbeziehungen zwischen einander bislang fremden Organisationen dynamisch bei Bedarf aushandeln, werden im Bereich des Trust & Reputation Managements entwickelt, haben jedoch im FIM-Umfeld noch keine praktische Bedeutung erlangt.

Im Rahmen dieser Arbeit wird deshalb davon ausgegangen, dass zwischen jeweils zwei Entitäten (Personen, Maschinen, Diensten oder Organisationen) A und B eine Menge von ganzzahligen **Trust Levels** $t_{AB_i} \in [-10;\ 10]$ mit $i \in I$ definiert ist, wobei I die Menge aller mittels FIM übertragbarer Datentypen ist, d. h. beispielsweise Authentifizierungs- und Autorisierungsbestätigungen sowie beliebige Subkategorien von allgemeinen Attributsauskünften umfasst. Ein positiver Trust Level reflektiert vorhandenes Vertrauen, ein negativer entsprechend vorhandenes Misstrauen. Über Schwellwertverfahren kann somit beispielsweise definiert werden, dass ein SP bestimmte Daten von einem IDP nur dann akzeptiert, wenn der entsprechende Trust Level einen Mindestwert erreicht. Durch die Unterscheidung verschiedener Datentypen wird erreicht, dass beispielsweise einem IDP hinsichtlich seiner Authentifizierungsbestätigungen vollkommen vertraut wird, die Qualität der von ihm gelieferten Adressinformationen jedoch angezweifelt wird. Nicht explizit gesetzte Trust Levels werden mit einer Voreinstellung initia-

lisiert, die bei konservativen Konfigurationen ≤ 0 ist.

Trust Levels können auch zwischen Personen und Organisationen definiert werden: Ob ein Dienst überhaupt benutzt wird und welche personenbezogenen Daten preisgegeben werden, hängt vom Grad des Vertrauens der Person in den Dienst bzw. SP ab. Andererseits kann das Vertrauen des Dienstes in eine Person im Laufe der Zeit steigen oder fallen, falls beispielsweise alle Transaktionen problemlos abgewickelt werden konnten oder der Benutzer wegen Verzögerungen im Zahlungsverkehr in Verruf gerät.

2.1.2.6. Datenschutz in FIM

Für SPs gelten im FIM-Umfeld in Bezug auf den Datenschutz im Wesentlichen dieselben Bedingungen wie bei I&AM-Systemen (siehe Abschnitt 2.1.1.6). Da die Akquisition von Daten durch FIM-Techniken automatisiert werden kann, sind besondere Maßnahmen notwendig, um den Benutzer vorab über die Erfassung seiner Daten zu informieren und falls notwendig sein Einverständnis einzuholen. Insbesondere sind auch Situationen zu betrachten, in denen personenbezogene Daten im Rahmen von Delegation an Dritte weitergegeben werden.

IDPs und AAs haben die Aufgabe, personenbezogene Daten an Dritte weiter zu geben; die Komplexität wird dadurch erhöht, dass die Datenempfänger je nach Dynamik der Föderation zum Zeitpunkt der Datenerfassung noch nicht bekannt sein können. Es müssen deshalb Mechanismen geschaffen werden, über die der Benutzer z. B. seinem IDP explizit erst bei Bedarf erlauben kann, bestimmte auf ihn bezogene Daten an einen SP zu übermitteln.

Damit verbunden ist auch, dass IDPs und AAs zwangsweise wissen, welche SPs welche Daten über welche Benutzer anfordern, gegebenenfalls auch, zu welchem Zweck diese Datenerfassung erfolgt. Die Speicherung und Auswertung auf diese Weise anfallender Informationen muss deshalb streng reglementiert werden.

Benutzer lassen sich anhand ihres subjektiven Schutzbedürfnisses in verschiedene Kategorien einteilen; dabei hat sich die folgende Vierteilung bewährt [PRIVEC]:

- Personen, die keinen Wert auf den Umgang mit ihren personenbezogenen Daten legen, werden als **not concerned** bezeichnet; diese Einstellung ist meist auf mangelndes Wissen über Missbrauchsmöglichkeiten und den Wert der eigenen Identitätsdaten für viele Dienstleister zurückzuführen.

- Das genaue Gegenteil der vorstehend genannten Kategorie sind Personen, die möglichst wenige Informationen über sich preisgeben wollen und aus der Befürchtung heraus, dass ihre Daten missbraucht werden könnten, auf die Nutzung entsprechender Dienste verzichten. Diese Gruppe wird häufig **privacy fundamentalists** genannt.

  Zwischen diesen beiden Extremen liegen diejenigen Benutzer, die bewusst und zielgerichtet mit ihren personenbezogenen Daten umgehen; in der Praxis kristallisieren sich dabei die beiden folgenden besonderen Benutzergruppen heraus (vgl. Datenkategorien Identitäts- und Profildaten in Abschnitt 2.1.2.2):

- Als **identity concerned** werden Personen bezeichnet, die zwar zum Zweck der Personalisierung – beispielsweise in Form von gezielten Produktempfehlungen – Informationen über ihre persönlichen Präferenzen an SPs übermitteln, jedoch darauf bedacht sind,

möglichst keine Informationen preiszugeben, anhand derer sie als reale Person eindeutig identifiziert werden können.

- Als **profile averse** gelten hingegen Personen, die zwar häufig unter ihrem Realnamen agieren, um beispielsweise an Internet-Gewinnspielen teilnehmen zu können, jedoch möglichst darum bemüht sind, keine profilbezogenen Angaben zu Hobbies, bevorzugten Herstellern und Marken et cetera zu machen.

In der Regel ist es unerwünscht, dass mehrere Service Provider ihre über eine Person gespeicherten Daten untereinander austauschen oder kombinieren. Eine technische Möglichkeit hierzu wäre, dass pro SP ein eigenes Pseudonym verwendet wird (vgl. Relationship Pseudonyms in Abschnitt 2.1.2.4). In der Praxis scheitert dieser Ansatz sehr häufig daran, dass den SPs Schlüsselattribute wie Kreditkartennummern vorgelegt werden, anhand derer die Profile trivial SP-übergreifend korreliert werden können [QUALIN]. Da das zugrundeliegende Problem prinzipbedingt praktisch nicht vermieden werden kann, werden technische Maßnahmen und Hilfsmittel benötigt, die die Umsetzung und Einhaltung diesbezüglicher legislativer Auflagen kontrollieren und sicherstellen können.

Die **zentrale Fragestellung** bezüglich Datenschutz im FIM-Umfeld ist deshalb,

- welche IDPs, AAs (und SPs im Rahmen von Delegation)
- welche personenbezogenen Daten aus welchen Benutzeridentitäten
- an welche SPs bzw. welche Dienste
- wie und in welcher Form (z. B. nur einmalig, nur verschlüsselt)
- unter welchen Bedingungen (z. B. Einverständnis des Benutzers mit dem Datenverarbeitungszweck)
- unter welchen Auflagen (z. B. Löschen beim Empfänger nach Gebrauch)

übermitteln dürfen. Die Ausprägungen dieser Aspekte und ihre Umsetzung durch formal spezifizierte, automatisiert auswertbare Policies werden in Abschnitt 5.3 behandelt.

Je nach Szenario können weitere Anforderungen hinzukommen; beispielsweise muss in B2B-Szenarien verhindert werden, dass externe Dienstleister vertrauliche firmeninterne Benutzerprofildaten abrufen können, auch wenn der Benutzer selbst diese Daten z. B. aus Unkenntnis nicht zurückhalten möchte. Ebenso ist denkbar, dass bereits früher vereinbarte Freigaberegelungen zum Zug kommen, obwohl der Benutzer in einem aktuellen Fall die betroffenen Daten nicht explizit freigegeben hat.

Es ist zu bedenken, dass die Schaffung der technischen Möglichkeiten zur Umsetzung dieser Datenschutzaspekte und die Bereitstellung intuitiv bedienbarer Benutzeroberflächen ausschlaggebend für die breite Akzeptanz jeglicher FIM-Ansätze sein wird. Die Defizite existierender FIM-Lösungen auf diesem Sektor, die in Kapitel 3 diskutiert werden, waren die maßgeblichen Auslöser für das Entstehen des in Abschnitt 2.1.3 beschriebenen User-Centric Identity Managements.

2.1.2.7. Grundlegende FIM-Workflows

Nachfolgend wird ein Überblick über die grundlegenden Abläufe und Datenflüsse beim Einsatz von FIM anhand eines IDPs und eines SPs gegeben. Die Details der Workflows und die

Inhalte der ausgetauschten Nachrichten sind von der zum Einsatz kommenden FIM-Technik abhängig und werden in Kapitel 3 erläutert. Da der Schwerpunkt von FIM-Anwendungen derzeit bei webbasierten Diensten liegt, wird im Folgenden davon ausgegangen, dass der Benutzer mit einem herkömmlichen Webbrowser arbeitet und eine über das Internet zugängliche Webapplikation nutzen möchte.

Aus Benutzersicht ist zu unterscheiden, ob der Dienst genutzt werden soll, *bevor* oder *nachdem* eine Authentifizierung beim IDP durchgeführt wurde; diese Differenzierung ist bei den meisten derzeit verfügbaren FIM-Techniken auch technisch essentiell. Im Folgenden werden beide Varianten beschrieben:

1. Der Benutzer authentifiziert sich zuerst bei seinem IDP („***IDP first* Use Case**“), bevor er den Dienst eines externen SPs nutzen möchte. Diese Authentifizierung kann beispielsweise durch den Login an einer Workstation des IDP erfolgen oder durch Anmeldung an einem Internet- oder Intranet-Webportal des IDP. Dabei wird festgehalten, wie sich der Benutzer authentifiziert hat, beispielsweise durch Wissen (z.B. Passwort), Besitz (z.B. Smartcard), Eigenschaften (z.B. biometrische Verfahren) oder eine Kombination aus mehreren dieser Verfahren (z.B. Smartcard mit Eingabe einer PIN).

   Nach erfolgreicher Authentifizierung bekommt der Benutzer vom IDP eine Liste über FIM nutzbarer Dienste zur Auswahl angeboten; eine charakteristische Einschränkung dieser Variante ist folglich, dass die möglichen SPs a priori bekannt und IDP-seitig vorkonfiguriert sein müssen, wodurch die Dynamik und die Skalierbarkeit eingeschränkt werden. Möchte der Benutzer den Dienst eines anderen SPs benutzen, muss wie im unten aufgeführten „*SP first* Use Case“ verfahren werden.

   Da die Dienstnutzung über Webbrowser erfolgt, besteht die Dienstauswahlliste im Allgemeinen aus HTML-Links, die auf den jeweiligen Dienst verweisen. Dieses Verfahren kann dazu genutzt werden, an den SP zusätzlich beliebige Parameter zu übergeben, indem sie in die vom Webbrowser des Benutzers abgerufene Adresse des Dienstes (URL) geeignet integriert werden. Damit ist es, wie in Abbildung 2.13 dargestellt wird, möglich, dem SP beim Aufruf des Dienstes mitzuteilen, um welchen Benutzer es sich handelt und zu welchem IDP er gehört.

   Diese Information kann vom SP auf zwei verschiedene Arten ausgewertet werden:

   a) Der SP kontaktiert den IDP, um eine Authentifizierungsbestätigung für den Benutzer zu erhalten, damit sichergestellt werden kann, dass sich kein Angreifer in betrügerischer Absicht für den eigentlichen Benutzer ausgibt. In diesem Fall sind Metadaten erforderlich, anhand derer der SP mit dem dafür zuständigen System seitens des IDP Kontakt aufnehmen kann, beispielsweise dessen IP-Adresse. Aus offensichtlichen Sicherheitsgründen würde es nicht ausreichen, diese Metadaten beim Dienstaufruf im Klartext zu übergeben, da ihre Fälschungssicherheit gewährleistet werden muss; vielmehr müssten sie bereits a priori beim SP hinterlegt worden sein, oder es muss ein entsprechender TTP-Service genutzt werden.
   b) Die im Dienstaufruf übergebenen Parameter werden vom IDP digital signiert, so dass sie nicht vom Benutzer oder im Rahmen eines Man-in-the-Middle-Angriffs verfälscht werden können. Aus Sicherheitsgründen müssen die übergebenen Daten zudem mit einem Zeitstempel und einer begrenzten Gültigkeitsdauer versehen

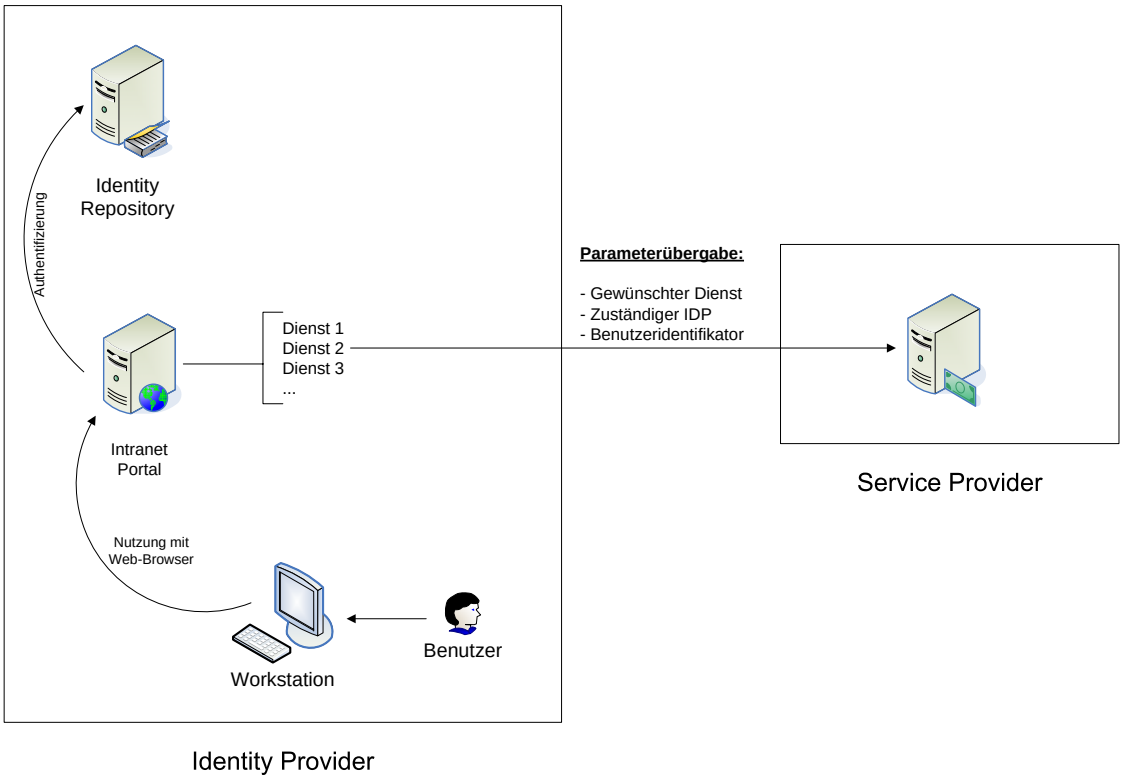


Abbildung 2.13.: Übergabe der Basisinformationen an den SP beim *IDP first* Use Case

werden, um eine spätere Wiedervorlage dieser Parameter durch einen Angreifer (*Replay Attack*) zu verhindern. Zur Überprüfung der Signatur ist es notwendig, dass dem SP das Zertifikat des IDPs bereits vorliegt oder dieses z. B. durch die Integration in eine gemeinsame PKI zur Laufzeit bezogen werden kann.

Obwohl diese Kommunikation bilateral abläuft und keinen direkten Bezug zu einer organisatorischen Gruppierung von IDP und SP zu einer Föderation impliziert, kann die Verwaltung der jeweils benötigten Metadaten nur im Rahmen einer Föderation effizient gestaltet werden.

Im Rahmen der Authentifizierungsbestätigung wird dem SP das vom IDP eingesetzte Authentifizierungsverfahren mitgeteilt. Der SP muss entscheiden, ob er dieses Verfahren anerkennt oder ob für die Nutzung seines Dienstes eine stärkere Authentifizierung erforderlich ist; beispielsweise könnte der SP eine Authentifizierung über Smartcard verlangen, so dass ein einfaches Passwortverfahren nicht ausreicht. Je nach eingesetzter FIM-Technik kann der SP eine **Re-Authentifizierung** durch den IDP verlangen oder muss diese selbst durchführen (vgl. Kapitel 3).

Im einfachsten Fall ist die Sicherstellung der Identität des Benutzers durch eine Authentifizierungsbestätigung ausreichend, um die Dienstnutzung zur ermöglichen. Gegebenenfalls können im Vorfeld der Dienstnutzung noch Autorisierungsbestätigungen und allgemeine Attributsauskünfte angefordert werden; die dazu notwendige Kommunikati-

on zwischen SP und IDP verläuft analog zur Authentifizierungsbestätigung.

Alle derzeitigen FIM-Ansätze sehen vor, dass eine Abfrage von Identitätsdaten nicht nur im Vorfeld, sondern auch während der Dienstnutzung erfolgen kann. Da die Nutzung webbasierter Dienste aufgrund der Eigenschaft des HTTP-Protokolls, zustandslos zu sein, in der Regel an so genannte Sessions gebunden ist, die eine beschränkte Gültigkeitsdauer haben (*Session Lifetime*), kann es jedoch zu Komplikationen kommen, wenn die Gültigkeitsdauer der Session beim SP länger ist als beim IDP; bei einer erneuten Anfrage durch den SP kann dann eine erneute Authentifizierung des Benutzers beim IDP erforderlich werden.

Die FIM-Ansätze unterscheiden sich jedoch in Bezug auf die Abfrage von Daten nach Beendigung der Dienstnutzung; bei den meisten FIM-Protokollen ist es erforderlich, dass erst später, beispielsweise zur Abrechnung, erforderliche Daten bereits während der Dienstnutzung abgerufen werden, da danach kein Zugriff auf diese Informationen mehr möglich ist.

Weiterhin ist bei den meisten FIM-Protokollen nicht vorgesehen, dass Änderungen an den abgerufenen Daten an die davon betroffenen SPs propagiert werden, so dass es zu temporären Inkonsistenzen kommen kann, die erst bei der nächsten Dienstnutzung beseitigt werden können.

Eine ähnliche Bedeutung wie dem durch Authentifizierungsbestätigungen erreichten Single Sign-On (SSO) kommt dem so genannten **Single Logout (SLO)** zu, mit dem erreicht werden soll, dass der Benutzer bei allen Diensten, die er gerade benutzt, durch eine einzige Interaktion, z. B. das Betätigen einer Schaltfläche im Webbrowser oder das Ausschalten seines Computers, abgemeldet wird. Dies wird zum einen bei nach Dauer der Nutzung abgerechneten Diensten benötigt, andererseits stellt es eine prophylaktische Sicherheitsmaßnahme da, um Missbrauch durch eine andere Person, die nachfolgend denselben Rechner verwendet, vorzubeugen. SLO ist analog zu SSO keine zwingende technische Notwendigkeit, sondern stellt eine Erhöhung der Benutzerfreundlichkeit und Sicherheit dar, da sich der Benutzer nicht mehr bei jedem Dienst einzeln abmelden muss. Wie in Kapitel 3 gezeigt wird, ist bei SLO zwischen einer Initiierung des Prozesses durch den IDP bzw. einen der SPs zu differenzieren; da eine bilaterale Kommunikation hierfür nicht ausreicht und die Datenflüsse sowie die technischen Anforderungen an den IDP komplexer sind als beim SSO, wird SLO derzeit noch von nur wenigen FIM-Protokollen unterstützt.

2. Die Situation, dass ein Benutzer den Dienst eines SPs benutzen möchte, noch bevor er sich bei seinem IDP authentifiziert hat, wird als „***Service Provider first* Use Case**“ bezeichnet. Um FIM-basierte Funktionen wie organisationsübergreifendes Single Sign-On und allgemeine Attributsauskünfte nutzen zu können, muss sich der Benutzer jedoch zwangsweise vorher bei seinem IDP anmelden.

   Der Unterschied zum *IDP first* Use Case liegt deshalb primär darin, dass der Benutzer vom SP möglichst transparent zu seinem IDP umgeleitet, dort authentifiziert und dann wiederum vom IDP zurück zum SP umgeleitet werden muss. Die Umleitung zwischen verschiedenen Webseiten kann durch die Redirect-Funktionalität des HTTP-Protokolls automatisiert werden, so dass sie für den Benutzer mit keinem manuellen Zusatzaufwand, aber unter Umständen spürbaren Verzögerungen verbunden ist.

Ein unscheinbares, aber technisch nicht triviales Problem ist die Ermittlung des für einen Benutzer zuständigen IDPs (**IDP Selection**). Wie in Kapitel 3 gezeigt wird, gibt es für diese Aufgabe noch keine standardisierte Lösung:

- Einfache FIM-Spezifikationen und deren Implementierungen erfordern, dass der Benutzer seinen IDP manuell beim SP spezifiziert, indem er beispielsweise dessen URL in einem Eingabefeld angibt.
- Die deutlich komplexeren, industriell standardisierten FIM-Protokolle empfehlen die Verwendung eines Trusted Third Party Services, bei dem der Benutzer aus einer Liste von IDPs auswählen kann, zu denen der SP eine entsprechende Vertrauensbeziehung aufgebaut hat.

  Eine Vorreiterrolle hat hierbei der im Rahmen von Shibboleth (vgl. Abschnitt 3.3.1) implementierte **WAYF-Service** („Where Are You From?“) gespielt. Der Benutzer wird dabei also nicht direkt zum IDP umgeleitet, sondern zuerst zum WAYF-Service. Da sowohl WAYF als auch IDP wissen müssen, zu welchem SP und Dienst der Benutzer nach erfolgreicher Authentifizierung zurück umgeleitet werden muss, ergeben sich aufwendigere Datenflüsse und zusätzliche datenschutzrechtliche Aspekte. Der prinzipielle Ablauf ist in Abbildung 2.14 dargestellt.
- Eine Alternative zur manuellen Angabe oder Auswahl des zuständigen IDPs besteht darin, diesen zum Beispiel aus der IP-Adresse oder dem DNS-Namen des vom Benutzer verwendeten Rechners abzuleiten. Abbildung 2.15 zeigt ein entsprechendes Beispiel. Hierzu sind passende Metadaten notwendig, die in der Regel nur im Rahmen einer formal definierten Föderation verfügbar sind; darüber hinaus entfallen mit diesem Verfahren die Möglichkeiten zur freien Wahl des IDP bzw. zur Verwendung mehrerer verschiedener IDPs.

Häufig wird das zu verwendende IDP Selection Verfahren von der Föderation vorgegeben, sofern das eingesetzte FIM-Protokoll mehrere Varianten unterstützt. Offensichtlich kann es zu Konflikten kommen, wenn ein SP an mehreren Föderationen mit unterschiedlichen Anforderungen teilnehmen möchte; diese können derzeit nur durch das Anbieten einer eigenen Dienstinstanz pro Föderation gelöst werden.

Die Kommunikation zwischen SP und IDP kann in folgenden Varianten erfolgen:

- **Request-Response-Verfahren**: Der SP stellt Anfragen z. B. nach allgemeinen Attributsauskünften, die der IDP beantwortet. Dabei sind je nach FIM-Protokoll zwei verschiedene Übertragungswege möglich:

  1. Der SP nimmt direkten Kontakt mit dem IDP auf, beispielsweise in Form einer TCP/IP-Verbindung, übermittelt seine Anfrage und erhält die Antwort über dieselbe Verbindung.
  2. Die Anfragen und Antworten werden mittelbar über den Client des Benutzers zwischen SP und IDP ausgetauscht. In diesem Fall werden wiederum HTTP-Redirects eingesetzt und die zu übertragenden Daten in URLs eingebettet; um zu verhindern, dass der Benutzer die ausgetauschten Nachrichten lesen oder modifizieren kann, müssen geeignete kryptographische Maßnahmen wie Verschlüsselung eingesetzt werden.

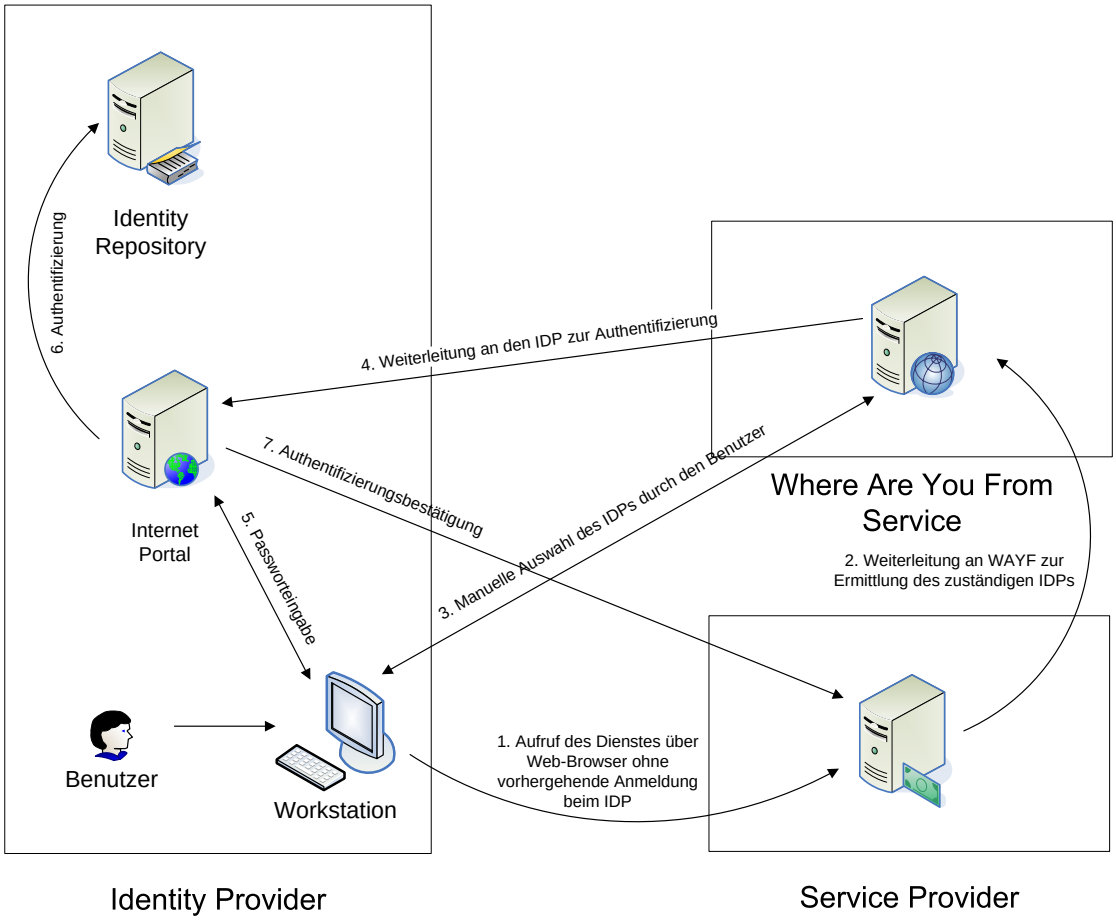


Abbildung 2.14.: Use Case *Service Provider first* unter Einsatz des *Where Are You From?* Services

Beide Varianten werden in Kapitel 3 näher beschrieben.

- **Push-Verfahren**: Die Daten werden dem SP beim Aufruf des Dienstes mitgeliefert, nachdem sich der Benutzer erfolgreich bei seinem IDP angemeldet hat. Dieses Verfahren setzt voraus, dass a priori bekannt ist, welche Daten der SP benötigt, spart jedoch einen Request-Response-Zyklus und resultiert somit in besserer Performanz, wenn insgesamt nur wenige Anfragen vom SP über den Benutzer gestellt werden.

Die optionale Kommunikation zwischen SP und AA erfolgt analog zur Kommunikation mit dem IDP über das Request-Response-Verfahren. Für die Ermittlung der für einen Benutzer zuständigen AAs können die folgenden Verfahren eingesetzt werden:

- Es wird ein Auswahl- bzw. Eingabeverfahren oder eine Heuristik wie bei der IDP Selection angewandt.
- Die relevanten AAs sind in Form von Attributen im Profil des Benutzers beim IDP hinterlegt.

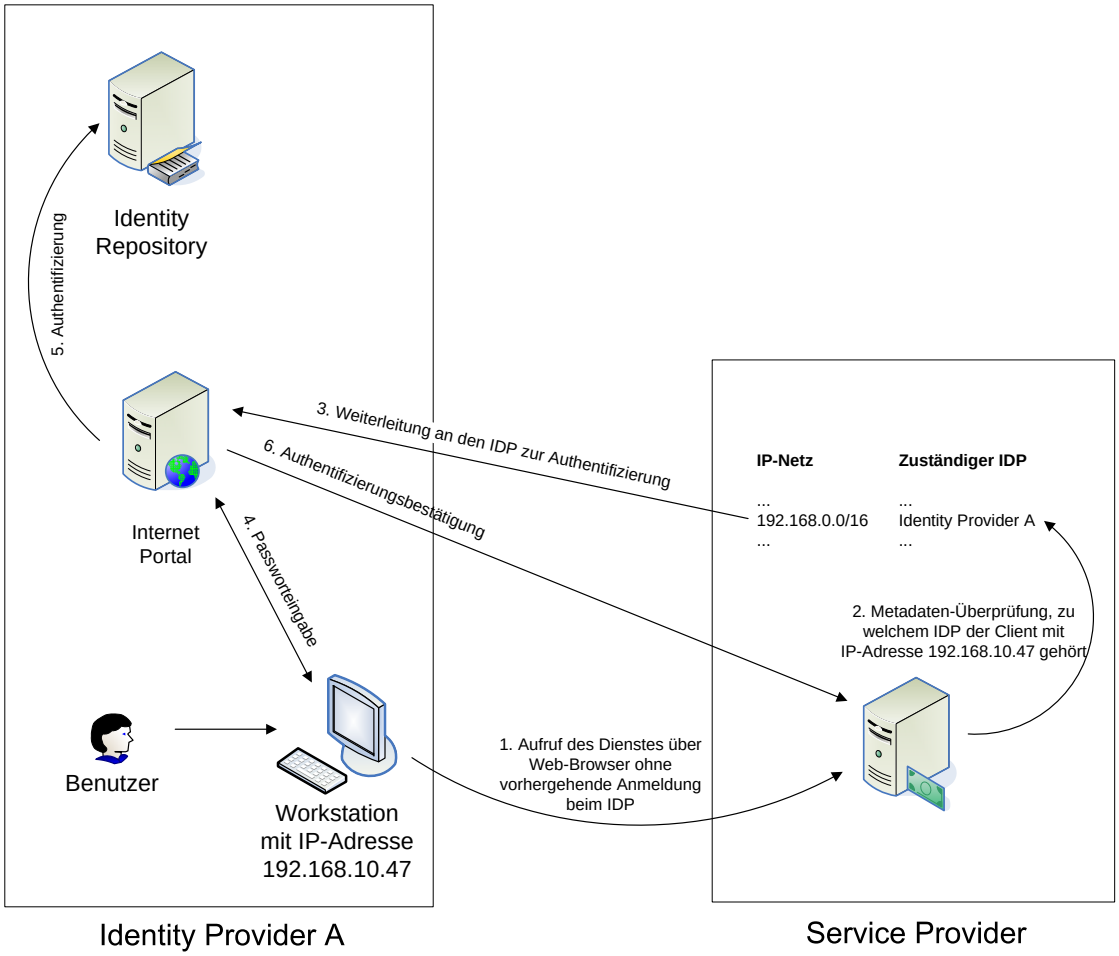


Abbildung 2.15.: Beispiel für die Ableitung des zuständigen IDPs aus der IP-Adresse des Clients

- Die zu verwendenden AAs sind beim SP fest vorkonfiguriert; dies ist der in der Praxis derzeit häufigste Fall.

- Es wird ein Broker bzw. eine Registry in Form eines TTP Services verwendet; da der Benutzer bereits authentifiziert und damit eindeutig identifiziert wurde, ist keine Interaktion erforderlich.

Die Datenübermittlung an den SP kann je nach FIM-Protokoll optional durch Rückfragen beim Benutzer unterbrochen werden, in denen dieser der Übertragung der Daten zustimmen muss. Details hierzu werden bei der Beschreibung der existierenden FIM-Ansätze in Abschnitt 3.5 erläutert.

2.1.2.8. Existierende FIM Deployments

Der Bedarf an organisationsübergreifendem Identity Management hat in der Vergangenheit zu verschiedenen Datenaustauschverfahren geführt, die vorrangig auf einer direkten Kopplung zwischen den Identity Repositories der beteiligten Organisationen, z. B. mittels Konnektoren, basierten. Dieser Lösungsansatz zeichnet sich durch einen hohen Implementierungsaufwand und begrenzte Skalierbarkeit aus und wirft zahlreiche Fragen in den Bereichen Security und Datenschutz auf.

Unter dem Begriff *Federated* Identity Management werden deshalb im engeren Sinn nur diejenigen Lösungen geführt, deren Datenflüsse analog zur Beschreibung im vorhergehenden Abschnitt gestaltet werden, bei denen also insbesondere keine pauschale Synchronisation von Identity Repositories erfolgt, sondern lediglich die wirklich benötigten Daten ausgetauscht werden.

Da alle FIM-Ansätze noch relativ neu und zum Teil noch unausgereift sind, existieren derzeit nur wenige Implementierungen, deren Installation und Konfiguration mit einem vergleichsweise hohen Aufwand verbunden sind, so dass FIM bei Weitem noch nicht überall dort im Einsatz ist, wo es benötigt wird oder Behelfslösungen sinnvoll ablösen könnte.

Um zu zeigen, dass FIM auf Basis der vorgestellten Konzepte und der in Kapitel 3 diskutierten Verfahren aber durchaus schon praktisch eingesetzt werden kann, wird nachfolgend ein sehr knapper Überblick über real existierende Einsatzgebiete gegeben:

Microsoft Passport (vgl. Abschnitt 3.2.3) Microsoft Passport kann retrospektiv als einer der ersten FIM-Ansätze mit großer Verbreitung bezeichnet werden. Dabei tritt Microsoft als einziger, zentraler IDP auf, der E-Commerce-spezifische Daten über die Benutzer erfasst, beispielsweise Anschrift und Kreditkartendaten. Von Service Providern wurde der Ansatz jedoch nur sehr zögerlich angenommen, da der kostenpflichtige Abruf der Benutzerdaten von einem einzigen IDP, der somit die Kunden des SP kennt, wirtschaftlich unattraktiv war. Datenschutzbedenken und das Bekanntwerden von Sicherheitslücken in der Implementierung haben den Kundenkreis klein gehalten. Passport ist aus diesem Grund fast nur noch im Rahmen des Microsoft Networks (MSN), zu dem populäre Webdienstleister wie Hotmail gehören, im Einsatz.

Liberty Alliance (vgl. Abschnitt 3.2.2) Die Liberty Alliance wurde ursprünglich als Gegenpol zu Microsoft Passport ins Leben gerufen und verfolgt seither einen dezentralisierten FIM-Ansatz. Erhebungen zeigen, dass die entwickelten Verfahren primär bei den an der Liberty Alliance beteiligten Organisationen im Einsatz sind [IMSURV], z. B.:

- General Motors, American Express und Sun bilden eine Föderation, um Mitarbeiterdaten im Rahmen von Outsourcingdiensten gemeinsam nutzen zu können.
- AOL und die France Telecom ermöglichen allen Breitband- und Mobilkunden die Nutzung gemeinsamer Dienste, zu der u. a. ein Micropayment-Provider mit 10 Millionen Kunden gehört.

Shibboleth (vgl. Abschnitt 3.3.1) Shibboleth ist ein Open Source Ansatz aus dem Umfeld von Hochschuleinrichtungen mit starken Parallelen zur Liberty Alliance. Shibboleth-Föderationen werden inzwischen von vielen National Research and Education Networks

(NRENs) betrieben, beispielsweise in den USA (Internet2), Australien (Projekt MAMS), Skandinavien, der Schweiz (SWITCH-AAI) und seit 2007 in Deutschland (DFN-AAI).

Hierbei wird primär ein organisationsübergreifender Zugang zu Bibliotheksbeständen realisiert, der aufgrund der Vielzahl unterschiedlichster Verträge zwischen Bibliotheken und Verlagen eine komplexe verteilte Autorisierungsinfrastruktur voraussetzt. Mit zunehmender Verbreitung von E-Learning-Systemen und der beginnenden systematischen Bereitstellung entsprechender Inhalte ist zu erwarten, dass auch diese Systeme bald in Shibboleth-Infrastrukturen integriert werden.

Eine vertiefende Betrachtung der Technik und der daraus resultierenden Anforderungen erfolgt in den Szenarien 3–5 in Abschnitt 2.2.

2.1.3. User Centric Identity Management

In diesem Abschnitt wird mit User Centric Identity Management (UCIM) die derzeit jüngste Identity Management Disziplin vorgestellt; da Unzulänglichkeiten existierender FIM-Ansätze maßgeblich zu ihrer Entwicklung beigetragen haben, können ausgewählte Anforderungen aus dem UCIM-Umfeld auf FIM übertragen werden.

Nach einer kurzen Zusammenfassung der historischen Entwicklung von UCIM und einer Betrachtung der Interoperabilität mit FIM werden die UCIM-spezifischen Datenschutzaspekte und Workflows erläutert. Szenario 2 illustriert den praktischen Einsatz von UCIM und dient der Ableitung entsprechend abstrahierter Anforderungen an FIM-Komponenten.

2.1.3.1. Historische Entwicklung von UCIM

UCIM ist die Konvergenz zweier ursprünglich voneinander unabhängiger Entwicklungen:

1. Mit der zunehmenden Anzahl von Dienstleistern im Internet stieg auch die Anzahl individuell zu merkender Benutzername-/Passwort-Kombinationen und mit den fast immer gleichen Daten auszufüllender Webformulare.

   Um den Benutzern die Verwaltung dieser vielen einzelnen Identitäten zu erleichtern, kamen zuerst so genannte **Passwort-Management-Tools** auf den Markt, mit denen Benutzer ihre verschiedenen Passwörter lokal speichern und ggf. durch ein einziges *Master Password* schützen können. Diese Funktionalität ist heute bereits in vielen Webbrowsern integriert.

   Eine Erweiterung des reinen Passwort-Managements stellte die Möglichkeit dar, mit ähnlichen Werkzeugen auch die auf Webseiten häufig einzugebenden Informationen wie Name, Anschrift und Abrechnungsdaten verwalten zu können. Durch Metadaten im HTML-Quelltext der Webformulare kann maschinenlesbar angegeben werden, welche Daten in welche Felder des Formulars einzutragen sind; entsprechende Hilfsmittel können dem Benutzer dann beim Ausfüllen des Formulars assistieren oder das Ausfüllen sogar komplett automatisieren.

   Fortgeschrittene Varianten dieser Werkzeuge führen ein Protokoll, welche Daten so an welchen Dienstleister übermittelt wurden und können dem Benutzer auf dieser Basis eine Übersicht seiner Webidentitäten präsentieren.

2. Parallel zu den Bemühungen der Liberty Alliance (vgl. Abschnitt 3.2.2), technische und organisatorische Maßnahmen zum Einsatz mehrerer dezentraler IDPs im FIM-Bereich zu standardisieren, hat sich im wissenschaftlichen Umfeld der **Privacy Enhancing Technologies (PET)** die Idee durchgesetzt, dass jeder Benutzer seinen eigenen IDP betreiben könnte, seine personenbezogenen Daten damit selbst verwaltet und sie keinem externen Dienstleister anvertrauen muss.

   Aufgrund der Analogie mit einer Brieftasche, die der Benutzer jederzeit mit sich herumträgt und in der verschiedene Visitenkarten enthalten sein können, die an Dienstleister ausgehändigt werden, wurde dieser Ansatz ursprünglich als *local wallet* bezeichnet. Zwischenzeitlich hat sich der Begriff UCIM sowohl in wissenschaftlichen Veröffentlichungen als auch bei kommerziellen und Open Source Implementierungen durchgesetzt.

2.1.3.2. Mangelnde Interoperabilität zwischen FIM und UCIM

Während der Einsatz von FIM-Protokollen mit lokalen IDP-Installationen bei jedem Benutzer zum Erreichen der Ziele von UCIM theoretisch durchaus möglich wäre, ergeben sich praktisch die folgenden gravierenden Differenzen:

- UCIM ist ein junges Marktsegment und noch in der charakteristischen Phase schneller und leichter Begeisterung. Hersteller von UCIM-Produkten sind dadurch derzeit gezwungen, sich angesichts mangelnder Standardisierung und Regulierung durch möglichst viele Innovationen von bereits Vorhandenem und möglichen Konkurrenten zu differenzieren. Konsequenterweise wurde eine Vielzahl neuer Kommunikationsprotokolle geschaffen, die zwar inzwischen nach und nach konsolidiert werden, sich jedoch nur langsam an Interoperabilität mit FIM-Komponenten annähern.

  Viele der neu geschaffenen Protokolle wurden mit dem Anspruch entwickelt, eine leichtgewichtige und relativ einfach zu implementierende Alternative zu den industriellen FIM-Standards schaffen zu wollen. Während sich der Betrieb eines IDPs lokal beim Benutzer durchaus vereinfachend auf die FIM-Workflows auswirkt (vgl. Abschnitt 2.1.2.7), hat sich gezeigt, dass die sukzessive Erweiterung der UCIM-Protokolle bei steigenden Anforderungen durchaus zu ähnlicher Komplexität führt.

- Vom Benutzer selbst betriebene IDPs erfüllen im Allgemeinen nicht das im Rahmen von FIM wichtige Kriterium, zuverlässige und vertrauenswürdige Datenquellen zu sein. Im Gegensatz zu professionell als Dienst betriebenen IDPs bestünde hier die Möglichkeit, dass die Benutzer die von ihnen verwalteten Daten nach Belieben manipulieren und der Wahrheitsgehalt der an einen SP übermittelten Daten keiner externen Überprüfung, beispielsweise durch Lichtbildkontrolle bei der Registrierung des Benutzers, unterzogen wurde. In Abschnitt 2.1.3.5 wird für dieses Problem ein Lösungsansatz, der von mehreren Herstellern derzeit angestrebt wird, beschrieben.

Wie in Kapitel 3 gezeigt wird, treffen viele der in dieser Arbeit behandelten FIM-Aspekte auch auf UCIM-Szenarien zu, so dass die erarbeiteten Ergebnisse auf UCIM übertragen werden können. Dadurch, dass bei lokal beim Benutzer betriebenen Komponenten keine Integration in organisationsweite I&AM-Systeme erforderlich ist, ergeben sich an einigen Stellen Vereinfachungen; der Schwerpunkt dieser Arbeit liegt deshalb auf FIM, berücksichtigt aber

entsprechende UCIM-Konzepte insbesondere in Szenarien, in denen FIM und UCIM parallel eingesetzt werden sollen.

2.1.3.3. Datenschutz und Trust Management in UCIM-Szenarien

Da UCIM alle Operationen des Identity Managements aus Benutzerperspektive betrachtet, vereinfacht sich die Einhaltung datenschutzrechtlicher Randbedingungen im Bezug auf die Übermittlung der Daten: Da der Benutzer immer selbst entscheidet, welche Daten er zum jeweiligen SP übermittelt, kann die Akquisition der Daten als äquivalent zur manuellen Selbstregistrierung gesehen werden. Dienstleisterseitig wird UCIM durch ein I&AM-System komplementiert, so dass die in Abschnitt 2.1.1.6 beschriebenen Auflagen gelten.

Wie im nachfolgenden Abschnitt 2.1.3.4 gezeigt wird, übermitteln SPs Anfragen nach personenbezogenen Daten in maschinenlesbarer Form an den vom Benutzer betriebenen IDP. In der Regel fragen UCIM-Implementierungen dann beispielsweise in Form eines Popup-Fensters im Browser beim Benutzer nach, ob die angeforderten Daten übermittelt werden sollen. Bei häufigen Anfragen könnte sich beim Benutzer jedoch ein Gewöhnungseffekt einstellen, der ihn dazu verleitet, die Datenübertragung immer zu bestätigen, ohne sich genauer über den Umfang der freigegebenen Informationen und den Zweck ihrer Erfassung zu informieren. Ein Forschungsschwerpunkt im UCIM-Umfeld ist deshalb die graphische Gestaltung von Benutzeroberflächen unter Usabilityaspekten, so dass die volle Aufmerksamkeit des Benutzers erzwungen wird [PRUSAB].

Da im Rahmen von UCIM keine organisationsübergreifenden Service Level Agreements getroffen werden, fehlt eine explizite Unterstützung des Trust Managements, wie sie beispielsweise durch auf Basis von Verträgen vordefinierten Trust Levels erreicht werden kann. Die Benutzer sind also darauf angewiesen, unabhängig von UCIM herkömmliche Kriterien zur Auswahl vertrauenswürdiger SPs anzuwenden und müssen die Risiken der Freigabe von personenbezogenen Daten selbst abschätzen.

2.1.3.4. Grundlegende UCIM-Workflows

Der Betrieb eines individuellen IDP kann prinzipiell auf zwei Arten erfolgen:

1. Die entsprechende Software ist lokal auf dem Gerät des Benutzers installiert. Diese Variante ist die weiter verbreitete und wird im Umfeld der Privacy Enhancing Technologies stark bevorzugt.

2. Der Benutzer betreibt die IDP-Software auf einem externen Server, beispielsweise bei einem Internetprovider, der auch die eventuell vorhandene persönliche Webseite des Benutzers hostet. Dadurch wird zwar eine Unabhängigkeit vom gerade verwendeten Endgerät und damit bessere Flexibilität und Mobilität erreicht; das Ziel, keinem externen Anbieter alle eigenen Daten anvertrauen zu müssen, wird dadurch jedoch nicht mehr erreicht.

Unabhängig davon, dass im zweiten Fall die Daten prinzipiell auch verfügbar wären, wenn das Gerät des Benutzers nicht eingeschaltet ist, sehen alle bisherigen UCIM-Ansätze vor, dass

ein Abruf der Daten nur interaktiv erfolgen kann, indem der Benutzer jeden Datenübertragungsvorgang bestätigen oder zumindest kontrollieren können muss.

Der Abruf von Daten durch den SP besteht aus folgenden Schritten:

1. Der Benutzer ruft den Dienst durch Eingabe des entsprechenden URL in seinem Webbrowser auf.

2. Das von einem UCIM-unterstützenden SP zurückgelieferte HTML-Dokument enthält die folgenden Bestandteile:

   a) Ein HTML-Formular, in das die für die Dienstnutzung benötigten Daten vom Benutzer manuell eingetragen werden können, um abwärtskompatibel mit herkömmlichen, nicht UCIM-fähigen Clients zu bleiben.

   b) Maschinenlesbare Metadaten, die dem Benutzer nicht angezeigt werden, aber von einem UCIM-Client ausgewertet werden können. Sie geben an, welche Daten in die Formularfelder einzutragen sind; die möglichen Datenfelder und damit das verwendete Informationsmodell werden dabei vom jeweiligen UCIM-Ansatz vorgegeben und können ggf. erweitert werden. Je nach UCIM-Protokoll können noch weitere Angaben enthalten sein, beispielsweise für welche Zwecke die Daten benötigt werden und welche Konsequenzen das Fehlen der Daten auf die Erbringung des Dienstes hätte.

   c) Ein optionales Eingabefeld, in dem der Benutzer die Adresse des von ihm betriebenen IDP spezifizieren kann, sofern dieser Dienst nicht auf dem von ihm gerade verwendeten Gerät läuft. In diesem Fall wird ein Zwischenschritt durchgeführt, in dem der Benutzer per HTTP-Redirect zu seinem IDP umgeleitet wird, wo er sich gegebenenfalls noch authentifizieren muss.

3. Die IDP-Software präsentiert dem Benutzer eine Liste der angeforderten Daten. Je nach im vorangegangenen Schritt übertragenen Metadaten und Implementierung kann diese Darstellung mit Zusatzinformationen angereichert werden, beispielsweise welche Daten bereits in der Vergangenheit an diesen SP übermittelt worden sind.

4. Der Benutzer muss die Übertragung der angeforderten Daten genehmigen; dabei sind je nach Implementierung folgende Möglichkeiten gegeben:

   - Die Datenübertragung kann nicht nur kollektiv für alle angeforderten Daten zugelassen oder verhindert werden, sondern es kann beispielsweise die Übermittlung einzelner Attribute verhindert werden.
   - Der Benutzer kann aus verschiedenen beim IDP hinterlegten Identitäten auswählen oder die an diesen SP zu sendenden Werte der Attribute manuell eintragen. Dieser Schritt ist insbesondere dann notwendig, wenn Attribute angefordert wurden, für die dem IDP noch kein Wert bekannt ist.
   - Optional kann der Benutzer angeben, dass die ausgewählte Menge an Attributen immer an diesen SP übermittelt werden darf, so dass er die Übertragung nicht jedes Mal bestätigen muss.

5. Die vom Benutzer freigegebenen Daten werden an den SP übermittelt. Je nach UCIM-Ansatz existiert hierfür ein dediziertes Protokoll oder die IDP-Software muss das in Schritt 2 bereitgestellte HTML-Formular automatisch ausfüllen und abschicken.

6. Weitere Anfragen durch den SP durchlaufen denselben Workflow ab Schritt 2.

Im Hinblick auf die Einhaltung von Datenschutzaspekten ist zu berücksichtigen, dass der Abdeckungsgrad aller aktuellen UCIM-Ansätze mit der Übergabe der Daten an den SP endet. Damit bietet auch UCIM insbesondere keine Maßnahmen, um beispielsweise die zweckgebundene Verarbeitung der Daten beim SP zu überwachen.

Die UCIM-Spezifikationen der Interaktionen zwischen IDP und Benutzer sind hingegen bereits sehr ausgereift und werden aufgrund ihrer Übertragbarkeit auf das FIM-Umfeld in dieser Arbeit aufgegriffen.

2.1.3.5. Einsatz von Attributszertifikaten in UCIM

Die Unterstützung von UCIM-Protokollen erhöht zwar den Komfort für die Benutzer, da sie ihre Daten nicht mehr jedesmal manuell eintragen müssen, sie ist für den Service Provider aber mit keiner Garantie für eine bessere Datenqualität verbunden, da die Benutzer nach wie vor absichtlich falsche Daten liefern könnten.

Ein Lösungsansatz für dieses Problem ist die Verwendung so genannter **Attributszertifikate** (*attribute certificates, ACs*). ACs werden in PKI-Standards wie X.509 unterstützt [RFCAC] und unterscheiden sich von den derzeit weiter verbreiteten Server- und User-Zertifikaten dadurch, dass die Certificate Authority (CA) nicht den Public Key einer verifizierten Entität durch digitale Signatur bestätigt, sondern eines oder mehrere ihrer Attribute. Das resultierende Zertifikat kann damit nicht für Identifikation und Authentifizierung des Benutzers eingesetzt werden, sondern für den beglaubigten Nachweis ausgewählter Attribute, auf deren Basis in der Regel Autorisierungsentscheidungen beim SP getroffen werden.

Es wäre damit beispielsweise möglich, alle abrechnungsrelevanten Attribute von der Hausbank des Benutzers zertifizieren zu lassen und das AC dann einem SP vorzulegen. Sofern dieser der Bank, die das AC ausgestellt hat, vertraut, und die Integrität und Gültigkeit des Zertifikats durch Verifizierung der Signatur prüft, liegen dem SP somit zuverlässige Daten vor.

Wie Zertifikate für digitale Signaturen haben sich auch ACs im Endanwenderbereich noch nicht durchgesetzt; dies ist insbesondere auf die mangelnde Attraktivität und die Komplexität des Verfahrens sowie auf das Fehlen intuitiver graphischer Benutzeroberflächen zurückzuführen [PKIFL].

Aufgrund des Bedarfs im UCIM-Umfeld und seinem Schwerpunkt auf benutzerfreundlichen Bedienoberflächen ist jedoch abzusehen, dass das Potential von ACs zukünftig besser ausgereizt werden wird. Insbesondere wird durch die Auslieferung der UCIM-Software Microsoft CardSpace zusammen mit dem Betriebssystem Windows Vista eine nahezu flächendeckende Grundversorgung erreicht. Es ist zu erwarten, dass durch die Verfügbarkeit dieses Hilfsmittels und umfassende Diskussion neuer Betriebssystemfunktionalitäten in den Medien für viele SPs Anreize geschaffen werden, das Verfahren zu unterstützen.

2.1.3.6. Szenario 2: UCIM am Beispiel von Microsoft CardSpace

Das folgende fiktive Beispiel illustriert den Einsatz von UCIM-Systemen am Beispiel von Microsoft CardSpace (siehe auch Abschnitt 3.9). In Abschnitt 2.1.3.7 werden daraus die auch für FIM relevanten Anforderungen abgeleitet.

Ausgangssituation Eine Videothek bietet ihren Ausleihservice über das Internet an. Für neue Benutzer fallen eine einmalige Einrichtungsgebühr und Kosten für jeden ausgeliehenen Titel an. Die Anmeldegebühr entfällt, wenn die vom Neukunden angegebene Adresse durch einen bekannten Internetprovider oder eine Kreditkartengesellschaft bestätigt wird, da der Anbieter über die Einrichtungsgebühr lediglich Kosten durch Rückläufe bei falschen Lieferadressen kompensieren möchte. Darüber hinaus wird Schülern und Studenten ein Rabatt auf die monatlichen Gebühren gewährt, sofern sie diesen Status nachweisen können.

Ein Student möchte sich für diesen Dienst anmelden und dabei beide Vergünstigungen nutzen. Er besitzt eine Kreditkarte, die er zum Nachweis seiner Adresse einsetzen möchte; um Missbrauch vorzubeugen, will er die laufenden Kosten jedoch auf Rechnung per Überweisung und nicht per Bankeinzug oder Kreditkartenzahlung begleichen.

Initiale Registrierung Der Benutzer ruft über seinen Webbrowser die Webseite des Anbieters auf und wählt den Menüpunkt für die Registrierung von Neukunden. Es wird ein Formular angezeigt, in das verschiedene Stammdaten, Kontaktinformationen und Angaben zur gewünschten Zahlungsweise eingetragen werden müssen.

Über die im Formular eingebetteten Metadaten erkennt die CardSpace-Software, dass vom Anbieter personenbezogene Daten angefordert werden. Daraufhin werden ohne weitere Interaktion durch den Benutzer folgende Aktionen durchgeführt:

1. Das Serverzertifikat des Anbieters wird abgerufen und mit der vom Benutzer eingegebenen Adresse der Webseite verglichen, um zu verifizieren, dass es sich um den richtigen Anbieter und nicht z. B. einen Phishing-Versuch handelt.

2. Dem Benutzer werden einige Informationen über den Anbieter angezeigt, unter anderem sein Logo und die Angabe, dass die im Serverzertifikat enthaltenen Angaben überprüft worden sind und zur aufgerufenen Webseite passen (siehe Abbildung 2.16).[2]

3. Darüber hinaus wird eine Liste der angeforderten Daten angezeigt, wobei die jeweiligen Verwendungszwecke und andere datenschutzrechtliche Angaben abgerufen werden können.

4. CardSpace verwaltet Mengen von Benutzerattributen in Form von Visitenkarten. Die Software berechnet einen Vorschlag, welche der vorhandenen Visitenkarten minimal an den Anbieter übermittelt werden müssten, um alle angeforderten Daten abzudecken.

[2] Die beiden abgedruckten Screenshots stammen aus einer Einführung in Microsoft CardSpace für Entwickler und passen nicht exakt zum beschriebenen Szenario [CARDSP]. Sie zeigen jedoch die wesentlichen Elemente der Benutzeroberfläche.

Abbildung 2.16.: Szenario 2: Anzeige von Informationen über den Service Provider in CardSpace (Bildquelle: [CARDSP])

Im vorliegenden Fall wird dem Benutzer vorgeschlagen, seine Visitenkarte mit Namen und Adresse sowie seine vollständigen Kreditkartendaten zu verwenden. Damit könnte jedoch einerseits der Rabatt für Studenten nicht genutzt werden, andererseits soll die Kreditkartennummer explizit nicht übertragen werden, da ein anderer Zahlungsweg gewünscht wird. Als Konsequenz müssen neue CardSpace-Visitenkarten angelegt werden, bevor die Dienstanmeldung fortgesetzt werden kann.

Akquisition von Attributszertifikaten Der Benutzer benötigt Nachweise seiner Adresse und seines Studentenstatus. Da die CardSpace-Software die entsprechenden Attributszertifikate nicht automatisch abrufen kann, ist ein manuelles Eingreifen durch den Benutzer erforderlich:

1. Über das Webportal seiner Hochschule kann der Student einen elektronischen, digital signierten Studentenausweis abrufen, dessen Gültigkeit auf das aktuelle Semester beschränkt ist. CardSpace erkennt, dass ein Attributszertifikat abgerufen wird und bietet die Möglichkeit an, es entweder in den lokalen Datenbestand zu integrieren oder für jedes Attribut nur einen Verweis zu speichern, wo es jederzeit aktuell abgerufen werden kann.

2. Die Kreditkartengesellschaft bietet online keine Möglichkeit, Attributszertifikate für beliebige Teilmengen der über den Kunden bekannten Daten auszustellen. Der Benutzer muss deshalb in die Filiale seiner Hausbank, über die er die Kreditkarte erhalten hat, und erhält dort ein entsprechendes Attributszertifikat auf einer CD. Dieses kann er an seinem Rechner in den CardSpace-Datenbestand importieren.

Übermittlung der CardSpace-Visitenkarten Da inzwischen weitere Visitenkarten verfügbar sind, ändert die CardSpace-Software ihren Vorschlag zur Übermittlung der Daten so ab, dass neben einer unzertifizierten Visitenkarte mit Namen und E-Mail-Adresse auch der elektro-

nische Studentenausweis und das Attributszertifikat mit der von der Bank im Namen der Kreditkartengesellschaft beglaubigten Adresse übermittelt werden.

Der Benutzer stimmt diesem Vorschlag zu; die CardSpace-Software überträgt die ausgewählten Daten an den Anbieter und trägt in ein Protokoll ein, welche Visitenkarten zu welchem Zeitpunkt an diesen Anbieter übertragen worden sind.

Der Dienst kann nun mit den angestrebten Vergünstigungen genutzt werden; da die Daten zur Auftragsverarbeitung, z. B. zur Etikettierung von Postsendungen, auch dann benötigt werden, wenn der Anwender den Dienst gerade nicht nutzt, ist der Anbieter darauf angewiesen, sie in einem lokalen I&AM-System zu speichern.

Reguläre Dienstnutzung Im laufenden Betrieb können zwei Arten von Ereignissen eintreten, die zu einer Aktualisierung der Daten führen, sofern diese nicht manuell vom Benutzer angestoßen wird:

1. Der Gültigkeitszeitraum eines Attributszertifikats läuft ab. Beispielsweise wird der Student jedes Semester dazu aufgefordert, innerhalb einer Karenzzeit einen neuen gültigen elektronischen Studentenausweis vorzulegen und verliert ansonsten seine Vergünstigungen.

2. Wenn der Student umzieht und seine neue Adresse in CardSpace einträgt, wird er darauf hingewiesen, dass diese auch der Online-Videothek mitgeteilt werden sollte. Da es sich bereits um einen Bestandskunden handelt, wird hierfür kein Attributszertifikat mehr benötigt. Der Benutzer muss jedoch auch dieser erneuten Übertragung seiner Daten zustimmen.

Über die CardSpace-Software kann sich der Benutzer jederzeit informieren, welche seiner personenbezogenen Daten wann an welche Dienstanbieter übermittelt wurden (siehe Abbildung 2.17).

Technische Komponenten Abbildung 2.18 gibt zusammenfassend einen Überblick über die am Szenario beteiligten technischen Komponenten:

- Der Service Provider bietet den genutzten Dienst an und speichert Benutzerprofile in einem lokalen Identity Repository. Aus Benutzerperspektive spielt es dabei keine Rolle, ob SP-seitig ein vollwertiges I&AM-System implementiert ist, solange der Dienst selbst UCIM-fähig ist.

- Die auf der Maschine des Benutzers installierte CardSpace-Software übernimmt die Rolle des Identity Providers. Sie speichert die benutzerspezifischen Visitenkarten in einem lokalen Identity Repository und stellt Konnektoren zum Service Provider sowie den Attribute Authorities bereit und verfügt über eine lokale Importschnittstelle für das Einspielen neuer Attributszertifikate. Da Änderungen an den Daten an die dafür relevanten SPs propagiert werden können, ähnelt die Funktionalität einem Meta-Directory.

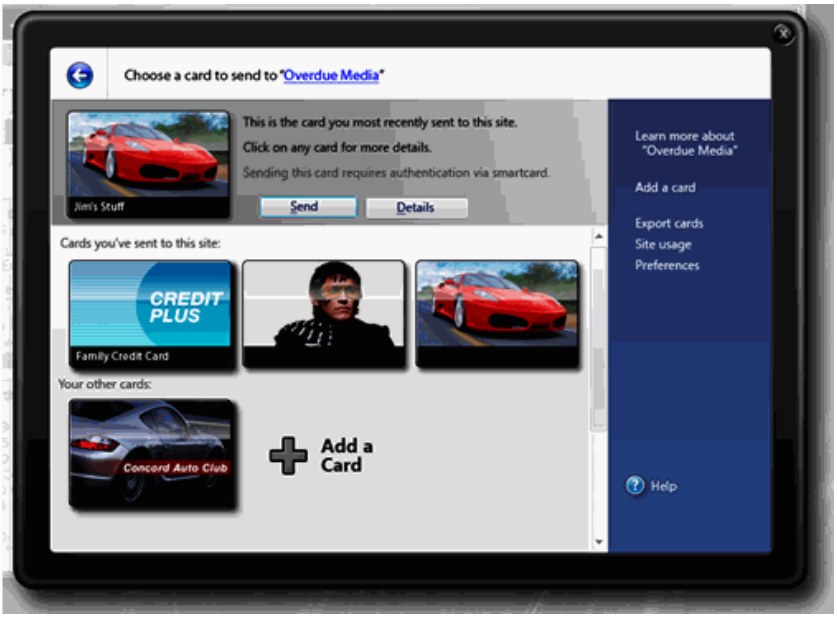


Abbildung 2.17.: Szenario 2: Anzeige bereits an einen Service Provider übertragener Informationen in CardSpace (Bildquelle: [CARDSP])

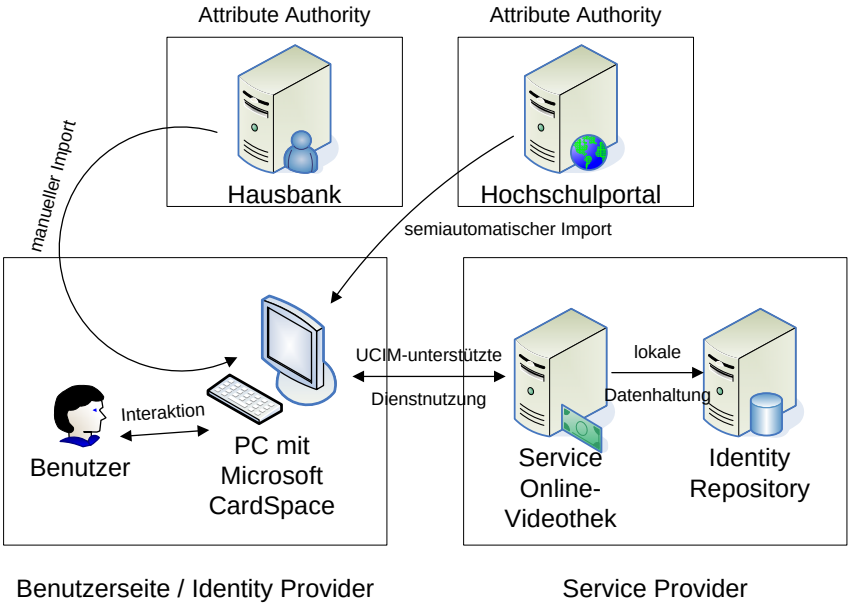


Abbildung 2.18.: Szenario 2: Überblick über die beteiligten Komponenten

- Attribute Authorities sind für die Erstellung der benötigten Attributszertifikate zuständig. Da es prinzipiell möglich ist, anstelle der Werte der Attribute nur einen Verweis auf den Speicherort der Attributswerte zu zertifizieren, kann es zu einem direkten Kontakt zwischen SP und AA kommen, wenn die Werte abgerufen werden.

Charakteristisch für UCIM ist die häufige Interaktion zwischen Benutzer und IDP sowie die Orchestrierung der Datenflüsse durch den IDP.

2.1.3.7. Anforderungen aus Szenario 2

Die umfassenden Möglichkeiten zur Steuerung und Kontrolle der Verbreitung personenbezogener Daten im UCIM-Umfeld bieten Vorteile, die auch beim Einsatz von FIM relevant sind und deshalb als Anforderungen an FIM-Komponenten aufgenommen werden:

Funktionale Anforderungen Durch die Betrachtung des Datenaustausches aus Benutzerperspektive ergeben sich folgende funktionale Schwerpunkte beim IDP:

- Der IDP muss dem Benutzer Vorschläge machen, wie Datenanfragen durch einen SP am Besten beantwortet werden können; bei einer festen Gruppierung von Attributen könnte ein Vorschlag beispielsweise

  – auf Basis von Prioritäten der Visitenkarten gebildet werden,
  – die Anfrage mit möglichst wenigen Visitenkarten beantwortet werden, oder
  – eine Antwort aus mehreren Visitenkarten mit jeweils möglichst wenigen Attributen konstruiert werden.

  Ziel muss dabei sein, möglichst nur genau diejenigen Attribute zu übermitteln, die angefordert wurden, um dem SP aus Datenschutzgründen keine darüber hinaus gehenden Informationen zukommen zu lassen. Dieses Ziel wird dadurch erschwert, dass es nicht möglich ist, einzelne Attribute aus einem Attributszertifikat zu entfernen, ohne dessen digitale Signatur zu zerstören [FA-IDP-Antwortvorschlag].

- Die Daten müssen dem SP im von ihm benötigten Format zur Verfügung gestellt werden. Hierzu sind gegebenenfalls Datenkonvertierungen durchzuführen; beim Einsatz von Attributszertifikaten kommt wiederum erschwerend hinzu, dass die Datenwerte nicht modifiziert werden können, ohne die digitale Signatur ungültig zu machen. Dies entspricht der Anforderung [FA-Schema] aus Szenario 1, erweitert um Attributszertifikate.

- Der Benutzer muss die Möglichkeit haben, aus verschiedenen Identitäten bzw. Profilen auswählen zu können [FA-Identitätswahl].

- Die IDP-Software muss den Benutzer beim Anlegen neuer Visitenkarten und beim Import von Attributszertifikaten unterstützen [FA-Import/Export].

- Service Provider und Attribute Authorities sollen die Möglichkeit haben, Daten nach Bestätigung durch den Benutzer in dessen Identity Repository schreiben zu können. Dadurch wird die Anforderung [FA-Schreibzugriff] aus Szenario 1 um Benutzerinteraktion erweitert.

- Änderungen an den Daten sollen an die betroffenen Service Provider propagiert werden können, um Inkonsistenzen zu vermeiden (entspricht [FA-Updates] aus Szenario 1).
- Sofern der Benutzer verschiedene Geräte verwenden möchte (z. B. Desktop-PC, Notebook und PDA), müssen der Datenbestand und die entsprechenden Metadaten zwischen diesen automatisiert abgeglichen werden können [FA-IDP-Verfügbarkeit].

Nichtfunktionale technische Anforderungen Durch den hohen Grad an Interaktivität zwischen Benutzer und IDP sind folgende Aspekte zu berücksichtigen:

- Die graphische Benutzeroberfläche muss intuitiv und ergonomisch zu bedienen sein [NFA-Usability].
- Das Verfahren muss skalierbar sein. Da durch die Selbstverwaltung der Daten durch jeden einzelnen Benutzer bereits ein sehr hoher Grad an Dezentralisierung erreicht wird, betrifft dies
  - einerseits die Möglichkeit, ähnliche Service Provider beispielsweise gruppieren und Datenfreigaben für SP-Gruppen statt für jeden einzelnen SP spezifizieren zu können,
  - andererseits die Akquisition und Verwaltung von Attributszertifikaten und deren periodische Erneuerung beim Ablauf der Gültigkeitszeiträume.

  Die entsprechenden Unterpunkte von [NFA-Skalierbarkeit] aus Szenario 1 werden hierdurch entsprechend erweitert.

Sicherheitsanforderungen Die Sicherheitsanforderungen im UCIM-Umfeld entsprechen denen bei I&AM- bzw. FIM-Systemen, wobei besondere Rücksicht darauf zu nehmen ist, dass einige Komponenten auf der Maschine des Benutzers betrieben werden:

- Die Datenübertragung muss sicher erfolgen; daraus ergeben sich die bereits bei Szenario 1 genannten Forderungen nach Maßnahmen zur Sicherstellung von Authentizität, Integrität und Vertraulichkeit der übertragenen Daten ([SEC-Datenübertragung]).
- Durch den Betrieb des IDP auf der Maschine des Benutzers ergeben sich neue Bedrohungen durch schadhafte Software wie Viren, Würmer und trojanische Pferde, mit denen privat genutzte PCs wesentlich häufiger infiziert werden als professionell betriebene IDP-Server. Umso mehr müssen Methoden wie die gegenseitige Isolation von Prozessen durch das Betriebssystem und die Verschlüsselung des lokalen Identity Repository angewandt werden, um Datenausspähversuche zumindest zu erschweren [SEC-IDP-Systemsicherheit].
- Angriffe durch die Wiedervorlage von Daten (*replay attack*), die ein Angreifer über das Netzwerk mitgeschnitten hat, um sich damit als der eigentliche Benutzer auszugeben, müssen beispielsweise durch signierte Zeitstempel und beschränkte Gültigkeitsdauern verhindert werden; dieser Teilaspekt der bei Szenario 1 genannten Anforderung [SEC-Integration] wird dadurch betont.

- Bei UCIM werden die vom SP gestellten Datenanfragen im Rahmen der vom Benutzer abgerufenen Webseiten übermittelt; durch die starke Integration der clientseitigen UCIM-Komponenten mit dem Webbrowser des Benutzers ist es nicht notwendig, dass der SP direkt mit dem IDP kommuniziert, so dass beispielsweise auch keine zusätzlichen Freigaben in Firewalls erforderlich sind.

  Aus dieser über den Client mittelbaren Datenübertragung zwischen IDP und SP ergibt sich eine aus IDP-Sicht sicherheitstechnisch positive Entkopplung, da die IDP-Komponenten nicht direkt für die SPs zugänglich sein müssen. Dieser Datenübertragungsweg sollte deshalb auch im FIM-Umfeld zur Wahl stehen [SEC-Übertragungswege].

Organisatorische Anforderungen Da der Einsatz von UCIM im Wesentlichen eine Alternative zur manuellen Selbstregistrierung für webbasierte Dienste darstellt, sind sowohl SP- als auch benutzerseitig keine organisatorischen Vorbereitungen zu treffen.

Der Einsatz von Attributszertifikaten bedingt jedoch SP-seitig eine Möglichkeit zur Verifikation dieser Zertifikate. Dazu muss entweder eine gemeinsame PKI aufgebaut werden oder die zur Verifikation von Zertifikaten benötigten Metadaten müssen den SPs in geeigneter Form bereitgestellt werden, beispielsweise durch einen automatisierten Austausch der jeweiligen CA-Wurzelzertifikate. Eine Nutzung existierender PKIs ist deshalb auch im FIM-Umfeld anzustreben [ORG-PKI].

Datenschutzanforderungen Die Einhaltung von Datenschutzrichtlinien ist bei UCIM ein explizit formuliertes Ziel und steht stärker im Vordergrund als bei den anderen Varianten des Identity Managements. Die Vorteile von UCIM lassen sich deshalb als Anforderungen an FIM-Komponenten postulieren:

- Benutzer müssen ihre Daten selbst verwalten und genau spezifizieren können, welche Teilmengen der Daten zu welchen Zwecken an welche SPs übermittelt werden. Die Interaktion mit dem Benutzer in der aus Szenario 1 bekannten Anforderung [DSA-ARPs] wird dadurch betont.
- Die Protokollierung durch den IDP, welche Daten wann an welche SPs übermittelt wurden, erleichtert die Umsetzung der informationellen Selbstbestimmung; sie ist jedoch kein Ersatz dafür, dass der Benutzer auch beim SP einsehen kann, welche Daten dort über ihn gespeichert werden. Insbesondere sollte es einfach möglich sein, die Differenzmengen zwischen den übertragenen und den tatsächlich gespeicherten Daten zu ermitteln [DSA-Selbstbestimmung].
- Die Weitergabe der Daten an Dritte durch einen Service Provider, z. B. im Rahmen von Delegation, muss beschränkt werden können [DSA-Delegation].
- Der Einsatz von Attributszertifikaten, die vom Benutzer an den SP übermittelt werden, bietet den Vorteil, dass der SP nicht direkt mit der AA in Kontakt tritt und diese somit auch nicht in Erfahrung bringt, welche Benutzerdaten von welchem SP für welche Zwecke abgefragt werden. Die AA kann somit kein Datenverkehrsprofil erstellen. Der Einsatz von Attributszertifikaten sollte somit auch bei FIM möglich sein [DSA-Attributszertifikate].

Wie in Kapitel 3 gezeigt wird, erfüllen nicht nur FIM-Ansätze, sondern auch viele UCIM-Varianten nur einen Teil dieser Anforderungen. Komplexere Szenarien, in denen beispielsweise die Abfrage der Eigenschaften von Gruppen, in denen ein Benutzer Mitglied ist, relevant sind, können mit UCIM derzeit nicht umgesetzt werden.

2.2. FIM-Szenarien und Anforderungen

In den folgenden Abschnitten 2.2.1–2.2.3 werden die FIM-Prozesse anhand dreier konkreter Szenarien erläutert und entsprechende Anforderungen an FIM-Lösungen und -Komponenten abgeleitet.

Jedes Szenario behandelt einen umfassenden Aspekt aus dem Dienstangebot des Leibniz-Rechenzentrums (LRZ) der Bayerischen Akademie der Wissenschaften und basiert somit auf realen Gegebenheiten. Die Szenarien wurden unter den folgenden Gesichtspunkten ausgewählt und zusammengestellt:

- Die reale praktische Notwendigkeit von FIM wird verdeutlicht und faktisch untermauert.
- Die Szenarien sind zwar fiktiv und idealisiert dargestellt, da in der Realität noch kein umfassendes FIM-Deployment vorliegt; sie reflektieren aber den aktuellen Stand an Zielen und Planungen.
- Zusammen mit Szenario 1 ergibt sich ein umfassendes und durchgängiges Gesamtbild, dessen Komplexität aufgrund der Heterogenität seiner Bestandteile durchaus mit den FIM-Aspekten umfangreicher Business-to-Business- und Supply-Chain-Management-Szenarien vergleichbar ist.
- Alle Anforderungen an und Eigenschaften von I&AM- und FIM-Komponenten sowie deren Zusammenspiel lassen sich anhand der Szenarien veranschaulichen, so dass in den Kapiteln 4 und 5 darauf zurückgegriffen werden kann.

Szenario 3 behandelt die Rolle des LRZ als Münchner Hochschulrechenzentrum. Die FIM-spezifischen Herausforderungen im Bereich des Hochleistungsrechnens und Grid Computings werden in Szenario 4 behandelt. Abschließend geht Szenario 5 auf Aspekte des über den Münchner Raum hinausgehenden hochschulübergreifenden Benutzerdatenaustausches ein, um Prozesse wie das IT-unterstützte Lernen und die Mobilität von Studenten zu verbessern.

2.2.1. Szenario 3: Das LRZ als Service Provider im MWN

Das LRZ unterscheidet sich von den meisten anderen Hochschulrechenzentren unter anderem dadurch, dass es nicht nur für genau eine, sondern für alle Hochschulen im Umkreis zuständig und organisatorisch wie auch juristisch unabhängig von ihnen ist.

Dieses Szenario befasst sich mit dem Dienstangebot des LRZ für die Münchner Hochschulen und seiner angestrebten Nutzung über FIM-Protokolle; der Einzugsbereich wird dabei durch das so genannte Münchner Wissenschaftsnetz (MWN) definiert.

2.2.1.1. Dienstspektrum und Ausgangssituation

Das LRZ bietet seinen Kunden im MWN eine Vielzahl verschiedenster Dienste an, von denen unter anderem die folgenden eine Authentifizierung und Autorisierung der Benutzer erfordern:

- Netzbetrieb: Neben der strukturierten Verkabelung von mehr als 60 Standorten werden Hunderte von WLAN Access Points betrieben, die authentifizierten Nutzern den Zugang zu virtuellen Privaten Netzen (VPNs) und die Nutzung von Diensten wie dem DFN-Roaming ermöglichen.
- E-Mail: Für eine Vielzahl von Einrichtungen in der Granularität von Fakultäten und Lehrstühlen werden E-Mail-Dienste mit dedizierten Domänennamen, zentraler Virenfilterung und Schutzmaßnahmen gegen Spam angeboten.
- Datenspeicher: Neben zentralen Fileservern stehen intensiv genutzte Backup- und Archivierungsdienste zur Verfügung.
- Hosting: Für mehrere Dienste wird Hosting angeboten, beispielsweise für Lehrstuhl- und Fakultätswebserver, auf denen Webapplikationen betrieben und an die hochverfügbaren Datenbanken des LRZ angebunden werden können.
- Software: Das LRZ koordiniert den Einkauf von Softwarelizenzen und ermöglicht dabei günstige Konditionen z. B. durch Mengenrabatte und Landeslizenzverträge. Darüber hinaus werden kostenlose Software-Update-Server für Virenschutz und verschiedene Betriebssysteme zur Verfügung gestellt.
- Hochleistungsrechnen: Unter der Voraussetzung der Genehmigung rechenintensiver Vorhaben stehen auch den Wissenschaftlern im MWN die in Szenario 4 beschriebenen Hochleistungsrechner zur Verfügung.

Während einige Dienste wie beispielsweise E-Mail über den LRZ Webmail-Dienst auch mit einem Browser als Client genutzt werden können, ist der Einsatz dedizierter Clients und Protokolle (bei E-Mail beispielsweise SMTP und IMAP bzw. POP3) auf absehbare Zeit noch wesentlich weiter verbreitet. Vor dem in Kapitel 3 diskutierten Hintergrund, dass alle aktuellen FIM-Ansätze auf webbasierte Dienste bzw. Web Services beschränkt sind, muss unbedingt berücksichtigt werden, dass der Einsatz von off-the-shelf FIM-Komponenten derzeit nicht möglich ist.

Die Kennungen und Berechtigungen der rund 100.000 Studenten und Mitarbeiter der Münchner Hochschulen werden vom LRZ in einem I&AM-System verwaltet. Die erfassten Daten lassen sich grob in vier Kategorien einteilen:

1. **Einrichtungen**: Hierbei handelt es sich um die Basisinformationen über die Kunden, beispielsweise den Namen und die Anschrift eines Lehrstuhls und seine Eingliederung in die Organisationsstruktur der jeweiligen Hochschule.
2. **Projekte**: Verträge zwischen Einrichtungen und dem LRZ werden von Form von SLAs, die als „Projekte“ bezeichnet werden, geschlossen; für sie wird jeweils definiert, wie viele Kennungen mit welchen Dienstberechtigungen für welchen Zweck unter welchen

Konditionen zur Verfügung gestellt werden. Für jedes Projekt wird mindestens ein so genannter Master User auf der Seite der Einrichtung ernannt, der als technischer Ansprechpartner für das LRZ fungiert.

3. **Personen**: Von Einrichtungsleitern, Master Usern und Benutzern werden Stamm- und Kontaktinformationen gespeichert.

4. **Kennungen**: Für jede Kennung werden ihre Berechtigungen zur Nutzung von Diensten sowie die dafür notwendigen Informationen (z. B. Passwort und numerische User-ID auf UNIX-Systemen) festgehalten. Eine Person kann mehrere Kennungen haben, wenn dies beispielsweise aus abrechnungstechnischen Gründen erforderlich ist.

Die Pflege dieser Daten wird dabei wie folgt delegiert:

- Die **zentrale Benutzerverwaltung** (ZBVW) des LRZ übernimmt die Erzeugung von Statistiken und einen Teil der Billing-Prozesse auf Basis der von den Diensten zur Verfügung gestellten Accountingdaten. Darüber hinaus werden die Softwarewerkzeuge für die nachfolgend genannten Anwendergruppen bereitgestellt und kontinuierlich weiterentwickelt.

- Die so genannten **LRZ-Betreuer** fungieren als Ansprechpartner für die Kunden und Master User in organisatorischen und technischen Belangen. Sie pflegen die Einrichtungs- und Projektdaten und stoßen die Bereitstellung der im Rahmen von Projekten vereinbarten Dienste und Ressourcen an.

- Die **Master User** verwalten die im Rahmen eines Projektes vergebenen Kennungen und führen die Zuordnung zu Benutzern durch, deren Kontaktdaten sie dazu eintragen müssen.

- Jeder **Benutzer** kann seine eigenen Daten über webbasierte Self Services einsehen und aktualisieren. Bei Fragen und Problemen wendet er sich an einen seiner Master User oder den LRZ Service Desk, aber nicht direkt an den LRZ-Betreuer.

Diese Zusammenhänge werden in Abbildung 2.19 veranschaulicht. Die Delegation administrativer Aufgaben an die Master User und die Pflege der eigenen Daten durch die Benutzer selbst ist ein kritischer Erfolgsfaktor für die Skalierbarkeit des gesamten Systems. Einerseits wäre eine zentrale Erfassung aller Personendaten aufgrund der Menge an Benutzern nicht handhabbar, andererseits ist jedoch die Qualität der Daten bei dezentraler Administration nur schwer zu kontrollieren und sicherzustellen. Beispielsweise werden Änderungen an den Anschriften einer Einrichtung nicht selten erst dadurch erkannt, dass ein einmal pro Jahr verschicktes Rundschreiben wegen Nichtzustellbarkeit retourniert wird, da die seitens der Einrichtung Verantwortlichen übersehen haben, die Änderung auch dem LRZ mitzuteilen.

Diese Schwierigkeiten sind insbesondere darauf zurückzuführen, dass die Benutzer ihre Daten mindestens doppelt pflegen müssen: Änderungen müssen einerseits der lokalen Hochschulverwaltung gemeldet werden, andererseits dem LRZ. In der Praxis kommt es damit zwangsweise zu partiell inkonsistenten, veralteten Daten. Ähnliche Probleme treten beim Service Support auf, da Benutzer manchmal nicht zwischen von einer lokalen Rechnerbetriebsgruppe und dem

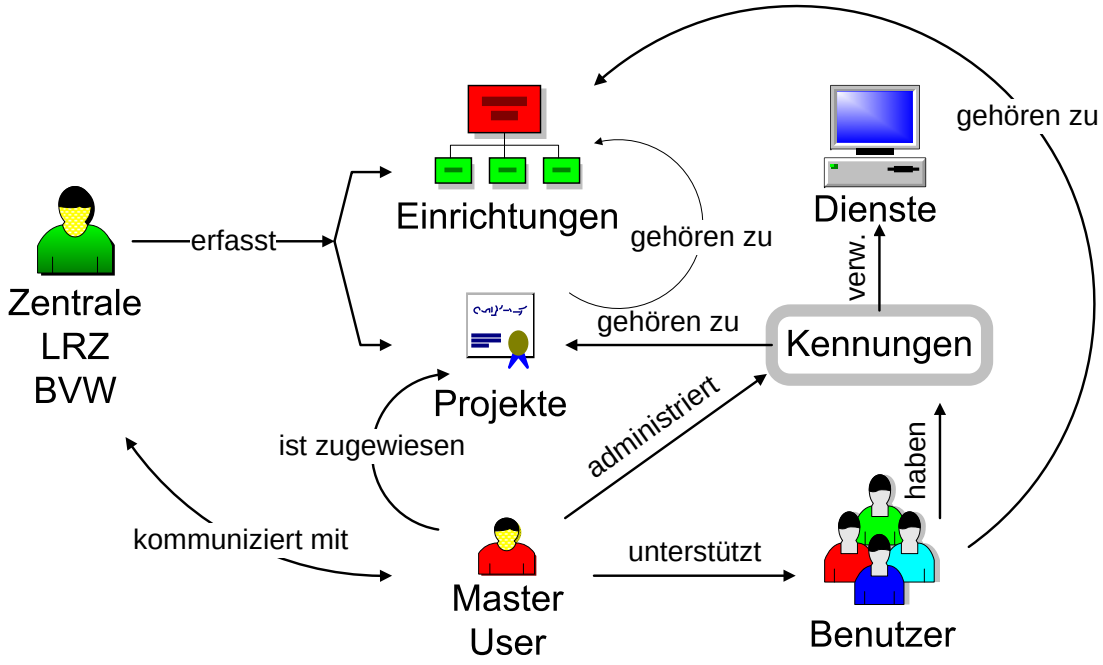


Abbildung 2.19.: Szenario 3: An Master User delegierte Administration

LRZ bereitgestellten Diensten unterscheiden können und Supportanfragen erst an die richtige Stelle weitergeleitet werden müssen.

Mit FIM soll deshalb einerseits die technische Basis dafür geschaffen werden, die an den Hochschulen lokal bereits vorhandenen Benutzerdatenbestände (vgl. Szenario 1) mit dem I&AM-System des LRZ abzugleichen, andererseits soll die organisatorische Grundlage gebildet werden, um die gemeinsamen, organisationsübergreifenden Geschäftsprozesse gesamtheitlich abzubilden und informationstechnisch zu unterstützen.

2.2.1.2. Das I&AM-System des LRZ

In diesem Abschnitt wird das am LRZ implementierte I&AM-System skizziert, um die beim Einsatz von FIM notwendigen Veränderungen und Integrationsmaßnahmen zu demonstrieren.

Abbildung 2.20 zeigt die Architektur des LRZ I&AM-Systems, an dessen Konzeption der Autor dieser Arbeit im Rahmen des Projekts LRZ-SIM („Sicheres Identitätsmanagement am LRZ“) beteiligt war; analog zu Szenario 1 werden mehrere miteinander über ein Meta-Directory synchronisierte Identity Repositories eingesetzt, um die Daten in verschiedenen Formaten zur Verfügung zu stellen:

- Der so genannte **Portalverzeichnisdienst** bildet die Schnittstelle zu webbasierten Managementfrontends wie beispielsweise den Self Services. Die Daten werden in einem Format vorgehalten, das einen effizienten Zugriff über die im Webumfeld populären Programmier- und Skriptsprachen erlaubt. Zudem werden Schreibzugriffe dedizierten

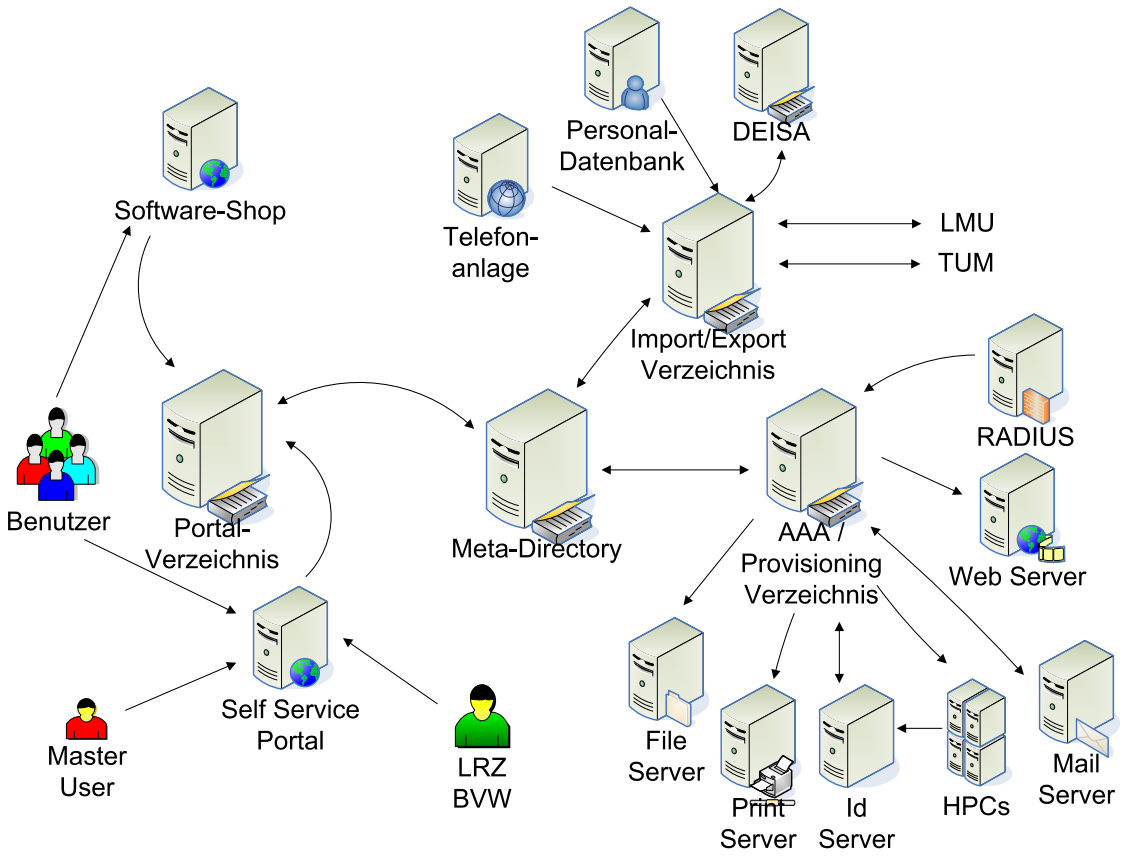


Abbildung 2.20.: Szenario 3: Architektur des LRZ Identity & Access Management Systems

Plausibilitätsprüfungen unterzogen, um die Ausnutzung eventueller Sicherheitslücken in den Frontends zu erschweren.

- Das **zentrale Meta-Directory** dient dem Datenabgleich zwischen den anderen Verzeichnisdiensten; Zugriffe auf die Daten erfolgen aus Sicherheitsgründen nur über die Konnektoren und nicht über Endsysteme oder durch Administratoren.

- Der **Authentifizierungs- und Autorisierungsverzeichnisdienst** stellt ausgewählte Daten über Kennungen und Projekte in standardisierten LDAP-Schemata zur Verfügung. LDAP-fähige Dienste und Rechnerplattformen können ihre Benutzer über diesen Verzeichnisdienst authentifizieren und benötigen keine lokale Benutzerverwaltung mehr. Zudem übernimmt dieser Server die Rolle eines Provisioningsystems und leitet die relevanten Benutzerdaten an Plattformen weiter, die noch nicht LDAP verwenden. Zu diesem Zweck werden die Daten in Form von Textdateien exportiert und in einem LRZ-spezifischen Verfahren an die Zielsysteme übermittelt; mittelfristig soll dieses proprietäre Verfahren durch den Standard SPML ersetzt werden (siehe Abschnitt 3.7.1).

- Der **Import-/Export-Verzeichnisdienst** bietet die Möglichkeit, weitere LRZ-interne Datenquellen und -abnehmer anzubinden. Beispielsweise wird die Organisationsstruktur des LRZ von seiner Verwaltung in Form einer Textdatei gepflegt und diese regelmäßig

importiert; ebenso können ausgewählte Daten des I&AM-Systems z. B. in relationale Datenbanken exportiert werden, um sie weiteren, nicht LDAP-fähigen Systemen zur Verfügung stellen zu können.

Der Import-/Export-Verzeichnisdienst dient darüber hinaus als mögliche Schnittstelle für den organisationsübergreifenden Datenaustausch, da er über Konnektoren mit den I&AM-Systemen anderer Organisationen verbunden werden kann. Diese Methodik wird aufgrund der in Kapitel 3 erläuterten Defizite aktueller FIM-Ansätze auch angewandt, stößt jedoch sehr schnell an ihre Grenzen:

- Es muss ein *dedizierter Konnektor* zum I&AM-System jeder Partnerorganisation implementiert werden. Dadurch ergeben sich unter anderem folgende Nachteile:
  - Der *Aufwand* ist z. B. aufgrund der zu implementierenden Datenkonversionen und Korrelationsmechanismen sehr hoch.
  - Konnektoren sind *statisch* und müssen manuell konfiguriert werden; dadurch wird die Dynamik hinsichtlich der Organisationen, mit denen Daten ausgetauscht werden können, massiv eingeschränkt.
  - Der Aufbau und die Schnittstellen von Konnektoren sind *nicht standardisiert*, so dass der volle Funktionsumfang in der Regel nur dann ausgeschöpft werden kann, wenn die I&AM-Systeme auf Quell- und Zielseite vom selben Hersteller stammen; an den beiden Münchner Universitäten und dem LRZ ist diese Bedingung erfüllt.
  - Konnektoren greifen tief ins System und ins Datenmodell ein, da sie beispielsweise Assoziationen zwischen den im Quell- und Zielsystem gespeicherten Objekten verwalten. Die Anzahl möglicher Konnektoren pro Verzeichnisdienst ist deshalb aus Performanzgründen begrenzt.
  - Durch die sehr enge Kopplung zwischen Quell- und Zielsystem wird das Change Management deutlich komplexer; beispielsweise müssen Änderungen sowohl an der netzwerkspezifischen Konfiguration von I&AM-Komponenten als auch am Datenmodell organisationsübergreifend berücksichtigt werden, so dass die Skalierbarkeit im praktischen Betrieb weiter eingeschränkt wird.
- Durch das Fehlen einer klaren technischen Trennung zwischen organisationsinternem und organisationsübergreifendem Datenaustausch ergeben sich neue Risiken:
  - Ein wechselseitiger direkter Zugriff auf die Datenbestände stellt eine nicht unerhebliche Sicherheitsbedrohung dar. Neben netzwerk- und dienstspezifischen Schutz- und Zugriffskontrollmaßnahmen ist deshalb eine außerordentlich starke Vertrauensbeziehung zwischen den beiden am Datenaustausch beteiligten Organisationen notwendig, die im Allgemeinen nicht vorliegt. Das LRZ-Szenario bildet diesbezüglich eine Ausnahme, da beispielsweise das in Szenario 1 beschriebene I&AM-System der TUM vom LRZ betrieben wird und somit einfacher als vertrauenswürdig eingestuft werden kann.
  - Durch das unmittelbare Einspeisen in die I&AM-Systeme anderer Organisationen gehen *Metainformationen* wie die Zweckbindung der erfassten Daten verloren.

Diese Informationen müssten somit explizit und organisationsübergreifend einheitlich abgebildet und mit übertragen werden. Derzeitige I&AM-Systeme sind darauf jedoch nicht ausgelegt, so dass aufwendige und tiefgehende Eingriffe in die technischen Abläufe und eine entsprechende Anpassung der Geschäftsprozesse notwendig werden würden. Im vorliegenden Szenario wurden entsprechende Vereinbarungen für die Auftragsdatenverarbeitung durch das LRZ außerhalb des I&AM-Systems getroffen und dort nicht explizit abgebildet.

- Einige Ziele von FIM wie das organisationsübergreifende Single Sign-On können nicht erreicht werden, da zwar Kennungen und Passwörter im Sinne eines Unified Logins abgeglichen werden können, sofern keine Konflikte im diesbezüglichen Namensraum vorliegen, aber keine gemeinsamen Authentifizierungs- und Autorisierungsinstanzen genutzt werden.

Im folgenden Abschnitt wird beschrieben, welche Ziele durch den Einsatz von FIM erreicht werden können und wie exemplarische LRZ-Dienste in diesem Rahmen genutzt werden könnten.

2.2.1.3. Ziele und exemplarische Prozesse beim Einsatz von FIM

In diesem Szenario wird davon ausgegangen, dass der Aufbau einer vertraglich geregelten Vertrauensbeziehung zwischen den beteiligten Organisationen möglich ist und diese über einen längeren Zeitraum konstant bleibt; im Gegensatz dazu geht Szenario 4 auf hochdynamische Situationen im Umfeld des Grid Computings ein.

Um die Probleme bei der in Abschnitt 2.2.1.1 beschriebenen Akquisition und Pflege der Daten zu lösen, wird durch FIM ein Abgleich der Daten zwischen den I&AM-Systemen des LRZ und seiner Kunden angestrebt, ohne die Systeme technisch zu stark zu koppeln, um die im vorhergehenden Abschnitt erläuterten Komplikationen zu vermeiden.

Für den Einsatz von FIM wird im Folgenden charakteristisch dargestellt, wie die Übernahme der Datensätze erst *bei Bedarf* zur Laufzeit erfolgt. Im Gegensatz zur organisationsübergreifenden Kopplung von I&AM-Systemen, bei der pauschal der gesamte Benutzerdatenbestand abgeglichen wird und eine Differenzierung nur über die jeweils lokal durchgeführte Rechteverwaltung erfolgt, wird somit auch dem Prinzip der Datensparsamkeit Folge geleistet. Die Vermeidung redundanter Datensätze trägt auch zur Effektivierung manueller Administrationsaufgaben und zur Steigerung der Performanz bei.

Die folgende Darstellung ist idealisiert, da der beschriebene Ablauf aufgrund der Beschränkungen aktueller FIM-Protokolle in dieser Form noch nicht möglich ist. Als erster Schritt wird die initiale Übernahme der Benutzerdaten über FIM erläutert:

1. Die TUM ist Kunde des LRZ und hat die Art und den Umfang der über Benutzer ausgetauschten Daten sowie deren Standardberechtigungen zur Nutzung der E-Mail-, Fileserver- und Backup-Dienste des LRZ vertraglich fixiert.

2. Neue Mitarbeiter der TUM werden in dem in Szenario 1 beschriebenen I&AM-System der TUM erfasst; sie stimmen dieser Verarbeitung ihrer Daten sowie der Weitergabe ausgewählter Teilmengen davon ans LRZ im Rahmen des Einstellungsverfahrens zu.

3. Einem neuen Mitarbeiter wird von einer lokalen Rechnerbetriebsgruppe ein Arbeitsplatzrechner zur Verfügung gestellt. Der Benutzer kann sich an diesem Rechner mit seiner Kennung-/Passwortkombination einloggen, mit der er auch die übrigen IT-Dienste der TUM nutzen kann.

4. Durch den Loginvorgang findet eine eindeutige Identifizierung und Authentifizierung des Benutzers gegenüber einem Endsystem statt; sofern dieses geeignet an das I&AM-System angebunden ist und ihm diesen Zustand kommuniziert, kann ein Single Sign-On für alle an das I&AM-System angebundenen Dienste erreicht werden.

5. Auf dem Arbeitsplatzrechner sollen automatisch der persönliche Speicherplatz auf dem Fileserver eingebunden und der E-Mail-Client vorkonfiguriert werden. Da die Fileserver- und E-Mail-Dienste vom LRZ betrieben werden, wird die Kennung des Benutzers zusammen mit der Information, dass dieser sich bereits erfolgreich authentifiziert hat, an die entsprechenden Systeme des LRZ übertragen.

6. Die beiden LRZ-Dienste stellen unabhängig voneinander auf Basis der übermittelten Kennung fest, dass es sich um einen neuen Benutzer der TUM handelt, der im I&AM-System des LRZ noch nicht erfasst zu sein scheint und für den noch keine Ressourcen reserviert wurden. Sie stoßen deshalb einen entsprechenden Prozess im I&AM-System des LRZ an.

7. Das LRZ übernimmt die Rolle eines FIM Service Providers und kontaktiert über seine FIM-Komponenten die entsprechenden FIM-Komponenten der TUM, die als Identity Provider fungiert. Die dazu benötigten Metadaten, z. B. Adresse des zuständigen Servers bei der TUM, wurden von einem Administrator des LRZ bereits hinterlegt; die SP- und IDP-Komponenten authentifizieren sich gegenseitig anhand von Serverzertifikaten, die im Rahmen der PKI des Deutschen Forschungsnetzes (DFN) ausgestellt wurden.

8. Alle vom LRZ benötigten Daten werden in Form allgemeiner Attributsauskünfte übermittelt; der Benutzer wird darüber optional in Form eines Hinweisdialogs informiert; da seine Zustimmung bereits vorliegt, muss diese nicht nochmals explizit eingeholt werden.

9. Die Daten werden vom I&AM-System des LRZ auf Vollständigkeit und auf Basis von Plausibilitätsprüfungen auf Korrektheit untersucht und wie folgt weiterverarbeitet:

   - Da aus den Daten hervorgeht, dass es sich um einen Mitarbeiter der TUM handelt, wird die Berechtigung für die Nutzung der E-Mail- und Fileserver-Dienste mit den vertraglich vereinbarten Dienstparametern (z. B. maximal nutzbarer Speicherplatz) erteilt und sein Arbeitsplatzrechner in die Liste der backup-berechtigten Maschinen aufgenommen.
   - Sofern auf Basis eines Korrelationsmechanismus erkannt wird, dass die Person bereits erfasst ist, da sie beispielsweise bereits als Student der LMU Dienste am LRZ genutzt hat, wird kein neuer Datensatz im LRZ I&AM-System angelegt, sondern der bereits vorhandene gegebenenfalls reaktiviert, so dass der Zugriff auf eventuell noch vorhandene Daten und reservierte Ressourcen auch vom TUM-Arbeitsplatz aus möglich wird.
   - Mit der Eintragung ins I&AM-System wird auch automatisch die Konfiguration der Accounting- und Billingsysteme aktualisiert.

- Optional werden der für den neuen Benutzer zuständige Master User über die erfolgreiche Erfassung informiert sowie beliebige weitere Aktivitäten angestoßen.

10. Informationen darüber, für welche Dienste der Benutzer am LRZ freigeschaltet wurde, werden an den IDP übermittelt und stehen damit beispielsweise auch dem Service Desk der TUM zur Verfügung.
11. Der Benutzer kann die Dienste ohne weitere Interaktion sofort nutzen.

Wenn der Benutzer die Dienste beispielsweise auch vom Heimarbeitsplatz aus nutzen möchte, muss er wiederum geeignet authentifiziert werden:

- Im einfachsten Fall wird im Rahmen des Datenaustausches zwischen IDP und SP auch das Benutzerpasswort synchronisiert. Dies birgt jedoch das Risiko, dass von einem kompromittierten oder böswilligen SP aus auch Dienste in der Heimatorganisation des Benutzers missbraucht werden könnten.
- Weiter verbreitet sind Roamingtechniken, bei denen das Passwort nicht lokal beim SP vorgehalten wird, sondern bei jedem Authentifizierungsvorgang zur Verifikation an den IDP übermittelt wird. Auch hierbei tritt jedoch das Problem auf, dass das Passwort beim SP eingegeben werden muss, wo es mitprotokolliert und missbraucht werden könnte. Fortgeschrittene Roamingansätze wie das DFN-Roaming oder eduRoam lösen dieses Problem über verschlüsselte Ende-zu-Ende-Verbindungen vom Gerät des Benutzers bis zum IDP.
- Bei den FIM-Ansätzen ist es am Weitesten verbreitet, dass der Benutzer zur Authentifizierung zum Webportal seines IDPs umgeleitet wird und im Anschluss eine Authentifizierungsbestätigung an den SP übertragen wird.

Bei Modifikationen an Daten ist zu beachten, welche Semantik sie haben und welche Datenquelle dafür autoritativ ist:

- Änderungen an Stamm- und Kontaktdaten werden in der Regel nur von IDP-seitig betriebenen Systemen, z. B. Self Services, durchgeführt. Vom IDP sind sie anschließend an den SP zu kommunizieren, der sie über sein I&AM-System wiederum an die betroffenen Dienste propagiert. Je nach FIM-Protokoll ist ein solcher Push-Mechanismus nicht möglich, so dass der SP die Daten bei Bedarf vom IDP abrufen muss; dieses Pull-Verfahren kann noch dadurch weiter eingeschränkt sein, dass ein Datenabruf nur während der Inanspruchnahme des Dienstes durch den Benutzer möglich ist.
- Veränderungen an den Berechtigungen eines Benutzers sind in der Regel mit einem Genehmigungsprozess verbunden. Beispielsweise könnte der Benutzer über ein Webinterface die Berechtigung zur Nutzung eines weiteren Dienstes beantragen. Diesbezüglich ist zu unterscheiden, ob der Antrag vom SP genehmigt werden muss oder ob diese Aufgabe an Administratoren beim IDP delegiert wurde, wie es beispielsweise in B2B-Outsourcingszenarien häufig vorkommt. Im letzteren Fall kann der beantragte Dienst erst genutzt werden, wenn eine entsprechende Autorisierungsbestätigung vorliegt und der entsprechende Provisioningprozess angestoßen wurde.

Mit dem Ausscheiden des Mitarbeiters an der TUM ist letztlich verbunden, dass ihm auch die am LRZ zugeteilten Berechtigungen wieder entzogen werden oder die Dienste beispielsweise nur noch mit einem für Alumni eingeschränkten Funktionsumfang zur Verfügung stehen. Dieser im FIM-Umfeld als **Deföderation** eines Benutzer bezeichnete Vorgang ist dem SP mitzuteilen, der darauf geeignet reagieren muss:

- Im einfachsten Fall wird die Kennung des Benutzers beim SP mit allen Berechtigungen gelöscht oder die Berechtigungen werden auf die üblicherweise für ehemalige Benutzer vorgesehenen Rechte reduziert; beispielsweise werden vom LRZ betriebene E-Mail-Accounts für TUM-Mitarbeiter auf ihre Weiterleitungsfunktionalität beschränkt, so dass die alte E-Mail-Adresse des Benutzers noch für den Empfang von E-Mails genutzt werden kann, ohne Speicherplatz am LRZ zu belegen.
- Die Kennung wird beim SP vorerst nur gesperrt, so dass die Dienste nicht mehr genutzt werden können. Nach einer Karenzzeit, beispielsweise am Ende der Abrechnungsperiode, wird sie ohne weiteres Zutun des IDP gelöscht; dies betrifft z. B. den Fileserverdienst, so dass das persönliche Homedirectory zwar nicht mehr genutzt werden kann, im Falle eines kurzfristigen Wiedereintritts des Mitarbeiters jedoch noch mit den früheren Inhalten zur Verfügung steht.
- Sofern der Benutzer über ein weiteres Vertragsverhältnis noch zur Nutzung dieser oder anderer Dienste berechtigt ist, darf die Kennung beim SP nicht gesperrt oder gelöscht, sondern nur durch den Entzug von Rechten entsprechend angepasst werden.

Die sich aus diesen Abläufen ergebenden Anforderungen werden im nachfolgenden Abschnitt dargestellt.

2.2.1.4. Anforderungen aus Szenario 3

Aufbauend auf den bereits aus Szenario 1 in Abschnitt 2.1.1.9 abgeleiteten Anforderungen werden die folgenden Ergänzungen und Verfeinerungen gefordert:

Funktionale Anforderungen Da im Szenario lediglich IDP und SP betrachtet wurden, ergeben sich folgende Kriterien bezüglich der Funktionalität einer FIM-Lösung:

- Der SP muss den Abruf von Daten vom IDP initiieren können, d. h. ein reines Push-Verfahren reicht nicht aus [FA-Pull&Push].
- Hinsichtlich der zu übertragenden Daten muss semantisch zwischen Authentifizierungs- und Autorisierungsbestätigungen sowie allgemeinen Attributsauskünften unterschieden werden können [FA-Datenkategorisierung].
- Um die Konsistenz zu gewährleisten, muss der SP Änderungen an den Daten erkennen und diese bei sich aktualisieren können. Das diesbezügliche Verhalten der FIM-Ansätze wird wie folgt differenziert und verfeinert damit die Anforderung [FA-Updates] aus Szenario 1:

1. **Benachrichtigung**: Es ist zu unterscheiden, ob der SP vom IDP automatisch über Änderungen an den Daten informiert wird oder nicht:
   - Im Fall einer Benachrichtigung durch den IDP ist ferner zu unterscheiden, ob nur das Ereignis der Änderung selbst kommuniziert wird (**Invalidierungsnachricht**) oder ob die neuen Datenwerte mitgeliefert werden (**Aktualisierungsnachricht**).
   - Ansonsten muss der SP regelmäßig oder bei Bedarf die Daten erneut abrufen und gegebenenfalls den lokalen Datenbestand aktualisieren.

   Insbesondere Aktualisierungsnachrichten können in Konflikt mit den Datenschutzinteressen des Benutzers stehen.
2. **Offline-Kommunikation**: Diesbezüglich wird unterschieden, ob ein Abruf der Daten nur möglich ist, während der Dienst genutzt wird, oder ob SP und IDP auch kommunizieren können, während der Benutzer offline ist [FA-UserOffline].
   Die Offline-Kommunikation ist auch datenschutzrechtlich zu untersuchen, da der Benutzer beispielsweise nicht interaktiv der Übertragung seiner Daten zustimmen kann.

- Der Benutzer soll aus Datenschutzperspektive optional über die Übertragung seiner Daten informiert werden und bei Bedarf seine Zustimmung oder Ablehnung ausdrücken können. Diese Möglichkeit zur Interaktion wird somit zur funktionalen Anforderung [FA-Interaktion].
- Anforderungen bezüglich selektiven Schreibzugriffs durch den SP auf die beim IDP gespeicherten Daten und die Unterstützung SP-seitiger Korrelationsmechanismen wurden bereits in Szenario 1 erläutert und haben auch hier Gültigkeit.

Ohne exemplarische Erläuterung im Szenario wird die folgende Anforderung festgehalten:

- Der Benutzer sollte seine Berechtigungen temporär und selektiv an einen anderen Benutzer delegieren können, beispielsweise im Rahmen einer Urlaubsvertretung [FA-Delegation]; diese Anforderung unterscheidet sich von der bei Szenario 2 genannten [DSA-Delegation] dadurch, dass die Delegation vom Benutzer selbst und nicht von einem SP angestoßen wird.

Nichtfunktionale technische Anforderungen Aufgrund der Einschränkungen, die eine organisationsübergreifende Kopplung von I&AM-Systemen mittels Konnektoren mit sich bringen würde, werden folgende Anforderungen gestellt:

- Die bei Szenario 1 genannten Anforderungen an die Plattformunabhängigkeit und Skalierbarkeit von FIM-Komponenten gelten auch hier.
- Die Dauer einer FIM-Transaktion sollte deutlich unter der für eine manuelle Erfassung und Pflege der Daten benötigten Zeit liegen. Wie in Kapitel 3 gezeigt wird, ist die Einhaltung dieses scheinbar trivialen Kriteriums aufgrund der Komplexität der FIM-Protokolle bei der Abfrage einzelner Attribute nicht immer gegeben [NFA-Performanz].

Sicherheitsanforderungen Auf der Seite des Identity Providers ergeben sich folgende Anforderungen:

- Die Abfrage von Daten muss auf einen bestimmten Benutzerkreis eingeschränkt werden können, so dass nicht alle im lokalen I&AM-System erfassten Datensätze abgefragt werden können [SEC-Benutzerkreis].
- Die Abfrage von Daten muss auf ausgewählte Attribute eingeschränkt werden können, so dass nicht nur komplette Datensätze und Profile, sondern auch Teilmengen davon übertragen werden können, um z. B. keine rein internen Informationen an externe SPs zu liefern. Dies ergänzt die Datenschutzanforderung [DSA-ARPs] aus Szenario 1 um organisationsseitige Sicherheitsvorgaben, die typischerweise separat administriert werden [SEC-ARPs].
- Die Abfrage der Daten muss auf ausgewählte Service Provider, zu denen ein entsprechendes Vertrauensverhältnis besteht, eingeschränkt werden können. Die Anforderung an das Trust Management besteht deshalb nicht nur auf organisatorischer (vgl. [ORG-Trust] bezüglich der Selektion von IDPs in Szenario 1), sondern auch auf sicherheitstechnischer Ebene; sie umfasst hier insbesondere den konkreten Einbezug gegebener Trust Levels, die ggf. auch vom Benutzer mitbestimmt werden können [SEC-Trust].
- Der Zugriff soll über dedizierte FIM-Komponenten erfolgen, so dass keine direkte Öffnung des I&AM-Systems für Anfragen außerhalb der lokalen Netze notwendig wird. Dies ist eine Verschärfung der Anforderung [SEC-Integration] aus Szenario 1.

Beim Service Provider kommt das folgende Kriterium hinzu:

- Vom IDP durchgeführte Löschoperationen dürfen nicht zu einem automatischen Löschen des Personeneintrags beim SP führen; das Ereignis ist dem SP zwar zu kommunizieren, muss aber beispielsweise in ein Sperren oder verzögertes Löschen beim SP umgewandelt werden können, um Prozesse wie Accounting und Billing geeignet durchführen zu können [SEC-Workflowentkopplung].

FIM-rollenübergreifend existiert darüber hinaus die folgende Anforderung:

- Die Verwaltung und Aktualisierung sicherheitsrelevanter Konfigurationsparameter wie Listen von Föderationsmitgliedern muss durch geeignete Distributionsmechanismen möglichst weitgehend automatisiert werden können, so dass diese Metadaten beispielsweise nur noch an einer zentralen Stelle gepflegt werden müssen [SEC-Metadaten].

Organisatorische Anforderungen Aus organisatorischer Sicht ergeben sich die folgenden Anforderungen:

- Die Anmeldungs- und Registrierungsabläufe sowie die Datenpflege muss beim SP um FIM-basierte Datenübertragung erweitert werden; die FIM-Lösung muss eine dafür geeignete Schnittstelle bieten [ORG-Registrierung].

- Die FIM-Prozesse und -Transaktionen müssen in den übrigen Geschäftsprozessen geeignet berücksichtigt werden:
  - Der Service Desk muss die entsprechenden neuen Fehlerquellen berücksichtigen.
  - Das Change Management muss angepasst werden:
    * Die Abhängigkeiten von externen Datenquellen müssen berücksichtigt werden.
    * Die Verfügbarkeit der Datenquellen und Daten ist zu beachten.
    * Die gegenseitigen Abhängigkeiten von I&AM- und FIM-Komponenten müssen berücksichtigt werden.

  Zur Erfüllung dieser Anforderungen muss die FIM-Lösung entsprechende Schnittstellen zur Verfügung stellen [ORG-Supportprozesse].

Datenschutzanforderungen Die diskutierten Datenschutzaspekte werden in Form der folgenden Kriterien festgehalten:

- Die Basismenge der mittels FIM von einem bestimmten SP über einen Benutzer abrufbaren Daten muss vertraglich geregelt und dem Betroffenen bekannt sein; eine solche Voreinstellung ist notwendig, um große Mengen von Benutzern effizient bewältigen zu können [DSA-DefaultARPs].

- Bei der Übertragung der Daten ist auf die Sicherstellung der Vertraulichkeit, beispielsweise durch Verschlüsselung, zu achten; die Anforderung [SEC-Datenübertragung] wird deshalb auch aus Datenschutzperspektive gestellt.

- Der IDP sollte die informationelle Selbstbestimmung seiner Benutzer unterstützen, indem er darüber Auskunft geben kann, welche Daten bereits an welche SPs übermittelt worden sind. Darüber hinaus muss eine Selbstauskunft beim jeweiligen SP möglich sein. Die in Szenario 2 für UCIM-Systeme gestellte Anforderung [DSA-Selbstbestimmung] ist somit auch im FIM-Umfeld wichtig.

- Für die Verarbeitung der Daten durch Dritte muss eine datenschutzrechtliche Freigabe vorliegen; dies ist geeignet in die organisatorischen Abläufe zu integrieren (vgl. [ORG-Registrierung]).

2.2.2. Szenario 4: Das LRZ in europäischen Grid-Projekten

Neben seiner Rolle als Hochschulrechenzentrum fungiert das LRZ auch als Hochleistungsrechenzentrum und stellt dazu Clustersysteme und Supercomputer zur Verfügung, die nach einem entsprechenden Genehmigungsverfahren landes- bzw. bundesweit genutzt werden können und auf denen für europäische Grid-Projekte Ressourcen reserviert wurden. Dieses Szenario betrachtet die Integration des LRZ in deutsche und europäische Grid Computing Projekte aus Sicht des Identity Managements.

2.2.2.1. Organisatorische und technische Ausgangssituation

Bei Grid-Projekten ergeben sich aufgrund der Zielsetzung, für den globalen Benutzerkreis einen vollständig transparenten Zugriff auf die verteilten Ressourcen und Services zu ermöglichen, gegenüber den bisher betrachteten Szenarien die folgenden Änderungen:

1. Im Rahmen von Grid-Projekten schließen sich mehrere reale Organisationen (ROs) zu einer so genannten **Virtuellen Organisation (VO)** zusammen. Dadurch werden verschiedene Zuständigkeiten von jeder RO an die VO delegiert, so dass die für Identity Management relevanten Geschäftsprozesse der VO berücksichtigt werden müssen.
2. Grid-Projekte setzen zur technischen Virtualisierung der bei jeder RO vorhandenen heterogenen Ressourcen und Dienste so genannte Grid-Middleware ein (siehe Abschnitt 3.7.3), die in der Regel auch für die Verwaltung der Grid-Benutzer zuständig ist. Daraus ergeben sich folgende Komplikationen:
   - Die Grid-Benutzerverwaltung und das lokale I&AM-System müssen integriert werden, beispielsweise durch Personenkorrelation und automatischen Abgleich der Benutzerdatensätze.
   - Da die Hochleistungsrechner des LRZ nicht für Grid-Projekte dediziert sind, sondern auch außerhalb des Grid-Kontextes genutzt werden können, müssen LRZ-Benutzerverwaltung und ggf. mehrere Grid-Middlewares parallel betrieben werden können.
   - Die derzeit in Grid-Projekten angebotenen Dienste sind sehr ressourcennah, da es sich überwiegend um Rechen- und Speicherkapazitäten in Form von CPU-Nutzung und global verteilten Dateisystemen handelt. Die Bereitstellung dieser Dienste durch die Grid-Middleware kann deshalb im Konflikt zu den vom lokalen I&AM-System vorgesehenen Provisioningmechanismen stehen.

Das LRZ nimmt an den Grid-Projekten in der Regel in zwei Rollen teil:

1. Als Service Provider stellt das LRZ reservierte Kontingente an Rechenleistung und Datenspeicher auf seinen Hochleistungsrechnern zur Verfügung.
2. Als Identity Provider ermöglicht das LRZ ausgewählten Wissenschaftlern aus dem MWN den Zugang zu den Grid-Services, die zusammen mit anderen ROs angeboten werden.

Wie in Abschnitt 3.7.3 gezeigt wird, lassen Grid-Projekte prinzipiell zwei Vorgehensweise im Bezug auf Identity Management zu:

1. Die Zusammenfassung mehrerer ROs zu einer VO bildet die organisatorische Basis für die Einführung eines VO-weiten I&AM-Systems. Aus dieser abstrahierten Grid-Perspektive kann somit der organisationsübergreifende Aspekt des Identity Managements vernachlässigt werden. Dieser Ansatz wurde historisch zuerst verfolgt; im nachfolgenden Abschnitt 2.2.2.2 wird anhand des DEISA-Projekts illustriert, welche Probleme damit verbunden sind. Im Allgemeinen führt er dazu, dass das RO-lokale I&AM-System

mit den I&AM-Systemen der Grid-Projekte, an denen die RO beteiligt ist, integriert werden muss. Dabei ergeben sich die in Abschnitt 2.2.1.2 auf Seite 74 diskutierten Schwierigkeiten, die insbesondere die mögliche Dynamik und Skalierbarkeit einschränken.

2. Im Zuge der Dynamisierung von Grid-Projekten, die sich organisatorisch in der Bildung so genannter **Dynamischer Virtueller Organisationen (DVOs)** niederschlägt, setzen Grid-Middlewares vermehrt auf Web Services als Kommunikationsschnittstelle und ermöglichen damit die Nutzung der in Kapitel 3 erörterten FIM-Ansätze zur gridweiten Bereitstellung der Benutzerdaten.

In Bezug auf technische Aspekte des FIM können (D)VOs deshalb mit Föderationen gleichgesetzt werden, wobei beachtet werden muss, dass die organisatorische Kopplung der ROs im Grid-Umfeld wesentlich stärker ist als bei FIM-Föderationen im Allgemeinen.

2.2.2.2. Benutzerverwaltung im Grid-Projekt DEISA

DEISA (Distributed European Infrastructure for Supercomputing Applications)[3] ist ein Zusammenschluss rund eines Dutzends als DEISA-Sites bezeichneter europäischer Hochleistungsrechenzentren, der im Rahmen eines Forschungsprojektes eine für wissenschaftliche Anwendungen geeignete Grid-Infrastruktur aufbauen und betreiben soll. Das als Service Activity 5 (SA5) bezeichnete Teilprojekt befasst sich mit der Bereitstellung der DEISA-weiten Benutzerverwaltung und ihrer Integration in eine gesamtheitliche Securityinfrastruktur.

Wie auch im I&AM-Umfeld üblich werden LDAP-Server als Identity Repositories eingesetzt. Allerdings wird dabei bewusst kein zentraler LDAP-Server eingesetzt, der gegebenenfalls zu jeder DEISA-Site repliziert werden könnte; vielmehr betreibt jede DEISA-Site ihren eigenen LDAP-Server, in den die jeweiligen lokalen Benutzer eingetragen werden können. Damit jede DEISA-Site auch auf die Benutzerdatenbestände der anderen Sites zugreifen kann, wird wie in Abbildung 2.21 dargestellt vom LDAP-Referral-Mechanismus Gebrauch gemacht, bei dem Verweise auf andere LDAP-Server hinterlegt werden können, die von den LDAP-Clients ausgewertet werden müssen. Beispielsweise kann eine von einem Client im MWN gestellte Anfrage nach einem Benutzerobjekt, das zum Barcelona Supercomputing Center gehört, nicht vom DEISA-LDAP-Server des LRZ beantwortet werden; dieser verweist per LDAP-Referral pauschal auf den übergeordneten DEISA-Root-LDAP-Server, der von SARA Computing and Network Services in den Niederlanden betrieben wird. Auch dieser kann die Anfrage nicht beantworten, den LDAP-Client aber an den ihm bekannten DEISA-LDAP-Server in Barcelona verweisen, von dem das Objekt schließlich abgerufen werden kann.

Um DEISA-Kennungen auf den pro Site lokalen Hochleistungsrechnern noch ihrem jeweiligen Ursprung zuordnen zu können, wurde DEISA-weit ein entsprechendes Namensschema festgelegt; beispielsweise müssen alle vom LRZ vergebenen DEISA-Kennungen mit dem Präfix `lrz` beginnen, auf das fünf frei wählbare Buchstaben und Ziffern folgen müssen.

Darüber hinaus müssen für DEISA-Kennungen auch Eigenschaften wie die numerische User-Id für UNIX-Systeme festgelegt werden, die zur Nutzung globaler Filesysteme auf allen Maschinen identisch sein muss; auch hierfür wurden pro DEISA-Site entsprechende Wertebereiche festgelegt, die pro Site lokal verwaltet werden.

[3] `http://www.deisa.org/`

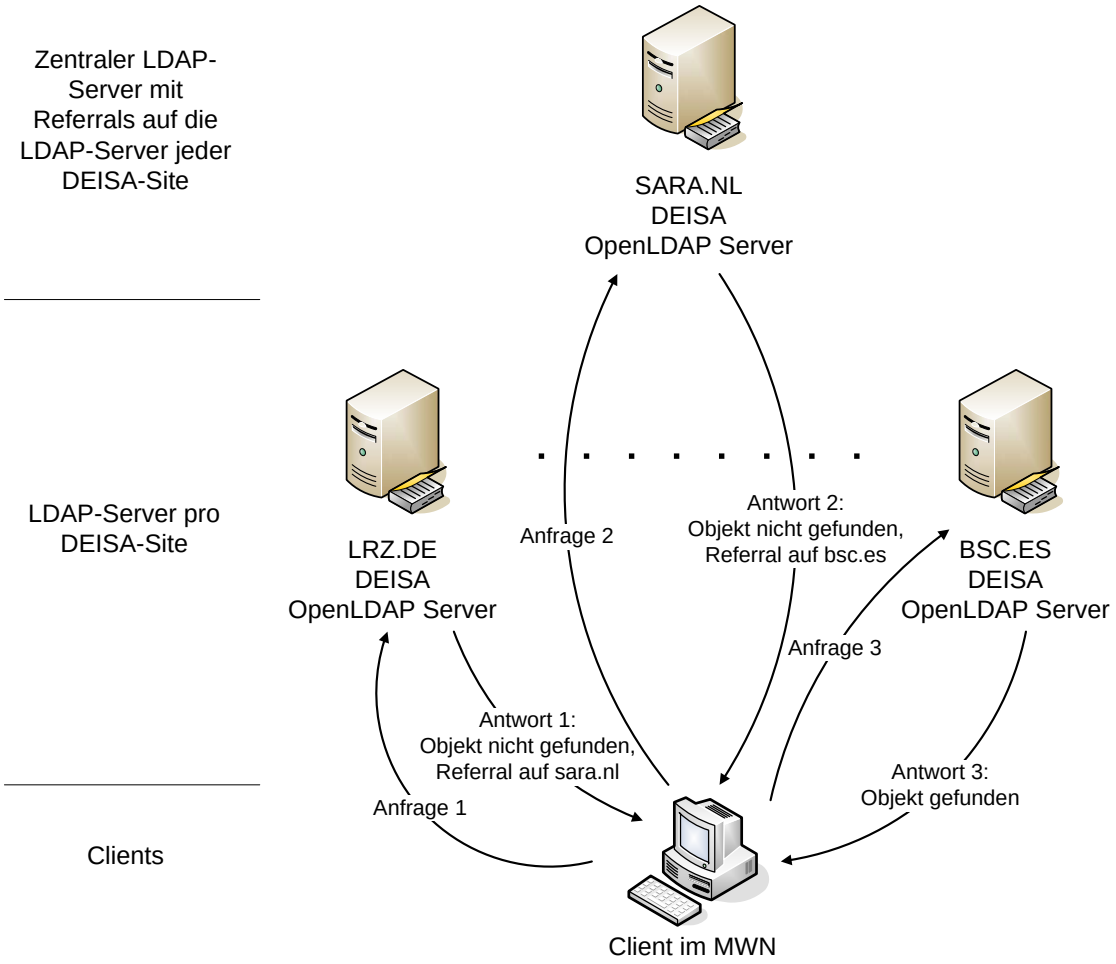


Abbildung 2.21.: Szenario 4: Einsatz des LDAP-Referral-Mechanismus in DEISA

Im Folgenden werden die IM-relevanten Prozesse für das Anlegen neuer Benutzer, das Modifizieren von Kennungen und das Deprovisioning skizziert.

Anlegen von DEISA-Kennungen Kennungen für neue DEISA-Benutzer werden von den Administratoren der zuständigen Site (so genannte Homesite des Benutzers) manuell in deren LDAP-Server eingetragen. Hierzu steht kein dediziertes Managementfrontend zur Verfügung, so dass auf Textdateien, die in den LDAP-Server importiert werden können, oder auf generische graphische LDAP-Editoren zurückgegriffen werden muss, die die Vollständigkeit der eingegebenen Daten und deren Semantik nicht überprüfen können.

Die Eintragung in den LDAP-Server stößt jedoch keine weiteren Aktionen an, so dass der Benutzer mindestens die DEISA-Dienste außerhalb seiner Homesite nicht unmittelbar benutzen kann. Vielmehr werden bei jeder DEISA-Site periodisch, in der Regel einmal pro Tag, Programme ausgeführt, die den über alle Sites verteilten Datenbestand komplett auslesen und auf neue Einträge hin untersuchen.

So ermittelte Kennungen werden in einen für die jeweilige Site spezifischen Workflow eingebracht, der am LRZ aus folgenden Schritten besteht:

1. Die ausgelesenen Daten werden in einer simpel strukturierten Textdatei gespeichert; dieser Mechanismus dient insbesondere als Puffer, wenn der LDAP-Server einer anderen DEISA-Site temporär nicht erreichbar ist.

2. Jeder DEISA-Kennung wird in Form eines 1:1-Mappings eine LRZ-Kennung zugewiesen, die auf den Hochleistungsrechnern des LRZ gültig ist. Dabei muss berücksichtigt werden, dass das entsprechende LRZ-Projekt über einen ausreichend großen Pool an Kennungen verfügt (vgl. Szenario 3). Dieser Schritt ist notwendig, da die im DEISA-Namensraum vergebenen Kennungen derzeit noch nicht auf den LRZ-Hochleistungsrechnern unterstützt werden.

3. Die DEISA-Kennungen werden zudem in die Benutzerdatenbank der Middleware *Unicore* eingetragen; diese Middleware ermöglicht unter anderem einen passwortfreien Zugang zu den Hochleistungsrechnern auf Basis von kryptographischen Clientzertifikaten.

Dem Benutzer stehen die DEISA-Services somit in der Regel nach spätestens 24 Stunden zur Verfügung. Eine explizite Autorisierung für die Nutzung einzelner Systeme ist nicht vorgesehen; es besteht jedoch die – bislang praktisch nicht genutzte – Möglichkeit, dass einzelne Sites ausgewählten Benutzern den Zugang zu den lokalen Systemen entziehen bzw. im Rahmen des sitespezifischen Workflows von Anfang an nicht gewähren.

Modifikation von DEISA-Accounts Änderungen, beispielsweise an den über einen Benutzer erfassten Kontaktinformationen, müssen wiederum manuell von der Administratoren der zuständigen DEISA-Site durchgeführt werden, da es für Benutzer keine Self Services gibt und die LDAP-Server aus Sicherheitsgründen so konfiguriert sind, dass Benutzer selbst keinen Zugriff auf die sie betreffenden LDAP-Objekte haben.

Die so aktualisierten Daten stehen den anderen Sites wiederum zum Abruf zur Verfügung; allerdings werden keine weiteren Aktionen ausgelöst und es wird auch nicht in Form von Metadaten explizit festgehalten, dass das entsprechende LDAP-Objekt verändert wurde. Implizit führen die eingesetzten LDAP-Server ein Attribut `modifyTimestamp`, das Datum und Uhrzeit der letzten Änderung festhält. Da die Systemuhren der LDAP-Server der DEISA-Sites jedoch nicht synchronisiert werden und anhand dieses Attributs nicht unterschieden werden kann, welches Benutzerattribut sich genau geändert hat, führt an einem kompletten Auslesen der Benutzerdatenbestände durch die anderen Sites praktisch kein Weg vorbei.

Deprovisioning in DEISA Im Rahmen des DEISA-Projektes ist vorgesehen, dass die Benutzerdaten nie aus den LDAP-Servern gelöscht werden, sondern nur die Kennungen als deaktiviert gekennzeichnet werden.

Das als Deprovisioning bezeichnete Deaktivieren einer Kennung entspricht einer Modifikation des entsprechenden LDAP-Attributs und wird somit nicht automatisch den anderen Sites kommuniziert. Insbesondere ist kein Prozess spezifiziert, der die Reaktion der Sites auf das Deaktivieren einer Kennung regelt. Es bleibt jeder Site somit selbst überlassen, ob sie die

Kennung auf ihren Systemen sofort sperrt oder löscht, dem Benutzer noch eine frei wählbare Karenzzeit einräumt oder das Deaktivieren schlichtweg ignoriert und dem Benutzer unbefristeten Zugriff auf die lokalen Ressourcen gewährt.

Weiterhin ist nicht vorgesehen, dass eine Kennung von einer anderen DEISA-Site deaktiviert werden kann als von derjenigen, über die sie eingetragen wurde. Im Fall von Missbrauch der Kennung muss somit erst die zuständige Site kontaktiert oder es müssen im Rahmen von DEISA nicht spezifizierte andere Maßnahmen ergriffen werden. Die Kommunikation zwischen den Sites erfolgt per E-Mail, in dringenden Fällen telefonisch; hierfür werden Rufnummernlisten und statische Passwörter zur Authentifizierung der Anrufer gepflegt. Eine IT-Unterstützung dieser Prozesse wird derzeit nicht angestrebt.

2.2.2.3. Defizite der DEISA-Benutzerverwaltung

Während die im vorhergehenden Abschnitt beschriebene DEISA-Benutzerverwaltung für den Einsatz in überschaubaren verteilten Umgebungen durchaus geeignet ist, ergeben sich eine Reihe von Problemen im Hinblick auf die Skalierbarkeit und die Integration mit bereits vorhandenen I&AM-Systemen:

- Mit jedem Hinzukommen oder Ausscheiden bzw. dem Eintreten von Änderungen an der LDAP-Serverkonfiguration einer DEISA-Site müssen alle anderen Sites ihre LDAP-Serverkonfiguration und ggf. auch Firewalls manuell anpassen, damit ein Zugriff von Clients über LDAP-Referrals ermöglicht wird. Die entsprechenden Metadaten werden nicht zentral verwaltet und automatisiert übertragen und bei jeder Site eingespielt, sondern lediglich über eine Mailingliste informell bekanntgegeben. Neben einem hohen Aufwand ist diese Vorgehensweise insbesondere mit Verzögerungen verbunden, so dass die LDAP-basierte Kommunikation mit der die Änderung durchführenden Site temporär nicht möglich ist.

- Für die Administration stehen keine geeigneten Managementwerkzeuge zur Verfügung; das Durchführen von Änderungen an der Serverkonfiguration und das Anlegen neuer Kennungen für Benutzer ist somit fehleranfällig und nicht intuitiv. Dies hat insbesondere Auswirkungen bei weniger routinierten Administratoren, die beispielsweise als Urlaubsvertretung fungieren; da keine Maßnahmen zur Qualitätssicherung definiert sind, pflanzen sich Fehler zu allen anderen Sites fort.

- Das Fehlen von Push-Mechanismen macht es notwendig, dass jede Site periodisch die kompletten Datenbestände aller anderen Sites ausliest, um Änderungen und Neuerungen erkennen zu können:

  - Der Umfang der regelmäßig zu übertragenden Daten und damit der bei jeder Site auf den Hochleistungsrechnern angelegten Kennungen wächst somit proportional zur Anzahl der beteiligten Sites und zur Anzahl der von diesen erfassten Benutzer.
  - Personenbezogene Daten werden von allen DEISA-Sites ausgelesen und eventuell auch außerhalb der LDAP-Serverinfrastruktur gespeichert, ohne dass sichergestellt wird, dass die jeweiligen Benutzer die lokalen Ressourcen auch wirklich in Anspruch nehmen wollen.

- In DEISA ist keine Personenkorrelation vorgesehen. Ein Benutzer kann bei mehreren Sites unabhängig voneinander mehrere Kennungen erhalten und muss dazu jedesmal seine personenbezogenen Daten angeben und eintragen lassen; die im Rahmen der Kontaktinformationen erfassten Vor- und Nachnamen reichen für eine zuverlässige Korrelation mit den lokalen I&AM-Systemen der DEISA-Sites nicht aus; extern vergebene Schlüsselattribute können in den DEISA-LDAP-Servern nicht als Fremdschlüssel hinterlegt werden.
- Durch die Vorgabe eines für jede Site spezifischen Präfixes für die Loginnamen vergebener Kennungen sowie die Reservierung von Wertemengen für numerische User- und Group-Ids kann es zu Inkompatibilitäten und Kollisionen kommen. Insbesondere bei den User-Ids ist es nicht unwahrscheinlich, dass ein für DEISA vereinbarter Bereich von einer Site bereits anderweitig genutzt wird; das Konfliktpotential erhöht sich, wenn mehrere Grid-Projekte ähnliche Vereinbarungen treffen, ohne sich gegenseitig abzusprechen oder eine zentrale Koordinationsinstanz hinzuzuziehen.
- Neu angelegte Kennungen können nicht unmittelbar eingesetzt werden und Änderungen werden nicht sofort bei allen Sites gültig. Da es keine festen Termine gibt, zu denen alle Sites ihre lokalen Datenbestände aktualisieren sollen, kann es insbesondere beim Anlegen von Kennungen dazu kommen, dass sie bei einigen Sites schon genutzt werden können, bei anderen jedoch noch nicht; der Benutzer und auch sein lokaler Administrator können diesen Status jedoch nicht einsehen, sondern der Benutzer wird gegebenenfalls mit technischen Fehlermeldungen konfrontiert, die er nicht richtig interpretieren kann, wenn er die DEISA-spezifischen Abläufe nicht kennt.
- Auch die Supportprozesse sind stark dezentralisiert. Insbesondere gibt es keinen zentralen Anlaufpunkt (Single Point of Contact) für Störungsmeldungen; diese müssen deshalb an den Administrator der Homesite gerichtet und von diesem an den Zuständigen weitergeleitet werden. Jede DEISA-Site ist somit First Level Support für die eigenen Benutzer und Second Level Support für die Benutzer der anderen DEISA Sites.
- Die Vorgehensweise beim Deprovisioning birgt mehrere Gefahren:
  - Die nicht vorgegebene Karenzzeit stellt ein Sicherheitsrisiko dar; insbesondere fehlt ein Mechanismus, mit der eine Kennung sofort gesperrt oder gelöscht werden kann.
  - Nur diejenige Site, die eine Kennung angelegt hat, kann diese auch wieder deaktivieren; für die anderen Sites besteht keine Möglichkeit, die Kennung z. B. aus Sicherheitsgründen mehr als nur lokal zu sperren, d. h. eine zentrale Securitykoordination ist nicht möglich.
  - Die unbegrenzte Dauer der Speicherung auch deaktivierter Kennungen in den LDAP-Servern ist datenschutzrechtlich bedenklich; insbesondere werden dadurch personenbezogene Daten auch solchen Sites zur Verfügung gestellt, die in den DEISA-Verband erst hinzukommen, nachdem die Kennung des Benutzers bereits deaktiviert worden ist.

Während sich einige dieser Schwierigkeiten durch die Spezifikation und Verbesserung der zugrundeliegenden Prozesse beheben lassen würden, verbleiben bei diesem Ansatz generell die Probleme der Integration in die lokalen I&AM-Systeme und der Skalierbarkeit bei wachsender Anzahl teilnehmender Sites und Benutzer.

2.2.2.4. Verbesserungen durch den Einsatz von FIM

Bei DEISA würden sich folgende Vorteile ergeben, wenn statt eines verteilten I&AM-Systems, das parallel zu den I&AM-Systemen der DEISA-Sites betrieben werden muss, auf FIM-Lösungen zurückgegriffen werden würde:

- Benutzerdaten werden vom Identity Provider erst abgerufen, wenn sie von einem Service Provider benötigt werden:
  - Neu angelegte Kennungen sind sofort einsatzbereit.
  - Modifikationen an Kennungen können zeitnah übernommen werden.
  - Das Deaktivieren oder Löschen von Kennungen kann sofort berücksichtigt werden.
  - Personenbezogene Daten werden nur an diejenigen SPs übermittelt, deren Dienste vom Benutzer in Anspruch genommen werden.
- Die Pflege der Metadaten, z. B. die Namen und Adressen der Server der teilnehmenden Sites, wird zentral und automatisiert abgewickelt; somit entfällt das manuelle Durchführen jeder Änderung bei jeder Site.
- Die Autorisierung der dezentral erfassten Benutzer und damit die Möglichkeit, einzelne Kennungen bei Sicherheitsvorfällen temporär zu sperren, kann beliebig verteilt erfolgen, so dass nicht zwingend auf Administratoren der Homesite zurückgegriffen werden muss.
- Fehlermeldungen, beispielsweise bei fehlenden oder inkorrekten Daten, werden dem Benutzer in einer einheitlichen, gridprojekt- und SP-unabhängigen Darstellung vermittelt. Er muss die DEISA-internen Benutzerverwaltungsprozesse somit nicht mehr im Detail kennen.
- Über FIM nutzbare Dienste unterstützen die organisationübergreifende Korrelation von Kennungen, ohne dass sehr systemnahe Parameter wie die User-Id vorgegeben werden müssen. Dadurch können durch Überschneidungen entstehende Konflikte a priori vermieden werden.
- Die Administratoren können auf bereits vorhandene Werkzeuge zum Eintragen und Pflegen der Benutzerdaten zurückgreifen, so dass im lokalen I&AM-System erfasste Anwender nur für die Nutzung der DEISA-Dienste freigeschaltet und nicht erneut erfasst werden müssen.

Die Einbindung einer FIM-Lösung im vorliegenden Szenario hätte die Besonderheit, dass das bereits etablierte, verteilte I&AM-System von ihr abgelöst werden würde. Im Allgemeinen entspricht dies einer Migration von einer proprietären, häufig selbstentwickelten FIM-Lösung zu einer standardbasierten.

2.2.2.5. Anforderungen aus Szenario 4

An eine FIM-Lösung, die in einem solchen Szenario eingesetzt werden kann, und ihre Integration in die vorhandenen I&AM-Systeme werden die folgenden Anforderungen gestellt:

Funktionale Anforderungen Die FIM-Lösung muss die folgenden Funktionalitäten bieten:

- Eine Komponente der FIM-Lösung muss als Konnektor zum lokalen I&AM-System fungieren und die bidirektionale Weitergabe von Änderungen in den Daten übernehmen [FA-Konnektor].
- Die Benutzer und ihre Kennungen müssen gridweit eindeutig identifiziert werden können; der dazu eingesetzte Primärschlüssel sollte jedoch unabhängig von systemnahen Parametern wie der User-Id auf den bereitgestellten lokalen Diensten sein [FA-AccountLinking].
- Es müssen SP-seitig asynchron ablaufende Prozesse wie das Accounting unterstützt und mit aktuellen Daten versorgt werden; dies betrifft die bereits genannte Anforderung [FA-Updates].
- Die Rollendualität einer Organisation, z. B. sowohl IDP als auch SP zu sein, muss unterstützt werden [FA-Rollen].
- IDP-seitig muss die Hinterlegung eventuell für ein Grid-Projekt notwendiger Zusatzdaten unterstützt werden; in DEISA muss beispielsweise die Nationalität jedes Benutzers erfasst werden, die in den lokalen I&AM-Systemen mehrerer teilnehmender Sites bislang nicht berücksichtigt wurde [FA-Zusatzdaten]. Eine Möglichkeit zur Erfüllung dieser Anforderung besteht in der expliziten Unterstützung von Attribute Authorities.
- Providerspezifische interne Abhängigkeiten sollen nicht nach außen sichtbar sein; am LRZ setzt der Zugriff auf im Rahmen von Grid-Projekten zugängliche Maschinen beispielsweise Einträge in den lokalen Authentifizierungs- und Fileservern voraus, die für die anderen Organisationen transparent vorgenommen werden sollen [FA-Abhängigkeiten].

Nichtfunktionale technische Anforderungen Zur Integration ins DEISA-Umfeld sind die folgenden Aspekte zu berücksichtigen:

- Die FIM-Lösung muss mit der im Grid-Projekt eingesetzten Middleware interoperabel sein. Dies impliziert insbesondere, dass Teile der FIM-Funktionalität wie organisationsübergreifendes Single Sign-On an die entsprechenden Module der Grid-Middleware delegiert werden können [NFA-Modularität].
- Die eingesetzte Lösung muss die Teilnahme an verschiedenen Föderationen bzw. Grid-Projekten unterstützen und mit dort eingesetzten anderen FIM-Komponenten koexistieren können [NFA-Koexistenz].
- Das System muss im Hinblick auf Hunderte von teilnehmenden Organisationen und Tausende von Anwendern skalierbar sein; die Vision eines globalen Grids verschärft somit die Anforderung [NFA-Skalierbarkeit] aus Szenario 1.

Sicherheitsanforderungen Im Bezug auf die Integration in vorhandene Netzwerk- und Systemsicherheitsinfrastrukturen ergeben sich die folgenden Anforderungen:

- Unabhängig von lokal gewährten Karenzzeiten müssen sicherheitsbedingte Sperrungen und andere, das Deprovisioning betreffende Benachrichtigungen zeitnah zugestellt werden [SEC-Deprovisioning].
- Es muss für den SP nachverfolgbar sein, woher welche Benutzerdatenbestände gekommen sind [SEC-Auditing].
- Benutzer müssen ausreichend stark authentifiziert werden, bevor sie die Dienste nutzen können und im Grid-Umfeld insbesondere eigenen Programmcode auf den Maschinen des SP ausführen dürfen [SEC-Benutzerauthentifizierung].

Organisatorische Anforderungen Organisatorisch sind mit dem Einsatz von FIM in einem Grid-Projekt folgende Anforderungen verbunden:

- Die Nutzer des Grid-Projekts sollen sowohl auf IDP- als auch auf SP-Seite wie die Nutzer anderer Dienste lokal verwaltet werden können. Die Anforderung [NFA-Management] aus Szenario 1 wird somit um die Aspekte der Dezentralisierung und Delegation erweitert.
- Das organisationsübergreifend zum Austausch der Personeninformationen anzuwendende Datenmodell muss definiert werden. Die technische Anforderung [FA-Schema] wird dadurch um einen wichtigen organisatorischen Aspekt erweitert; zudem muss die FIM-Lösung ggf. neben dem lokalen auch mit einem föderationsspezifischen Datenmodell umgehen können [ORG-Schema].
- Die über FIM bezogenen Daten müssen in die lokalen Prozesse integriert werden können, beispielsweise für Statistiken und Kapazitätsplanungen; hierfür sind entsprechende Schnittstellen notwendig [ORG-Datennutzung].

Datenschutzanforderungen Datenschutz spielt in Grid-Projekten derzeit aufgrund der geringen Anzahl der Teilnehmer und Nutzer eine nur untergeordnete Rolle; bei der angestrebten Realisierung eines globalen Grids mit beliebiger Anzahl von Systemen und Anwendern sind jedoch folgende Anforderungen zu erfüllen:

- Die durch Grid-Middleware geschaffene Transparenz macht es für Benutzer schwieriger, die Verbreitung ihrer personenbezogenen Daten zu kontrollieren. Generell sollte beispielsweise für RO-übergreifende Statistiken und andere Datenauswertungen deshalb eine ausreichend anonymisierte Weitergabe entsprechender Datensätze unterstützt werden [DSA-Anonymisierung].
- SP-spezifische Benutzerrichtlinien, die über die Bedingungen für die allgemeine Teilnahme am Grid-Projekt hinausgehen, müssen dem Benutzer vorab zur Erklärung seines Einverständnisses vorgelegt werden. Am LRZ gilt dies beispielsweise für Compute-Jobs, die einen Schwellwert bezüglich des Umfangs an CPU-Rechenleistung überschreiten. Diese Dynamik muss in der Anforderung [DSA-Zustimmung] berücksichtigt werden.

2.2.3. Szenario 5: Virtuelle Hochschule Bayern (VHB)

Die Virtuelle Hochschule Bayern (VHB) bietet für die Studenten ihrer Trägerhochschulen kostenlose studienvertiefende und -ergänzende E-Learning-Materialien und Online-Kurse an; anderen Personen stehen diese Dienste gegen Bezahlung zur Verfügung.

Für die VHB ergibt sich damit die grundlegende Anforderung, alle Studenten ausgewählter Hochschulen authentifizieren zu können, bevor diesen Zugriff auf die bereitgestellten Ressourcen gewährt wird. Bei der Durchführung von Online-Kursen ist es darüber hinaus notwendig, studienrelevante Informationen über die Benutzer abrufen zu können, beispielsweise deren Haupt- und Nebenfächer; gegebenenfalls müssen Zulassungsvoraussetzungen überprüft werden können, z. B. das Bestehen von an der Hochschule abgehaltenen Prüfungen, eventuell auch deren Zensuren.

Die dabei übertragenen Daten zeichnen sich also durch eine besonders hohe datenschutzrechtliche Sensibilität aus, die sich technisch insbesondere darin niederschlägt, dass einige der entsprechenden Datenfelder in der Regel nicht in den lokalen I&AM-Systemen der Hochschulen (vgl. Szenario 1) vorgehalten werden; somit muss auf zusätzliche Attribute Authorities zurückgegriffen werden.

Ein weiterer wesentlicher technischer Aspekt ist der schreibende Zugriff der VHB auf die an der Heimathochschule der Studenten gespeicherten Profile, beispielsweise um die Ergebnisse von Prüfungen von Online-Kursen in Form von Zensuren oder erreichten Punkten eintragen zu können. Neben anwendungsdomänenspezifischen semantischen Fragestellungen, beispielsweise welche VHB-Kurse in welchem Umfang für welche lokalen Studiengänge einer Trägerhochschule anerkannt werden, ist der schreibende Zugriff von Service Providern auf bei Identity Providern oder Attribute Authorities gespeicherte Daten in vielen FIM-Protokollen noch nicht vorgesehen (vgl. Kapitel 3).

In den folgenden Abschnitten werden die am Szenario beteiligten Entitäten und die technischen Abläufe näher beschrieben.

2.2.3.1. Organisationsstruktur und Architektur aus FIM-Perspektive

Die VHB plant, mittelfristig FIM-Techniken auf Basis von Shibboleth (vgl. Abschnitt 3.3.1) einzusetzen. Das nachfolgend beschriebene Szenario ist deshalb derzeit fiktiv, könnte jedoch langfristig in einer sehr ähnlichen Form realisiert werden.

Wie in Abbildung 2.22 dargestellt ist, sind die folgenden Organisationen am Szenario beteiligt:

- Die VHB selbst nimmt mehrere Rollen ein:
  - Sie stellt als SP eigene Dienste bereit, beispielsweise E-Learning-Materialien und die Plattform zur Durchführung von Online-Prüfungen.
  - Sie verwaltet die Metadaten der VHB-Föderation, d. h. insbesondere die benötigten Serverzertifikate der beteiligten Trägerhochschulen sowie der übrigen Dienstleister. Im Gegensatz zur relativ hohen Fluktuation bei den Benutzern ist die Föderation selbst nahezu statisch, da sich nur selten Änderungen an den beteiligten Organisationen ergeben.

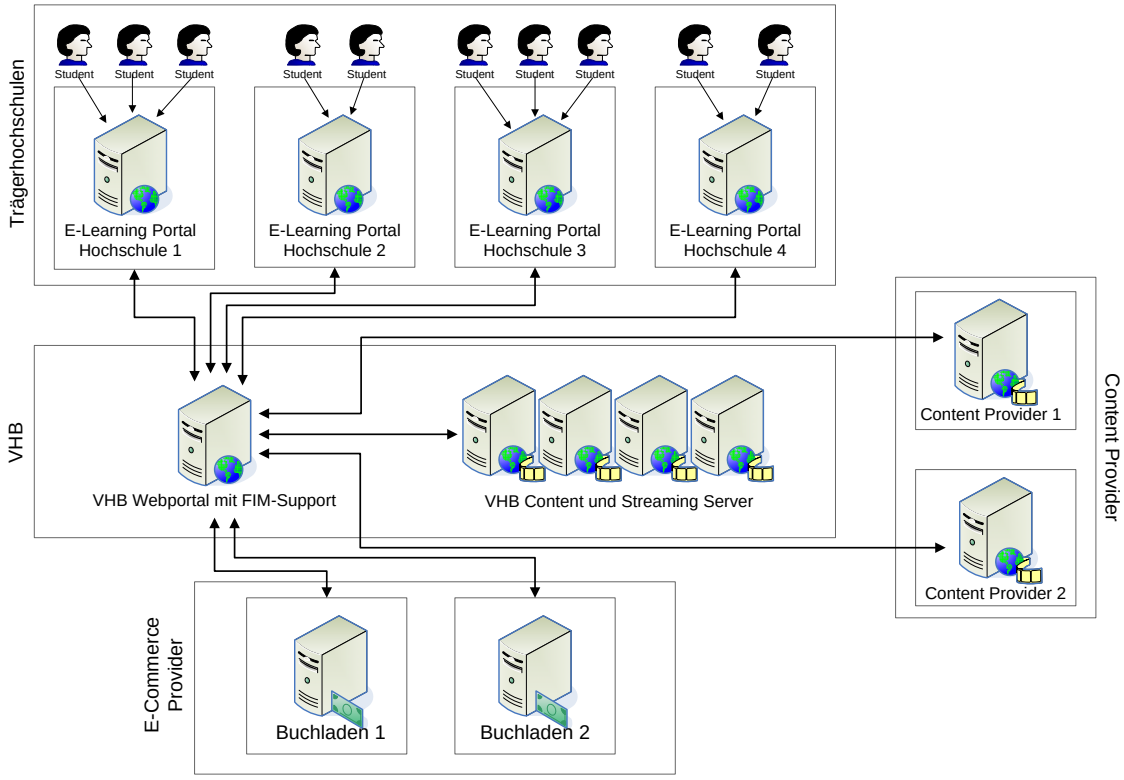


Abbildung 2.22.: Szenario 5: Organisationsstruktur und vertragliche Beziehungen

  - Sie fungiert als AA, beispielsweise wenn gegenüber einem Drittanbieter bestätigt werden soll, dass ein Benutzer aufgrund seiner gewählten Kurse bestimmte Dienste nutzen darf. Die VHB hat somit auch die Funktion eines Brokers, der Benutzer an ausgewählte externe SPs vermittelt.

- Die VHB-Trägerhochschulen fungieren primär als IDPs und AAs für ihre Studenten, so dass diese beispielsweise authentifiziert und die relevanten personen- und studienbezogenen Daten abgerufen werden können.

  Darüber hinaus können Hochschulen, die über eigene E-Learning-Systeme verfügen, diese auch für VHB-Benutzer öffnen und somit als SPs auftreten.

- Kommerzielle Drittanbieter agieren als weitere SPs. Im Folgenden wird vereinfachend zwischen den folgenden beiden Typen unterschieden:

  1. Content Provider bieten analog zur VHB selbst E-Learning-Materialien und Online-Kurse an. Die Nutzung dieser Dienste wird von der VHB vermittelt; insbesondere muss die VHB im Sinne delegierter Autorisierung bestätigen, dass ein Benutzer für den gewählten Dienst berechtigt ist.
  2. E-Commerce Provider: In diesem Szenario wird davon ausgegangen, dass die VHB Verträge mit ausgewählten Online-Buchläden schließt, in denen die Studenten in Analogie zu Hörerscheinen kursrelevante Literatur zu vergünstigten Konditionen

erwerben können. Auch hierfür ist wiederum eine Bestätigung seitens der VHB notwendig, dass ein Benutzer zur entsprechenden Ermäßigung berechtigt ist.

Bei den am Szenario beteiligten Benutzern wird davon ausgegangen, dass sie jeweils genau einer der VHB-Trägerhochschulen als Heimathochschule zugeordnet werden können. Bei Studenten, die parallel an mehr als einer Hochschule immatrikuliert sind, wird davon ausgegangen, dass jede FIM-Transaktion dem Kontext genau einer Hochschule bzw. eines Studiengangs zugeordnet werden kann. Die Verwaltung von externen, zahlungspflichtigen Benutzern wird nachfolgend ohne Beschränkung der Allgemeinheit vernachlässigt: Sofern für diese Benutzer IDPs und AAs bekannt sind, können FIM-Techniken angewandt werden; alternativ ist die Administration über ein VHB-lokales I&AM-System denkbar.

2.2.3.2. Ablauf von FIM-Transaktionen im VHB-Szenario

Nachfolgend wird der FIM-basierte Datenaustausch zwischen den beteiligten Organisationen vorgestellt, wenn ein Student über die VHB an einen Content Provider vermittelt wird und zum belegten Kurs über einen der angebundenen Online-Buchläden vergünstigt Literatur erwerben möchte.

Der erste Workflow behandelt die Anmeldung des Benutzers bei der VHB:

- Der Student ist an einer der VHB-Trägerhochschulen immatrikuliert und interessiert sich für einen Kurs mit einer Online-Abschlussprüfung, deren Ergebnis von seiner Heimathochschule im Rahmen der für ihn relevanten Prüfungsordnung voll anerkannt wird.

  Da er ihre Dienste noch nie genutzt hat, muss sich der Student als erstes initial bei der VHB anmelden. Auf der entsprechenden Webseite der VHB wird er dazu aufgefordert, seine Heimathochschule aus einer Liste aller VHB-Trägerhochschulen auszuwählen und seine Matrikelnummer einzugeben. Auf Basis seiner Angaben wird er zur Webseite seines IDPs weitergeleitet, wo er sich mit seinem Passwort authentisieren muss. Die erfolgreiche Anmeldung wird der VHB in Form einer Authentifizierungsbestätigung durch die Heimathochschule mitgeteilt und der Benutzer wieder auf die Webseiten der VHB umgeleitet.

- Um dem Studenten die für seine Studiengänge in Frage kommenden Kurse anzeigen zu können, benötigt die VHB einige Basisinformationen, u. a. sein Haupt- und Nebenfach. Dazu wird eine entsprechende allgemeine Attributsanfrage gestellt, die IDP-seitig dazu führt, dass der Benutzer gefragt wird, ob er mit der Freigabe dieser Daten einverstanden ist. Der Student gibt sein Einverständnis und die von der VHB angeforderten Daten werden aus dem I&AM-System des IDP ausgelesen und an die VHB übermittelt, die daraufhin eine Liste der für den Studenten verfügbaren Kurse anzeigt.

- Der vom Benutzer gewünschte Kurs setzt voraus, dass dieser bereits einen überdurchschnittlich guten Bachelorabschluss erworben hat. Die VHB stellt eine entsprechende allgemeine Attributsanfrage an den IDP, in dessen lokalem I&AM-System diese Angabe jedoch nicht enthalten ist. An die VHB wird deshalb eine Fehlermeldung zurückgeliefert, die jedoch auch einen Verweis auf eine Attribute Authority enthält, die diese Informationen potentiell bereithält.

- Die VHB wendet sich an die angegebene Attribute Authority, um die Note des Bachelorabschlusses in Erfahrung zu bringen; die AA fragt beim Studenten nach, ob diese Information herausgegeben werden darf und weist ihn auf die damit verbundene Datenschutzproblematik hin.

- Der Student entscheidet sich, der VHB seine Zensur nur unter der Auflage zukommen zu lassen, dass sie lediglich einmalig für die Entscheidung über die Autorisierung zur Teilnahme am gewünschten Kurs verwendet werden darf und dann VHB-seitig umgehend gelöscht werden muss. Für die Teilnahme an weiteren Kursen bedeutet dies, dass diese Information bei Bedarf erneut angefordert werden und den Genehmigungsprozess durchlaufen muss.

Der zweite Workflow beschreibt die reguläre Nutzung des Dienstes:

- Das Abrufen der aktuellen Kursunterlagen setzt voraus, dass sich der Benutzer auf den Webseiten der VHB einloggt; hierzu wird analog zum ersten Schritt des ersten Workflows eine Authentifizierung vom IDP durchgeführt und ihr Erfolg an die VHB als SP kommuniziert.

- Die von der VHB bereitgestellten Materialien können optional durch Videomaterial ergänzt werden, das von einem externen Content Provider angeboten wird. Der Zugriff darauf ist authentifizierten, eingeschriebenen Kursteilnehmern vorbehalten; der Content Provider möchte für die Optimierung seines Angebots auf Basis statistischer Daten ferner wissen, von welcher Heimathochschule der Benutzer kommt. Da der VHB beide Informationen vorliegen, wendet sich der Content Provider mit jeweils einer entsprechenden Autorisierungs- bzw. Attributsanfrage an die VHB, die somit neben ihrer Rolle als SP auch als Authorization Provider und Attribute Authority fungieren soll.

- Die VHB stellt die passende Autorisierungsbestätigung aus; bezüglich der Weitergabe der Hochschulzugehörigkeit zum vom Content Provider angegebenen Zweck wird der Student interaktiv um Genehmigung gefragt. Zudem bestätigt die VHB dem Content Provider, dass sich der Benutzer bereits erfolgreich authentifiziert hat.

- Der Student hat daraufhin Zugriff auf die kursrelevanten Ergänzungsmaterialien. Hierbei ist zu beachten, dass er dem Content Provider zwar nicht namentlich bekannt ist, aber beispielsweise über die IP-Adresse des von ihm verwendeten Rechners oder der Liste der abgerufenen Inhalte eine entsprechende Profilbildung möglich bleibt.

Der dritte Workflow geht auf die Nutzung des Online-Buchladens ein:

- Im Verlauf des Kurses wird dem Studenten vertiefende Literatur empfohlen, zu deren Autoren der Kursleiter gehört. In Analogie zu Hörerscheinen hat die VHB mit einigen Online-Buchläden vereinbart, dass die Teilnehmer der Kurse diese Literatur zu vergünstigten Konditionen erwerben können. Hieraus ergibt sich die grundlegende Notwendigkeit, dass die Benutzer des Online-Buchladens authentifiziert und für den Rabatt autorisiert sind, wobei die VHB entsprechende Authentifizierungs- und Autorisierungsbestätigungen ausstellen kann.

- Für die Kauf- und Lieferungsabwicklung benötigt der Online-Buchladen Informationen wie die vollständige Anschrift und die Bankverbindung des Benutzers, die jedoch auch der VHB nicht vorliegen. Eine entsprechende allgemeine Attributsanfrage wird deshalb mit einer Fehlermeldung und einem Verweis auf den IDP des Benutzers quittiert.
- Der Online-Buchladen stellt die entsprechende Anfrage an den IDP:
  - Da keine dedizierte Lieferanschrift beim IDP hinterlegt ist, schlägt das FIM-System der Heimathochschule dem Studenten vor, seine aktuelle Semesteranschrift dafür zu verwenden und die Freigabe der Daten zu erlauben; der Benutzer nimmt diesen Vorschlag an.
  - Weil der IDP ferner keine Bankverbindung des Benutzers gespeichert hat, fordert er diesen zur Eingabe der entsprechenden Daten auf und schlägt ihm vor, diese Angaben auch im Rahmen einer Einzugsermächtigung für die Semestergebühren zu verwenden. Der Student lehnt diesen Vorschlag jedoch ab, da er auch beim Online-Buchladen lieber per Überweisung nach Rechnungseingang zahlen möchte.

  Somit wird lediglich die Lieferanschrift in Form einer allgemeinen Attributsauskunft an den SP übermittelt.
- Der Online-Buchladen weist den Benutzer darauf hin, dass die für die Bezahlung benötigten Informationen noch nicht vorliegen; ebenso erscheint eine Meldung, dass eine Zahlung per Rechnung für Neukunden nicht möglich ist. Der Student muss deshalb seine Konto- oder Kreditkartendaten manuell auf der Webseite des Online-Buchladens nachtragen, da eine Reparametrisierung des FIM-Workflows nicht unterstützt wird.

Der abschließende vierte Workflow betrifft die Durchführung von Online-Prüfungen:

- Die Prüfung wird von der VHB als SP durchgeführt und setzt eine Authentifizierung des Studenten durch seinen IDP voraus. Die Überprüfung der Autorisierung zur Teilnahme an der Prüfung wird von der VHB intern durchgeführt, beispielsweise auf Basis der während des Kurses eingereichten Hausaufgaben.
- Die erreichte Zensur wird der Heimathochschule von der VHB mitgeteilt; für den entsprechenden schreibenden Zugriff in das Benutzerprofil bei der AA wurde die VHB als SP auf Basis des Vertrags der VHB mit den Trägerhochschulen durch einen AA-seitigen Administrator bereits freigeschaltet. Je nach Prüfungsordnung und Kurs kann dem Studenten die Möglichkeit eingeräumt werden, mitzubestimmen, ob die Prüfungsleistung übernommen oder verworfen wird.

Aus der Beschreibung der vier Workflows wird ersichtlich, dass jeder von ihnen durch FIM essentiell unterstützt wird: Authentifizierungsbestätigungen ermöglichen die für den Benutzer transparente Nutzung verschiedener Dienste nach einmaligem Einloggen, dynamische Autorisierungsbestätigungen lösen ohne FIM zwangsweise statisch zu hinterlegende Zugangsregelungen ab und die allgemeinen Attributsauskünfte ermöglichen eine benutzerkontrollierte Übertragung personenbezogener Daten, ohne dass diese erneut manuell eingepflegt werden müssen.

2.2.3.3. Anforderungen aus Szenario 5

Die funktionalen, nicht-funktionalen technischen und sicherheitsspezifischen Anforderungen decken sich mit den in den Szenarien 1–4 aufgeführten; darüber hinaus ergeben sich die folgenden Ergänzungen:

Organisatorische Anforderungen Die folgenden organisatorischen Anforderungen reflektieren die praktische Notwendigkeit, an mehr als einer Föderation teilnehmen zu können:

- Die Bildung und Verwaltung von Föderationen nach verschiedenen Föderationsmodellen müssen unterstützt werden, da Organisationen an mehreren Föderationen beteiligt sein können; dies muss in der FIM-Lösung geeignet abgebildet werden können [ORG-Föderationsmodelle].
- Die Implementierung der FIM-Lösung und die Teilnahme an einer Föderation müssen mit angemessenem Aufwand realisierbar und betreibbar sein [ORG-Realisierbarkeit].
- Bei IDPs und AAs, die zur Beantwortung von Anfragen auf andere AAs verweisen, zu denen ein SP keine explizite Vertrauensbeziehung hat, müssen Garantien hinsichtlich der Güteparameter übermittelt werden können [ORG-Verweisgüte].

Datenschutzanforderungen Durch die besonders sensiblen Daten und die Schreibzugriffe des SP ergeben sich die folgenden Anforderungen:

- Der Benutzer muss in Abhängigkeit vom Szenario neue personenbezogene Daten, die ein SP z. B. in seine Identität beim IDP eintragen möchte, einsehen und genehmigen können [DSA-Schreibzugriff].
- Freigaben von Datenfeldern an SPs müssen pro SP konfiguriert werden können. Die Freigaben für einen SP gelten nicht transitiv für weitere SPs, an die der Benutzer vermittelt wird oder die der ursprüngliche SP im Rahmen von Delegation oder Dienstabhängigkeiten verwendet. Die Anforderung [DSA-ARPs] wird dadurch verschärft.
- Neben Bedingungen, die über die Übermittlung personenbezogener Daten an einen SP entscheiden, müssen Auflagen unterstützt werden, unter denen der SP die Daten verarbeiten darf [DSA-Obligationen].

2.3. Ergänzung und Gewichtung der FIM-Anforderungen

Die auf Basis der Szenarien ermittelten Anforderungen werden im nachfolgenden Abschnitt um einige weitere ergänzt. Alle Anforderungen werden im Anschluss knapp zusammengefasst und begründet gewichtet, um eine differenzierte Bewertung vornehmen zu können, und schließlich in Abschnitt 2.4 in einer Übersichtstabelle dargestellt.

2.3.1. Ergänzende Anforderungen

Die im Folgenden angegebenen Anforderungen sind für die Bewertung existierender und eigener FIM-Lösungsansätze relevant, aber nicht FIM-spezifisch:

- Die Behandlung von Fehlersituationen muss unterstützt werden; dies betrifft sowohl das Fehlermanagement durch Administratoren beteiligter Organisationen als auch die Darstellung der aufgetretenen Probleme gegenüber dem Benutzer [FA-Fehlermanagement].

- Für die Einführung der Lösung müssen Migrationspfade bzw. Methodiken aufgezeigt werden, die flexibel an die lokalen Gegebenheiten angepasst werden können [ORG-Migration]. Hierzu sind entsprechende Schnittstellen zu existierenden Systemen vorzusehen.

- Konzepte und Produkte müssen angemessen dokumentiert sein [NFA-Dokumentation]; aufgrund der Bestrebung nach Standardisierung und Interoperabilität haben nicht offengelegte Protokolle im FIM-Umfeld nur eine zu vernachlässigende Bedeutung, so dass in der Regel öffentlich zugängliche Dokumentation vorhanden ist. Auf Ausnahmen wird in Kapitel 3 explizit hingewiesen.

Aus dem Forschungsgebiet der Privacy Enhancing Technologies kommt die folgende Anforderungen hinzu, die im Hinblick auf eine möglichst universelle Eignung von FIM-Ansätzen zu berücksichtigen ist:

- Bei pseudonym nutzbaren Diensten sollen IDPs und AAs automatisch für jeden SP unterschiedliche Pseudonyme für denselben Benutzer verwenden, um der Bildung eines gesamtheitlichen Profils durch die unerwünschte Kooperation zwischen SPs vorzubeugen [DSA-Unlinkability]. Analoges gilt für anonym nutzbare Dienste, die beispielsweise nur demographische Daten abrufen möchten (vgl. [WBS+05]).

Abbildung 2.23 zeigt zusammenfassend alle ermittelten Anforderungen und ihre bereichsübergreifenden Abhängigkeiten; von einer nicht erfüllten Anforderung abhängige Anforderungen können nur eingeschränkt erfüllt werden.

2.3.2. Gewichtung der Anforderungen

Im Folgenden werden alle Anforderungen in einer Liste zusammengefasst und die im Rahmen dieser Arbeit vorgenommene Gewichtung der ermittelten Anforderungen vorgestellt und jeweils knapp begründet; die Gewichtung basiert auf den in den Szenarien 1–5 vorgestellten Notwendigkeiten und zielt auf gesamtheitliche, gut nachvollziehbare Bewertung von *FIM-Konzepten* ab. Der resultierende Anforderungskatalog kann deshalb als Basis für die Auswahl vom *FIM-Produkten* dienen, muss dafür jedoch an die szenarienspezifischen Anforderungen angepasst und um weitere Aspekte, z. B. Anschaffungs- und Betriebskosten, erweitert werden.

Jeder Anforderung wird eines der folgenden drei Gewichte zugeordnet:

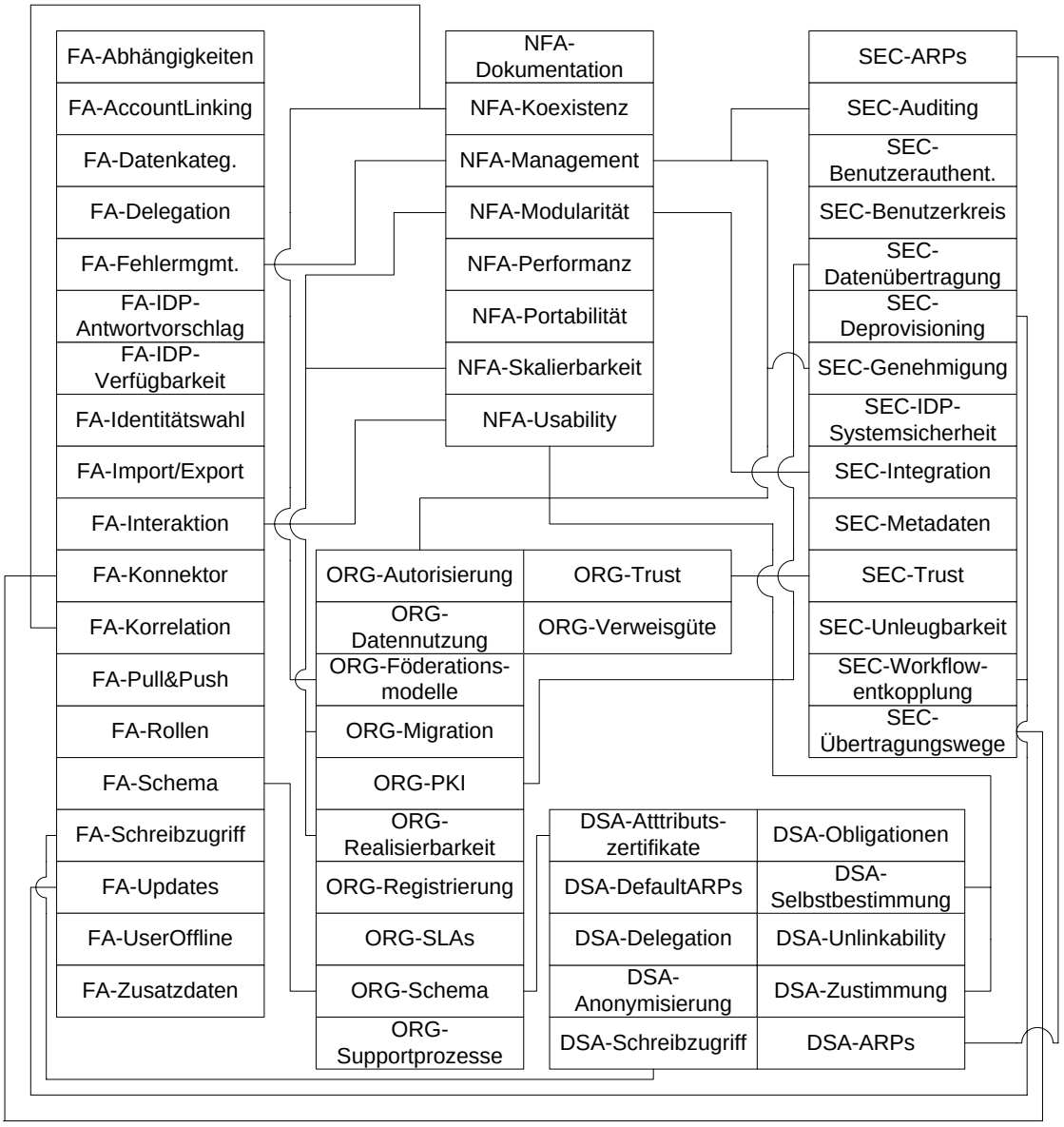


Abbildung 2.23.: Übersicht über die Anforderungen und bereichsübergreifende Abhängigkeiten

- Faktor 1 – **empfehlenswert**: Das Nichterfüllen der Anforderung führt zu szenarienspezifischen Einschränkungen, die im Allgemeinen toleriert werden können, aber zu höheren Realisierungsaufwenden führen – diese Alternativen werden bei so gewichteten Anforderungen kurz skizziert.
- Faktor 2 – **wichtig**: Die allgemeine Eignung eines Ansatzes wird durch Nichterfüllen einer wichtigen Anforderung deutlich beeinträchtigt; ein Konzept, das mehrere wichtige Anforderungen nicht erfüllt, wird gesamtheitlich als praktisch nicht einsetzbar bewertet – der in dieser Arbeit hierfür gewählte Schwellwert liegt bei einem Drittel der wichtigen Anforderungen.
- Faktor 3 – **essentiell**: In diese Kategorie fallen Ausschlusskriterien; ein Konzept, das eine essentielle Anforderung nicht erfüllt, gilt als allgemein ungeeignet für den praktischen Einsatz.

Die *funktionalen Anforderungen* werden wie folgt gewichtet:

- [FA-Abhängigkeiten] – Faktor 1 – empfehlenswert (siehe Seite 89)

  Zusammenfassung: SP-seitige interne Dienstabhängigkeiten sollen nach außen transparent unterstützt werden.

  Begründung der Gewichtung: Falls eine implizite Unterstützung dieser Abhängigkeiten durch die FIM-Lösung fehlt, muss entweder jeder beteiligte Dienst explizit über FIM mit Daten beliefert werden oder eine entsprechende Lösung in den betroffenen Dienst integriert werden.

- [FA-AccountLinking] – Faktor 1 – empfehlenswert (siehe Seite 89)

  Zusammenfassung: Kennungen derselben Person bei unterschiedlichen SPs sollen explizit verknüpft werden können, um herkömmliche verteilte Systeme, die darauf angewiesen sind, unterstützen zu können.

  Begründung der Gewichtung: Die Anforderung betrifft nur Dienste, die die Möglichkeiten des FIM-Kommunikationsmodells nicht ausschöpfen; alternativ muss die Verknüpfung außerhalb der FIM-Lösung durchgeführt werden und kann in Form allgemeiner Attributsauskünfte propagiert werden.

- [FA-Datenkategorisierung] – Faktor 2 – wichtig (siehe Seite 78)

  Zusammenfassung: Die über FIM zu übertragenden Daten sollen mindestens in die Hauptkategorien Authentifizierungs- und Autorisierungsinformationen sowie allgemeine Attributsauskünfte kategorisiert und entsprechend übertragen und ausgewertet werden können.

  Begründung der Gewichtung: Die Unterscheidung ist grundlegend für die Realisierung der beschriebenen FIM-Transaktionen. Da in Abhängigkeit vom Szenario jedoch nicht alle drei Kategorien unbedingt erforderlich sind könnten, ist die Anforderung nicht essentiell.

- [FA-Delegation] – Faktor 1 – empfehlenswert (siehe Seite 79)

Zusammenfassung: Benutzer sollen die Möglichkeit haben, ihre Berechtigungen temporär an andere Personen weiterzugeben; dadurch werden klassische Sicherheitsrisiken wie die Weitergabe von Passwörtern vermieden.

Begründung der Gewichtung: Fehlende Unterstützung für Delegation kann durch administrative Eingriffe kompensiert werden, indem dem Delegationsempfänger die entsprechenden Rechte eingeräumt bzw. wieder entzogen werden.

- [FA-Fehlermanagement] – Faktor 2 – wichtig (siehe Seite 97)

  Zusammenfassung: Die Kommunikation von Fehlerzuständen an Benutzer muss verständlich sein und Administratoren müssen bei der Fehlerbehebung geeignet unterstützt werden.

  Begründung der Gewichtung: Aufgrund der Komplexität der FIM-Kommunikationsvorgänge ist eine klare Diagnose von Fehlern eine grundlegende Voraussetzung für den praktischen Einsatz.

- [FA-IDP-Antwortvorschlag] – Faktor 1 – empfehlenswert (siehe Seite 66)

  Zusammenfassung: Wenn Anfragen eines SPs auf verschiedene Arten beantwortet werden können, da der Benutzer beispielsweise über mehrere Identitäten, parametrisierte Rollen oder Attributszertifikate mit überlappenden Datenmengen verfügt, soll der IDP bei der Zusammenstellung einer passenden Attributsauskunft assistieren.

  Begründung der Gewichtung: Das Erfüllen der Anforderung ermöglicht eine hohe Flexibilität in komplexeren Szenarien, kann jedoch durch einen entsprechenden manuellen Mehraufwand für den Benutzer kompensiert werden.

- [FA-IDP-Verfügbarkeit] – Faktor 2 – wichtig (siehe Seite 67)

  Zusammenfassung: Die Verfügbarkeit der Benutzerinformationen muss gewährleistet werden, insbesondere auch unabhängig von der vom Benutzer eingesetzten Hard- und Software.

  Begründung der Gewichtung: Aus Anwender- und SP-Perspektive wird die Akzeptanz der FIM-Lösung stark von der Verfügbarkeit der Daten beeinflusst.

- [FA-Identitätswahl] – Faktor 1 – empfehlenswert (siehe Seite 66)

  Zusammenfassung: Benutzer sollen die Möglichkeit haben, bei ihrem IDP mehrere Identitäten und Profile verwalten und selektiv einsetzen zu können.

  Begründung der Gewichtung: Durch die Erfüllung dieser Anforderung wird einer unnötig redundanten Speicherung der Basisdaten der Benutzer vorgebeugt. Alternativ kann ein komplexeres Datenmodell in Kombination mit entsprechenden Freigabepolicies eingesetzt werden, das die Speicherung aller benötigten Informationen in einem Datensatz unterstützt; die Pflege der Daten und Policies wird dadurch jedoch deutlich komplexer.

- [FA-Import/Export] – Faktor 1 – empfehlenswert (siehe Seite 66)

  Zusammenfassung: Das Einspielen und Generieren von Attributszertifikaten soll IDP- und AA-seitig unterstützt werden.

Begründung der Gewichtung: Alternativ zu Attributszertifikaten kann die Möglichkeit zur Kommunikation zwischen SPs und AAs genutzt werden; der Einsatz von Attributszertifikaten kann eine FIM-Transaktion jedoch insbesondere dann deutlich vereinfachen, wenn die zuständige AA erst dynamisch ermittelt werden müsste.

- [FA-Interaktion] – Faktor 3 – essentiell (siehe Seite 79)

  Zusammenfassung: Der Benutzer muss mit seinem IDP und ggf. AAs interagieren können, um beispielsweise seine Daten pflegen und der Freigabe seiner Daten für SPs explizit zustimmen zu können.

  Begründung der Gewichtung: Abgesehen von den relativ wenigen Szenarien, in denen Benutzer auf die über sie gespeicherten und übertragenen Daten bewusst keinen Einfluss haben sollen, ist dies die elementarste Anforderung, um datenschutzrechtliche Auflagen zu erfüllen und die Akzeptanz durch die Anwender zu erreichen.

- [FA-Konnektor] – Faktor 2 – wichtig (siehe Seite 89)

  Zusammenfassung: Die organisationsinterne Schnittstelle zwischen FIM-Komponenten und I&AM-System muss eine mit Konnektoren vergleichbare Funktionalität aufweisen.

  Begründung der Gewichtung: Eine nahtlose Integration vom FIM und I&AM ist aufgrund der Charakteristik von I&AM-Systemen nur auf dieser Basis möglich.

- [FA-Korrelation] – Faktor 2 – wichtig (siehe Seite 35)

  Zusammenfassung: Über FIM akquirierte Datensätze müssen mit beim SP bereits vorhandenen Einträgen korreliert werden können, um die redundante Mehrfacherfassung und potentielle Inkonsistenzen zu vermeiden.

  Begründung der Gewichtung: Die Korrelation ist ein wesentliches Ziel von I&AM-Systemen, das in Kombination mit FIM nicht aufgegeben werden darf.

- [FA-Pull&Push] – Faktor 1 – empfehlenswert (siehe Seite 78)

  Zusammenfassung: Der FIM-basierte Datenaustausch soll sowohl IDP- als auch SP-seitig initiiert werden können.

  Begründung der Gewichtung: Das Erfüllen dieser Anforderung trägt zu einer Flexibilisierung von FIM-Abläufen bei und hilft bei der Vermeidung unnötiger Request-Response-Zyklen. Zur Gewährleistung der FIM-Funktionalität würde jedoch ein SP-seitig angestoßenes Pullverfahren ausreichen.

- [FA-Rollen] – Faktor 2 – wichtig (siehe Seite 89)

  Zusammenfassung: Organisationen müssen parallel in mehreren Rollen, z. B. sowohl IDP als auch SP, agieren können.

  Begründung der Gewichtung: Gängige Föderationsmodelle wie Circles of Trust sind explizit auf die Rollendualität IDP/SP ausgelegt; wird sie technisch nicht unterstützt, ist der Aufwand zum Betrieb mehrerer FIM-Instanzen nicht auf eine Organisation beschränkt, sondern führt beispielsweise auch zu höherer Komplexität beim Management der Föderationsmetadaten.

- [FA-Schema] – Faktor 2 – wichtig (siehe Seite 35)

Zusammenfassung: Über FIM akquirierte Daten müssen dem I&AM-System jeder beteiligten Organisation im jeweils lokal benötigten Format vorliegen.

Begründung der Gewichtung: Eine nahtlose Integration von FIM- und I&AM-Systemen ist in heterogenen Föderationen nur möglich, wenn die IDP-seitig bereits vorhandenen Datenbestände genutzt und SP-seitig wie die Bestandsdaten verarbeitet werden können.

- [FA-Schreibzugriff] – Faktor 2 – wichtig (siehe Seite 35)

  Zusammenfassung: SPs sollen selektiv schreibend auf die bei IDPs und AAs gespeicherten Benutzerprofile zugreifen können, um beispielsweise für den IDP relevante Ergebnisse der Dienstnutzung oder Accountingdaten ablegen zu können.

  Begründung der Gewichtung: Der bidirektionale Datenaustausch zwischen IDP und SP ist keine essentielle Anforderung, um die Nutzung von Diensten über FIM zu ermöglichen; ein fehlende Unterstützung für Schreibzugriffe schränkt jedoch das Anwendungsspektrum der FIM-Lösung deutlich ein.

- [FA-Updates] – Faktor 2 – wichtig (siehe Seite 35)

  Zusammenfassung: Änderungen an Benutzerdaten müssen den SPs zeitnah kommuniziert werden.

  Begründung der Gewichtung: Das Erfüllen dieser Anforderung ist ausschlaggebend für die Vermeidung veralteter Daten auf SP-Seite und damit von Inkonsistenzen innerhalb der Föderation.

- [FA-UserOffline] – Faktor 1 – empfehlenswert (siehe Seite 79)

  Zusammenfassung: Auf die bei IDPs und AAs gespeicherten Benutzerdaten soll durch SPs zugegriffen werden können, auch wenn der Benutzer gerade nicht online ist.

  Begründung der Gewichtung: SP-seitig asynchrone Prozesse wie Billing können dadurch flexibilisiert werden; wird die Anforderung nicht erfüllt, kann alternativ ein Abruf aller benötigten Informationen während der Dienstnutzung in Kombination mit [FA-Updates] erfolgen.

- [FA-Zusatzdaten] – Faktor 1 – empfehlenswert (siehe Seite 89)

  Zusammenfassung: Datenquellenseitig sollen föderationsspezifische Datenfelder unterstützt werden.

  Begründung der Gewichtung: Die Bereitstellung der entsprechenden Daten ist im organisatorischen Bereich angesiedelt (vgl. [ORG-Schema]); der Datenbestand von IDPs kann durch AAs ergänzt werden. Fehlt dem FIM-Ansatz die Unterstützung verschiedener Föderationskontexte, muss diese durch entsprechend aufwendigere Datenfreigabepolicies ersetzt werden.

Die *nichtfunktionalen technischen Anforderungen* werden wie folgt gewichtet:

- [NFA-Dokumentation] – Faktor 2 – wichtig (siehe Seite 97)

  Zusammenfassung: Die Spezifikationen des Lösungsansatzes sollen offengelegt und Produkte ausreichend dokumentiert sein.

Begründung der Gewichtung: Präzise Spezifikationen sind Voraussetzung für die interoperable Implementierung durch Softwarehersteller und die effiziente Planung der Umsetzung und den Betrieb durch die Föderationsteilnehmer.

- [NFA-Koexistenz] – Faktor 2 – wichtig (siehe Seite 89)

  Zusammenfassung: Die FIM-Lösung muss mit anderen koexistieren können, da Organisationen an mehreren Föderationen mit unterschiedlichen Realisierungsvarianten beteiligt sein können.

  Begründung der Gewichtung: Die Alternative, für die Teilnahme an jeder Föderation eine eigene Dienstinstanz auf einem dedizierten System anzubieten, ist für viele Dienste nicht praktikabel (vgl. Hochleistungsrechner in Szenario 4) und würde den Einsatz von FIM stark einschränken.

- [NFA-Management] – Faktor 2 – wichtig (siehe Seite 35)

  Zusammenfassung: Existierende Managementinfrastrukturen und -werkzeuge müssen für die Verwaltung FIM-relevanter Benutzerdatenbestände weiterverwendet werden können.

  Begründung der Gewichtung: Der Einführungs- und Betriebsaufwand von FIM würde massiv steigen, wenn lokale und FIM-spezifische Datenbestände getrennt administriert werden müssten.

- [NFA-Modularität] – Faktor 1 – empfehlenswert (siehe Seite 89)

  Zusammenfassung: Die schrittweise Migration soll ermöglicht werden, indem bereits vorhandene Komponenten, die auch von FIM gebotene Teilfunktionalitäten wie Single Sign-On realisieren, weiter genutzt werden können.

  Begründung der Gewichtung: Die Einführung einer FIM-Lösung wird erleichtert, wenn nur die für die gewünschten Funktionalitäten benötigten Komponenten installiert und betrieben werden müssen; der reale Nutzungsumfang der FIM-Möglichkeiten kann und muss jedoch gezielt vom jeweiligen SP gesteuert werden.

- [NFA-Performanz] – Faktor 2 – wichtig (siehe Seite 79)

  Zusammenfassung: Der Ablauf von FIM-Transaktionen soll möglichst performant sein, also beispielsweise nur mit minimalen Verzögerungen bei der Nutzung von Diensten verbunden sein und die Kapazitäten der beteiligten Hardwarekomponenten nicht übermäßig belasten.

  Begründung der Gewichtung: In Kombination mit den Anforderungen [NFA-Skalierbarkeit] und [NFA-Usability] handelt es sich um ein grundlegendes Akzeptanzkriterium für Betreiber und Benutzer; durch die Steigerung der Leistungsfähigkeit der eingesetzten Hardware und die zunehmende Bandbreite der Rechnernetze werden jedoch auch komplexere Transaktionen ermöglicht.

- [NFA-Portabilität] – Faktor 1 – empfehlenswert (siehe Seite 35)

  Zusammenfassung: Die FIM-Lösung soll plattform- und betriebssystemunabhängig sein.

  Begründung der Gewichtung: Das Erfüllen der Anforderung kommt der Integration in bestehende IuK-Infrastrukturen entgegen, ist beim professionellen Einsatz im Umfeld größerer Organisationen jedoch nicht ausschlaggebend.

- [NFA-Skalierbarkeit] – Faktor 3 – essentiell (siehe Seite 35)

  Zusammenfassung: Die Skalierbarkeit einer generischen FIM-Lösung in Hinblick auf die Anzahl beteiligter Organisationen, Dienste und Benutzer darf nicht bereits durch sein Konzept beschränkt sein.

  Begründung der Gewichtung: FIM hat die explizite Zielsetzung, die inhärenten Skalierbarkeitsprobleme herkömmlicher Lösungen wie der direkten Kopplung von I&AM-Systemen zu lösen; die Anwendbarkeit auf komplexe Szenarien mit einer Vielzahl von Teilnehmern ist deshalb von besonderer Bedeutung.

- [NFA-Usability] – Faktor 2 – wichtig (siehe Seite 67)

  Zusammenfassung: Die den Anwendern zur Verfügung gestellten graphischen Bedienoberflächen müssen intuitiv und effizient nutzbar gestaltet werden.

  Begründung der Gewichtung: Aufgrund der Komplexität der FIM-Abläufe und der Sensibilität der dabei übertragenen Daten hängt die Akzeptanz und damit die Verbreitung einer FIM-Lösung wesentlich von ihrer Benutzbarkeit ab.

Die *Sicherheitsanforderungen* werden wie folgt gewichtet:

- [SEC-ARPs] – Faktor 1 – empfehlenswert (siehe Seite 80, vgl. [DSA-ARPs])

  Zusammenfassung: Als IDPs agierende Organisationen benötigen eine policybasierte Möglichkeit zur Steuerung, welche Datenfelder prinzipiell im Rahmen von FIM übertragen werden können.

  Begründung der Gewichtung: Fehlt eine entsprechende Möglichkeit, so müssen herkömmliche Schutzmechanismen für die Identity Repositories, beispielsweise LDAP Access Control Lists, eingesetzt werden, wodurch die Konfiguration deutlich komplexer und aufwendiger wird.

- [SEC-Auditing] – Faktor 2 – wichtig (siehe Seite 90)

  Zusammenfassung: Für einen SP muss nachvollziehbar sein, welche Benutzer von welchen IDPs welche seiner Dienste nutzen.

  Begründung der Gewichtung: Diese Nachverfolgbarkeit ist grundlegend für das Sicherheitskonzept eines SPs und entscheidet über das Spektrum der über FIM praktisch anbietbaren Dienste.

- [SEC-Benutzerauthentifizierung] – Faktor 1 – empfehlenswert (siehe Seite 90)

  Zusammenfassung: IDP-seitig soll die Authentifizierung von Benutzern auf Basis verschiedener, insbesondere auch „starker“ Authentifizierungsmechanismen wie Smartcards und biometrische Verfahren unterstützt werden; der SP soll das zu verwendende Verfahren je nach Schutzbedürfnis des Dienstes vorgeben können. Neben der mit der Authentifizierung verbundenen Single Sign-On Funktionalität soll ein Single Logout ermöglicht werden.

  Begründung der Gewichtung: Sofern eine technische Unterstützung fehlt, muss alternativ auf organisatorischer Basis sichergestellt werden, dass Benutzer IDP-seitig mit dem benötigten Verfahren authentifiziert werden; anstelle eines Single Logout kann wie

bisher üblich ein explizites Abmelden durch den Benutzer bei jedem einzelnen Dienst erfolgen.

- [SEC-Benutzerkreis] – Faktor 1 – empfehlenswert (siehe Seite 80)

  Zusammenfassung: Komplementär zu [SEC-ARPs] (Spezifikation der prinzipiell abrufbaren Attribute von Benutzern) muss der Zugriff auf die für eine Föderation bzw. jeden SP relevante Teilmenge des eigenen Benutzerdatenbestandes eingeschränkt werden können.

  Begründung der Gewichtung: Alternativ und mit höherem Aufwand verbunden können auch hierfür herkömmliche Schutzmechanismen wie LDAP-ACLs eingesetzt werden.

- [SEC-Datenübertragung] – Faktor 3 – essentiell (siehe Seite 36)

  Zusammenfassung: Die *sichere* Datenübertragung unter Gewährleistung von Authentifizierung des Kommunikationspartners sowie der Integrität und Vertraulichkeit der Daten muss gewährleistet werden.

  Begründung der Gewichtung: Aufgrund der Relevanz der übertragenen Daten für den Empfänger und deren Sensibilität sind FIM-Ansätze, die keine sichere Datenübertragung ermöglichen, inakzeptabel.

- [SEC-Deprovisioning] – Faktor 2 – wichtig (siehe Seite 90)

  Zusammenfassung: Informationen über den temporären oder dauerhaften Entzug der Autorisierung zur Nutzung von Diensten müssen zeitnah an SPs kommuniziert werden.

  Begründung der Gewichtung: Insbesondere wenn SP-seitig nicht FIM-fähige Dienste zur Verfügung gestellt werden, die nicht bei jeder Nutzung überprüfen können, ob der Benutzer noch Mitglied seiner ursprünglichen Heimatorganisation ist, spielen Benachrichtigungen dieser Art eine wesentliche Rolle.

- [SEC-Genehmigung] – Faktor 1 – empfehlenswert (siehe Seite 36)

  Zusammenfassung: Über FIM eingehende Dienstnutzungsanträge sollen dieselben optionalen Genehmigungsprozesse durchlaufen können wie herkömmlich akquirierte.

  Begründung der Gewichtung: Für eine nahtlose Integration von FIM in das vorhandene Dienstportfolio ist die Erfüllung dieser Anforderung anzustreben; alternativ müssen entsprechende Voraussetzungen auf organisatorischer Ebene geschaffen werden oder entsprechende Teilprozesse zum IDP ausgelagert werden.

- [SEC-IDP-Systemsicherheit] – Faktor 2 – wichtig (siehe Seite 67)

  Zusammenfassung: Die IDP-Komponenten stellen aufgrund der über sie beziehbaren Daten ein besonders interessantes Angriffsziel dar, das entsprechend geschützt werden muss.

  Begründung der Gewichtung: Dem Schutz der FIM-Datenquellen kommt dieselbe Bedeutung zu wie dem Schutz von Quellsystemen für I&AM-Systeme und deren Identity Repositories. FIM-lösungsspezifische Konzepte zur Positionierung und Absicherung von IDP-Komponenten sind deshalb von grundlegender Bedeutung.

- [SEC-Integration] – Faktor 2 – wichtig (siehe Seite 36)

Zusammenfassung: Alle FIM-Komponenten müssen in existierende Netzwerksicherheitsinfrastrukturen integriert werden können; hierzu gehören auch Konzepte zur Vorbeugung netzwerk- bzw. FIM-protokollspezifischer Angriffsarten.

Begründung der Gewichtung: Die Einführung und der Betrieb einer FIM-Lösung sind aus Perspektive des Security Managements nur dann effizient realisierbar, wenn diese Bedingung erfüllt wird.

- [SEC-Metadaten] – Faktor 2 – wichtig (siehe Seite 80)

  Zusammenfassung: Föderationsmetadaten müssen zentral gepflegt und unter Sicherstellung ihrer Integrität zu den Föderationsteilnehmern übertragen und dort möglichst weitgehend automatisiert ausgerollt werden können.

  Begründung der Gewichtung: Bei größeren Föderationen kann eine Verwaltung der Metadaten nicht mehr effizient dezentral bei jedem Föderationsteilnehmer durchgeführt werden; Inkonsistenzen in den Metadaten würden darüber hinaus die Fehlersuche massiv erschweren.

- [SEC-Trust] – Faktor 1 – empfehlenswert (siehe Seite 80)

  Zusammenfassung: Die Datenübertragung muss auf vertrauenswürdige, autorisierte Kommunikationspartner eingeschränkt werden können.

  Begründung der Gewichtung: Alternativ muss eine Einschränkung der Kommunikationspfade über herkömmliche Netzwerksecuritykomponenten wie Firewalls realisiert werden.

- [SEC-Unleugbarkeit] – Faktor 1 – empfehlenswert (siehe Seite 36)

  Zusammenfassung: Personen dürfen die tatsächliche Nutzung von Diensten über FIM nicht erfolgreich nachträglich abstreiten können.

  Begründung der Gewichtung: Fehlt eine explizite Unterstützung durch die FIM-Lösung, muss auf entsprechende herkömmliche Verfahren zurückgegriffen werden; beispielsweise könnte auf stärkere Authentifizierung Wert gelegt werden (vgl. [SEC-Benutzerauthentifizierung]).

- [SEC-Workflowentkopplung] – Faktor 1 – empfehlenswert (siehe Seite 80)

  Zusammenfassung: Workflows von IDP und SP sollen voneinander entkoppelt ablaufen können; dadurch soll sichergestellt werden, dass asynchrone Prozesse wie Accounting und Billing nicht beeinträchtigt werden.

  Begründung der Gewichtung: Erzwingt die FIM-Lösung eine starke Kopplung der Datenbestände und verhindert damit, dass dem SP die Daten eines Benutzers auch nach seinem Ausscheiden beim IDP noch zur Verfügung stehen, müssen zusätzliche SP-seitige Puffermechanismen umgesetzt werden.

- [SEC-Übertragungswege] – Faktor 1 – empfehlenswert (siehe Seite 68)

  Zusammenfassung: Es soll die Möglichkeit geben, zwischen einer direkten Datenübertragung zwischen IDP und SP bzw. einer mittelbaren Kommunikation über den Benutzerclient zu wählen.

Begründung der Gewichtung: Das Erfüllen dieser Anforderung ermöglicht flexiblere Kommunikationsabläufe, ist jedoch keine zwingende Voraussetzung für die Nutzung der FIM-Funktionalität.

Die *organisatorischen Anforderungen* werden wie folgt gewichtet:

- [ORG-Autorisierung] – Faktor 2 – wichtig (siehe Seite 37)

  Zusammenfassung: Auf organisatorischer Ebene getroffene Vereinbarung zum Aufbau einer dezentralen Autorisierungsinfrastruktur müssen abgebildet werden können.

  Begründung der Gewichtung: Die verteilte Speicherung und Auswertung von Autorisierungsinformationen ist ein unmittelbarer Mehrwert der FIM-basierten Datenübertragung und maßgeblich für den FIM-Einsatz beispielsweise in B2B- und Outsourcingszenarien.

- [ORG-Datennutzung] – Faktor 2 – wichtig (siehe Seite 90)

  Zusammenfassung: Die Nutzung der über FIM bezogenen Daten im Rahmen weiterer SP-seitiger Prozesse neben der Speisung des eigentlichen Dienstes, beispielsweise im Rahmen von Kapazitätsplanungen, ist eine Voraussetzung für eine vollständige Integration in die vorhandene Infrastruktur.

  Begründung der Gewichtung: Die Anforderung ist nicht essentiell für die Nutzung der FIM-Funktionalität im Rahmen der Diensterbringung, aber wichtig für die Integration der FIM-Lösung in die Geschäftsprozesse des SPs.

- [ORG-Föderationsmodelle] – Faktor 2 – wichtig (siehe Seite 96)

  Zusammenfassung: Es müssen verschiedene Föderationsmodelle unterstützt werden, mit denen die vertraglichen Beziehungen zwischen den Föderationsteilnehmern abgebildet werden können.

  Begründung der Gewichtung: Die FIM-Lösung muss flexibel genug sein, um entsprechende organisatorische Vorgaben zu erfüllen, da die technische Lösung andernfalls nicht die Realität reflektiert; sie ist für die Nutzung von bilateralen FIM-Kommunikationsabläufen jedoch nicht essentiell.

- [ORG-Migration] – Faktor 2 – wichtig (siehe Seite 97)

  Zusammenfassung: Für die Umsetzung der FIM-Lösung müssen flexible Migrationspfade aufgezeigt werden.

  Begründung der Gewichtung: Die Einführung einer FIM-Lösung hängt stark von einem lösungsspezifischen Migrationskonzept ab.

- [ORG-PKI] – Faktor 2 – wichtig (siehe Seite 68)

  Zusammenfassung: Die Verifizierung elektronisch signierter Daten wird in der Praxis fast ausschließlich auf Basis asymmetrischer Verschlüsselungsverfahren umgesetzt, die durch eine Public-Key Infrastruktur gemanagt und von der FIM-Lösung unterstützt werden müssen.

  Begründung der Gewichtung: Für Föderationen, die nur wenige Teilnehmer haben oder auf signierte Daten bewusst verzichten können, sind einfachere Alternativen, z. B. über

symmetrische Verschlüsselung mit vorherigem Austausch des Schlüssels zwischen den Organisationen, denkbar; in sehr heterogenen Föderationen kann die Schaffung einer gemeinsamen PKI zu aufwendig sein. Im Allgemeinen sollten vorhandene PKIs jedoch auf jeden Fall genutzt werden können.

- [ORG-Realisierbarkeit] – Faktor 3 – essentiell (siehe Seite 96)

  Zusammenfassung: Der Aufwand für Realisierung und Betrieb muss angemessen sein.

  Begründung der Gewichtung: Lösungen, die zu komplex sind oder nur sehr schwer an szenarienspezifische Anforderungen angepasst werden können, sind praktisch irrelevant.

- [ORG-Registrierung] – Faktor 2 – wichtig (siehe Seite 80)

  Zusammenfassung: Die FIM-basierte Datenakquisition muss in die SP-seitig vorhandenen Benutzerregistrierungsprozesse integriert werden können, z.B. durch die Einspeisung der Daten in die dafür bereits vorgesehenen Verarbeitungsprozesse.

  Begründung der Gewichtung: Ein Nichterfüllen dieser Anforderung verhindert eine nahtlose Integration von FIM-Prozessen in die bestehenden Abläufe beim SP und würde den dauerhaften Betrieb zweier Verfahren mit demselben Ziel erforderlich machen.

- [ORG-SLAs] – Faktor 2 – wichtig (siehe Seite 37)

  Zusammenfassung: Für die Föderation müssen Dienstgüteparameter vereinbart werden können, deren Einhaltung überwacht werden kann.

  Begründung der Gewichtung: In vielen Szenarien, in denen der Einsatz von FIM technische Vorteile bietet, wird auf die explizite vertragliche Vereinbarung verzichtet und der Dienst bestmöglich ohne weiterführende Garantien erbracht. Sofern SLAs aber vorhanden sind, müssen sie abgebildet werden können.

- [ORG-Schema] – Faktor 2 – wichtig (siehe Seite 90)

  Zusammenfassung: Im Zusammenspiel mit der funktionalen Anforderung, die Daten im benötigten Format bereitzustellen [FA-Schema], ergibt sich die Notwendigkeit eines föderationsweit gemeinsamen Verständnisses der ausgetauschten Daten.

  Begründung der Gewichtung: Die Komplexität dieser Anforderung variiert stark mit der Heterogenität der Föderationsteilnehmer und dem Umfang der zu übertragenden Daten; während sie in homogenen Föderationen, bei denen jeder Teilnehmer bereits dasselbe Datenmodell verwendet, implizit erfüllt ist, kann ihre Nichterfüllung die Nutzung von FIM in heterogenen Szenarien massiv einschränken. Im Allgemeinen muss die Verwendung eines föderationsspezifischen Datenmodells unterstützt werden.

- [ORG-Supportprozesse] – Faktor 2 – wichtig (siehe Seite 81)

  Zusammenfassung: Die FIM-Prozesse müssen in die IT Service Support Prozesse nahtlos integriert werden können.

  Begründung der Gewichtung: Eine Verfehlung dieser Anforderung hätte große Auswirkungen auf den Dienstbetrieb bei IDPs und SPs; die Anforderung kann jedoch nicht alleine von der FIM-Lösung erfüllt werden, sondern erfordert auch entsprechende Flexibilität bei den bereits bestehenden Prozessen.

- [ORG-Trust] – Faktor 1 – empfehlenswert (siehe Seite 36)

  Zusammenfassung: Der Grad des Vertrauens zwischen Föderationsteilnehmern muss individuell bestimmt und in der FIM-Lösung abgebildet werden können.

  Begründung der Gewichtung: Die Alternative, zweckgebundene Föderationen mit einheitlichen Vertrauensbeziehungen zu gründen, ist derzeit in der Praxis vorherrschend. Um einer Bildung unnötig vieler Föderationen mit einem hohen Überlappungsgrad der teilnehmenden Organisationen vorzubeugen, sollte der FIM-Lösungsansatz diese Parametrisierung unterstützen.

- [ORG-Verweisgüte] – Faktor 1 – empfehlenswert (siehe Seite 96)

  Zusammenfassung: Wenn IDPs zur Beantwortung einer Anfrage auf AAs verweisen, sollen Garantien bezüglich der zwischen SP und IDP vereinbarten Güteparameter kommuniziert werden können.

  Begründung der Gewichtung: Die Anforderung ist nur relevant, wenn die AA kein explizites Mitglied der Föderation ist, so dass entsprechende SLAs bereits vereinbart wurden. In der Praxis tritt dieser Fall selten auf, ermöglicht jedoch die flexiblere Bereitstellung von zuverlässigen Daten.

Die *Datenschutzanforderungen* werden wie folgt gewichtet:

- [DSA-ARPs] – Faktor 3 – essentiell (siehe Seite 37)

  Zusammenfassung: Benutzer müssen im Rahmen so genannter Attribute Release Policies kontrollieren können, welche Informationen über sie an welche SPs übermittelt werden.

  Begründung der Gewichtung: Die Kontrolle des Benutzers über seine Daten ist die grundlegendste, gesetzlich verankerte Datenschutzanforderung. Diese Anforderung geht deutlich über [SEC-Benutzerkreis] und [SEC-ARPs] hinaus und es stehen keine Alternativen zur Verfügung.

- [DSA-Anonymisierung] – Faktor 1 – empfehlenswert (siehe Seite 90)

  Zusammenfassung: Daten, die über Benutzer z. B. für statistische Auswertungen weitergegeben oder -verwendet werden, sollen ausreichend anonymisiert werden.

  Begründung der Gewichtung: Die Nutzung von FIM für diesen Zweck stellt einen Spezialfall der Kombination von Attribute Release Policies [DSA-ARPs] mit Datenkonvertierungen [FA-Schema] dar; in einer universell einsetzbaren FIM-Lösung sollte dieser Anwendungsfall explizit unterstützt werden, ansonsten ist auf herkömmliche Methoden zurückzugreifen.

- [DSA-Attributszertifikate] – Faktor 1 – empfehlenswert (siehe Seite 68)

  Zusammenfassung: Der Einsatz von Attributszertifikaten ermöglicht die Lieferung der von einer AA signierten Daten an einen SP, ohne dass die AA implizit davon erfährt und beispielsweise mitprotokollieren kann, welche SPs ein Benutzer verwendet.

  Begründung der Gewichtung: Der Vorteil für den Benutzer ist bei geeigneten Datenschutzvereinbarungen mit den beteiligten AAs marginal und mit dem höheren Aufwand für die Akquisition und Pflege seiner Attributszertifikate verbunden; die Akzeptanz der

FIM-Lösung durch besonders datenschutzsensible Benutzer kann damit jedoch deutlich erhöht werden.

- [DSA-DefaultARPs] – Faktor 2 – wichtig (siehe Seite 81)

  Zusammenfassung: Administratoren von FIM-Datenquellen müssen Voreinstellungen für Attribute Release Policies vorgeben können. Beispielsweise müssen Vereinbarungen zu Datenfreigaben, die mit neuen Mitarbeitern im Rahmen ihrer Einstellung getroffen werden, vorkonfiguriert werden können; dadurch können Benutzer, die sich mit ARPs nicht befassen möchten, schneller die benötigten Dienste nutzen, ohne dass ihre Schutzinteressen verletzt werden.

  Begründung der Gewichtung: Voreinstellungen, die für möglichst alle davon Betroffenen geeignet sind, sind zum effizienten Umgang mit großen Benutzermengen wichtig.

- [DSA-Delegation] – Faktor 1 – empfehlenswert (siehe Seite 68)

  Zusammenfassung: Die Weitergabe von personenbezogenen Daten durch SPs an Dritte muss vom Benutzer gesteuert werden können, indem entsprechende Policies zusammen mit den Daten übermittelt werden.

  Begründung der Gewichtung: Eine Alternative für SPs, die zur Erbringung des Dienstes auf weitere *externe* Dienste angewiesen sind, besteht in der expliziten Vereinbarung von Attribute Release Policies bei diesen; die Möglichkeit, diese im Rahmen der ursprünglichen Datenübermittlung an den SP mitführen zu können, ermöglicht ein effizientes und umfassendes zentrales ARP-Management durch den Benutzer.

- [DSA-Obligationen] – Faktor 1 – empfehlenswert (siehe Seite 96)

  Zusammenfassung: An die Übermittlung von Daten an einen SP sollen Auflagen an die *interne* Weiterverarbeitung geknüpft werden können, beispielsweise dass sie 90 Tage, nachdem sie nicht mehr benötigt werden, gelöscht werden müssen.

  Begründung der Gewichtung: Analog zu [DSA-Delegation] und in der Praxis vorherrschend ist es alternativ möglich, dass der Benutzer entsprechende Vereinbarungen direkt mit dem SP trifft; das Erfüllen der Anforderung ermöglicht jedoch ein effizientes ARP-Management beim IDP und vermeidet die unnötige Herausgabe von Daten, wenn die Auflagen nicht erfüllt werden können.

- [DSA-Schreibzugriff] – Faktor 2 – wichtig (siehe Seite 96)

  Zusammenfassung: Einträge, die ein SP in den Datensatz des Benutzers beim IDP eintragen möchte, sollen vom Benutzer kontrolliert und genehmigt werden können.

  Begründung der Gewichtung: Gesetzliche Datenschutzrichtlinie sehen vor, dass Personen die über sie gespeicherten Daten einsehen und falsche Angaben korrigieren können müssen. Durch den Genehmigungsprozess werden diese Auflagen unterstützt und der Verarbeitung falscher Daten vorgebeugt.

- [DSA-Selbstbestimmung] – Faktor 1 – empfehlenswert (siehe Seite 68)

  Zusammenfassung: Der IDP soll das Recht zur informationellen Selbstbestimmung des Benutzers unterstützen können, indem er *optional* mitprotokolliert, welche Daten bereits an welche SPs übermittelt worden sind, so dass sich der Benutzer einfach einen Überblick beschaffen kann.

Begründung der Gewichtung: Je nach Szenario kann das Mitprotokollieren durch den IDP auch explizit unerwünscht sein; alternativ muss sich der Benutzer mit seinem Auskunftsersuchen direkt an jeden SP wenden.

- [DSA-Unlinkability] – Faktor 1 – empfehlenswert (siehe Seite 97)

  Zusammenfassung: Bei anonymer oder pseudonymer Dienstnutzung soll der IDP die Verwendung unterschiedlicher technischer Bezeichner für dieselbe Person unterstützen, um Korrelationen durch böswillige, kooperierende SPs zu verhindern. Bei anonymer Dienstnutzung steht diese Anforderung im Konflikt mit der Anforderung [FA-Korrelation], die auf eine SP-interne Korrelation von Benutzerdatensätzen abzielt.

  Begründung der Gewichtung: Diese Anforderung ist für Szenarien wichtig, in denen primär Authentifizierungs- und Autorisierungsinformationen, aber keine oder nur weniger Personendaten transportiert werden sollen. Da sich bei der Erfüllung dieser Anforderung, die sich durch die explizite Übertragung anderer Identifikationsmerkmale kompensieren lässt, keine negativen Konsequenzen ergeben, sollte diese Eigenschaft generell angestrebt werden.

- [DSA-Zustimmung] – Faktor 1 – empfehlenswert (siehe Seite 37)

  Zusammenfassung: Anwender müssen den Benutzungsrichtlinien über FIM genutzter Dienste explizit zustimmen können.

  Begründung der Gewichtung: Sofern dieser Vorgang nicht in die FIM-Transaktionen integriert ist, muss er alternativ SP-seitig vor der ersten Nutzung des Dienstes nachgeholt werden.

2.4. Anforderungskatalog

Die nachfolgende Tabelle fasst alle Anforderungen und ihre Gewichtung zusammen und dient als Anforderungskatalog in den weiteren Kapiteln.

Funktionale Anforderungen			
[FA-Abhängigkeiten]	1	[FA-Konnektor]	2
[FA-AccountLinking]	1	[FA-Korrelation]	2
[FA-Datenkategorisierung]	2	[FA-Pull&Push]	1
[FA-Delegation]	1	[FA-Rollen]	2
[FA-Fehlermanagement]	2	[FA-Schema]	2
[FA-IDP-Antwortvorschlag]	1	[FA-Schreibzugriff]	2
[FA-IDP-Verfügbarkeit]	2	[FA-Updates]	2
[FA-Identitätswahl]	1	[FA-UserOffline]	1
[FA-Import/Export]	1	[FA-Zusatzdaten]	1
[FA-Interaktion]	3		

Nichtfunktionale Anforderungen			
[NFA-Dokumentation]	2	[NFA-Performanz]	2
[NFA-Koexistenz]	2	[NFA-Portabilität]	1
[NFA-Management]	2	[NFA-Skalierbarkeit]	3
[NFA-Modularität]	1	[NFA-Usability]	2
Sicherheitsanforderungen			
[SEC-ARPs]	1	[SEC-IDP-Systemsicherheit]	2
[SEC-Auditing]	2	[SEC-Integration]	2
[SEC-Benutzerauthentifizierung]	1	[SEC-Metadaten]	2
[SEC-Benutzerkreis]	1	[SEC-Trust]	1
[SEC-Datenübertragung]	3	[SEC-Unleugbarkeit]	1
[SEC-Deprovisioning]	2	[SEC-Workflowentkopplung]	1
[SEC-Genehmigung]	1	[SEC-Übertragungswege]	1
Organisatorische Anforderungen			
[ORG-Autorisierung]	2	[ORG-Registrierung]	2
[ORG-Datennutzung]	2	[ORG-SLAs]	2
[ORG-Föderationsmodelle]	2	[ORG-Schema]	2
[ORG-Migration]	2	[ORG-Supportprozesse]	2
[ORG-PKI]	2	[ORG-Trust]	1
[ORG-Realisierbarkeit]	3	[ORG-Verweisgüte]	1
Datenschutzanforderungen			
[DSA-ARPs]	3	[DSA-Obligationen]	1
[DSA-Anonymisierung]	1	[DSA-Schreibzugriff]	2
[DSA-Attributszertifikate]	1	[DSA-Selbstbestimmung]	1
[DSA-DefaultARPs]	2	[DSA-Unlinkability]	1
[DSA-Delegation]	1	[DSA-Zustimmung]	1

Somit existieren 5 essentielle und 30 wichtige Anforderungen, die für Bewertung von FIM-Ansätzen besonders relevant sind.

Kapitel 3.

Status Quo des Federated Identity Managements

Inhalt dieses Kapitels

In diesem Kapitel werden existierende FIM-Konzepte und -Lösungen aus Industrie und Forschung kurz vorgestellt und ihre jeweiligen Stärken sowie Defizite anhand des in Kapitel 2 aufgestellten Anforderungskatalogs analysiert, um ihren potentiellen Beitrag zu dem ab Kapitel 4 entwickelten Lösungsansatz beurteilen zu können. Nach einem sehr knappen Überblick über die historische Entwicklung von FIM-Ansätzen in Abschnitt 3.1 werden die aktuellen Industriestandards in Abschnitt 3.2 erläutert; sie bilden einerseits die Grundlage, auf denen einige der in Abschnitt 3.3 vorgestellten Forschungsansätze aufbauen und wurden andererseits im Rahmen von zum Teil frei verfügbaren Softwareprodukten umgesetzt. Eine Auswahl davon wird in Abschnitt 3.4 skizziert, da Open Source Implementierungen wiederum die Basis eigener im Rahmen dieser Arbeit durchgeführten Entwicklungen darstellen.

In den Abschnitten 3.5 bis 3.8 wird vertiefend auf weitere Standards und Forschungsansätze zu den Themen Privacy Management, Federated User Provisioning und Interoperabilität heterogener Informationsmodelle eingegangen; sie bilden die Ausgangsbasis für die in Kapitel 5 vorgestellten Werkzeugkonzepte, wodurch die verhältnismäßig umfangreiche Darstellung in diesem Kapitel begründet wird.

Ein Überblick über die relevanten UCIM-Entwicklungen und eine zusammenfassende Bewertung der vorgestellten Konzepte schließen dieses Kapitel ab, dessen Vorgehensmodell in Abbildung 3.1 zusammenfassend dargestellt ist.

3.1. Historische Entwicklung

Der Bedarf, Mitarbeitern und Kunden von Partnerorganisationen Zugriff auf eigene Dienste zu gewähren, existierte selbstverständlich bereits lange bevor sich Begriffe und Konzepte rund um das Identity Management gebildet hatten. Im Folgenden wird die historische Entwicklung hin zum heutigen Federated Identity Management skizziert:

1. Die einfachste und auch derzeit noch am Weitesten verbreitete Lösung war, externe Personen manuell in die lokalen Benutzerverwaltungssysteme aufzunehmen. Die entsprechenden Datensätze wurden geeignet gekennzeichnet, um sie von organisationsinternen Identitäten unterscheiden zu können; häufig wurde bereits eine Unterscheidungsmöglichkeit anhand des vergebenen Benutzernamens oder der ggf. damit assoziierten E-Mail-Adressen vorgesehen (z. B. `name@`*`partner.`*`example.com`). Offensichtlich erhöht sich damit der Aufwand durch die mehrfache Erfassung und Pflege der Daten bei jeder beteiligten Organisation; zudem können – wie in Szenario 3 erläutert – Inkonsistenzen auftreten, wenn die Daten nicht in jedem Identity Repository zeitnah aktualisiert werden.

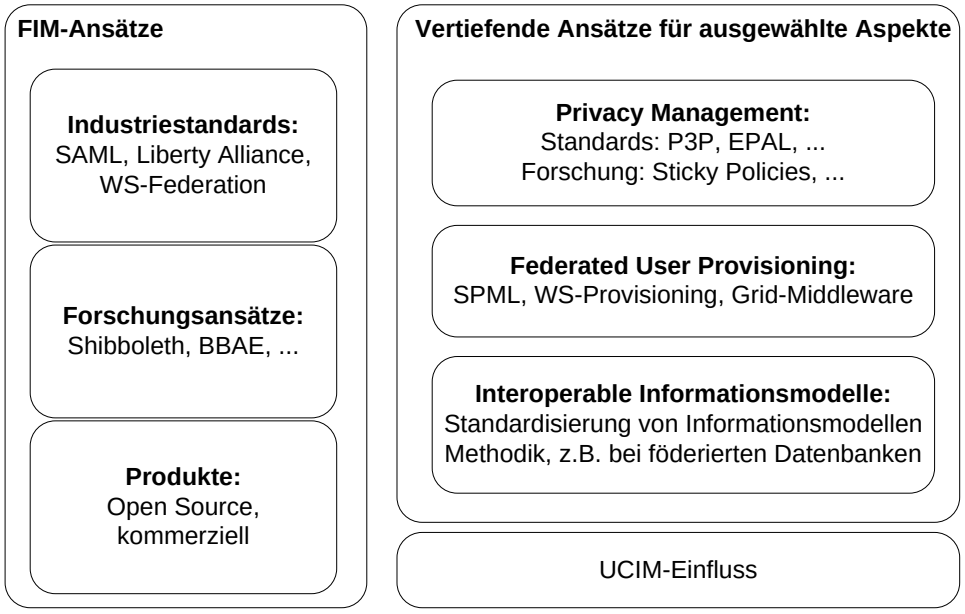


Abbildung 3.1.: Überblick über die analysierten relevanten Arbeiten

2. Mit der Einführung von I&AM-Systemen lag es nahe, diese über Konnektoren organisationsübergreifend zu koppeln. Dieser Ansatz ermöglicht eine weitgehende Automatisierung, ist jedoch mit den in Abschnitt 2.2.1.2 auf Seite 74 beschriebenen Nachteilen behaftet; je nach Umfang der anzubietenden Dienste und Anzahl der Kunden stellt er allerdings aufgrund der Defizite aktueller FIM-Lösungen noch die beste Möglichkeit dar.

3. In Ergänzung zum unter Punkt 1 genannten Verfahren können alternativ zur Kopplung von I&AM-Systemen auch Abbildungstabellen zwischen den jeweils lokalen Identitäten der beteiligten Organisationen oder zwischen den lokalen und den globalen Identitäten der Benutzer gepflegt werden. Dieser Ansatz ist nach wie vor im Grid-Umfeld aktuell, in dem so genannte Mappingfiles eingesetzt werden, in denen jedem Grid-Benutzer eine lokale Identität zugeordnet wird. Offensichtlich entsteht dadurch ein noch höherer Verwaltungsaufwand und die Dienste müssen mit dieser Form der Verknüpfung umgehen können; bei Grids ist dies Aufgabe der Middleware (siehe Abschnitt 3.7.3).

4. Mit den Sprachen **S2ML** (Security Services Markup Language) und **AuthXML** wurden im Jahr 2000 zwei konkurrierende, nicht interoperable Lösungs- und Standardisierungsvorschläge geschaffen. Während S2ML Authentifizierungsbestätigungen und Attributsauskünfte unterstützte, konnte AuthXML für Authentifizierungs- und Autorisierungsbestätigungen eingesetzt werden. Auf Druck von Softwareherstellern wurde ein Gremium zur Vereinheitlichung beider Ansätze einberufen, dessen Ergebnis die erste Version des heute vorherrschenden, unten beschriebenen Standards SAML war.

Parallel zu dieser Entwicklung im Identity Management gab es in diversen anderen Bereichen Bemühungen zur organisationsübergreifenden Integration von Diensten, die in dieser Arbeit

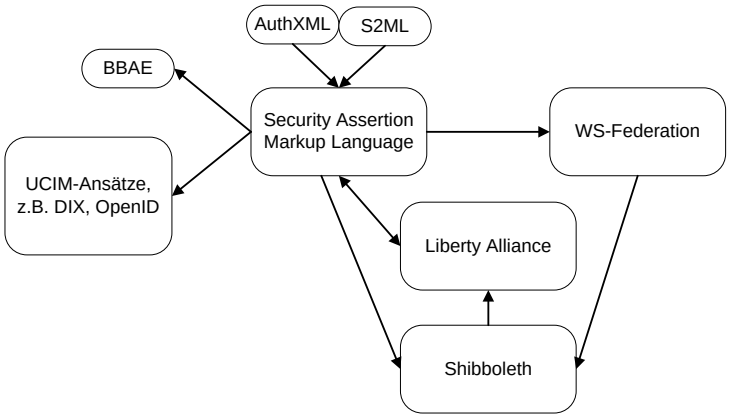


Abbildung 3.2.: Direkte gegenseitige Einflüsse der FIM- und UCIM-Ansätze

nicht näher untersucht werden; zu berücksichtigen ist jedoch das Aufkommen so genannter **Webportale**, deren Schwerpunkt zwar generell in der Bereitstellung von *Content Management Systemen* (CMS) liegt, die aber stark dazu beigetragen haben, dass verschiedenste Dienste wie E-Mail, Gruppenkalender und Dateizugriff unter einer gemeinsamen Oberfläche nach einmaliger Authentifizierung genutzt werden können. Bei diesen webbasierten Diensten zeichnet sich deshalb auch eine besonders hohe Aktivität hinsichtlich der Anpassung an FIM-Standards ab.

3.2. FIM-Industriestandards

Mit der Security Assertion Markup Language, den Spezifikationen der Liberty Alliance und WS-Federation werden in diesem Abschnitt die drei FIM-Industriestandards vorgestellt und anhand des in Kapitel 2 definierten Kriterienkatalogs bewertet.

Da die Liberty Alliance Spezifikationen ursprünglich auf SAML 1.0 basierten und diverse Erweiterungen inzwischen auch in SAML 2.0 eingeflossen sind, müssen sich FIM-Softwarehersteller derzeit in der Regel zwischen einer SAML- bzw. WS-Federation-basierten Lösung entscheiden oder beide Varianten unterstützen. Auch hier findet eine erste Annäherung beider Standards statt, da WS-Federation inzwischen das zentrale Datenelement von SAML, die so genannte SAML Assertion, unterstützt; inwieweit davon in der Praxis Gebrauch gemacht werden wird, muss sich jedoch noch zeigen. Die gegenseitige Einflussnahme der in diesem Kapitel vorgestellten Ansätze ist in Abbildung 3.2 veranschaulicht und wird in den entsprechenden Abschnitten beschrieben.

3.2.1. OASIS Security Assertion Markup Language (SAML)

OASIS (Organization for the Advancement of Structured Information Standards, `http://www.oasis-open.org/`) ist ein internationales Konsortium mit über 600 Mitgliedern,

das sich der Entwicklung und Umsetzung von E-Business Standards widmet. Die Security Assertion Markup Language (SAML) wird vom OASIS Security Services Technical Committee spezifiziert, das von Vertretern im IM-Umfeld namhafter Hersteller wie Sun, RSA, BMC und Bea geleitet wird.

SAML 1.0 wurde 2001 entwickelt und 2002 zum OASIS Standard ernannt; im Jahr 2003 wurde SAML 1.1 freigegeben und enthielt im Wesentlichen Fehlerkorrekturen gegenüber Version 1.0. Die derzeit aktuelle Version 2.0 wurde von der zwischenzeitlichen Weiterentwicklung durch die Liberty Alliance motiviert und ist seit März 2005 ein OASIS Standard. Weiterführende Aktivitäten bestehen in der kontinuierlichen Korrektur der formalen Spezifikationen und der Bereitstellung zusätzlicher Dokumentation.

3.2.1.1. Funktionsumfang und zugrundeliegende Spezifikationen von SAML

SAML unterstützt die Übertragung von Authentifizierungs- und Autorisierungsbestätigungen sowie allgemeinen Attributsauskünften, die als *authentication assertions*, *authorization assertions* und *attribute assertions* bezeichnet werden. Der Aufbau dieser XML-basierten **SAML Assertions** wird im Rahmen eines *Informationsmodells* syntaktisch und semantisch spezifiziert, wobei die möglichen Inhalte allgemeiner Attributsauskünfte nicht eingeschränkt oder spezifiziert werden, so dass sich die Teilnehmer SAML-basierter Föderationen auf ein geeignetes Informationsmodell einigen müssen [S2CORE]. Die Semantik von authentifizierungsrelevanten Daten, z. B. die Angabe der Methode, mit der ein Benutzer authentifiziert wurde (Passwort, Smartcard, ...), wird in einem separaten Dokument beschrieben [S2AUTH].

Das nachfolgende Codebeispiel ist an [S2OVER] angelehnt und zeigt die folgenden Elemente:[1]

- Allgemeine Attributsauskunft: Die E-Mail-Adresse des Benutzers wird übermittelt (Zeilen 5–9).
- Authentifizierungsbestätigung: Der Benutzer wurde erfolgreich mittels Passwort authentifiziert (Zeilen 14–20).
- Metadaten: Es werden der Ausstellungszeitpunkt und Aussteller angegeben (Zeilen 1-4) und Gültigkeitszeitraum der gesamten Assertion eingeschränkt (Zeilen 10–13).

```
1  <saml:Assertion Version="2.0" IssueInstant="2007-01-31T12:00:00Z">
2    <saml:Issuer Format=entity>
3      http://idp.lrz-muenchen.de
4    </saml:Issuer>
5    <saml:Subject>
6      <saml:NameID Format="emailAddress">
7        wolfgang.hommel@lrz-muenchen.de
8      </saml:NameID>
9   </saml:Subject>
10  <saml:Conditions
11     NotBefore="2007-01-31T12:00:00Z"
12     NotOnOrAfter="2007-01-31T12:10:00Z">
13  </saml:Conditions>
14  <saml:AuthnStatement AuthnInstant="2007-01-31T12:00:00Z" SessionIndex="12345">
15    <saml:AuthnContext>
16      <saml:AuthnContextClassRef>
17        SAML:2.0:PasswordProtectedTransport
18      </saml:AuthnContextClassRef>
19    </saml:AuthnContext>
20  </saml:AuthnStatement>
21 </saml:Assertion>
```

[1] Zur besseren Lesbarkeit wird in diesem Kapitel auf die Angabe der jeweils vollständigen XML-Namespaces verzichtet.

Aufbauend auf diesem Datenformat wird das *Kommunikationsmodell* in Form von **Request-Response-Protokollen** spezifiziert, die beispielsweise zur Einholung allgemeiner Attributsauskünfte verwendet werden können und somit eine Client-Server-Architektur vorgeben. Diese Protokolle sind abstrakt, d. h. ohne Angabe der darunterliegenden Transportschicht, spezifiziert und werden durch die **SAML Bindings** mit Standardprotokollen wie HTTP und SOAP, die wiederum TCP/IP-basiert sind, verknüpft [S2BIND]. Das *Funktionsmodell* von SAML umfasst seit Version 2.0 neben Single Sign-On auch Single Logout und neben dem *IDP first Use Case* auch den *SP first Use Case* (vgl. Abschnitt 2.1.2.7).[2]

Als **SAML Profil** wird die für ein konkretes Szenario gewählte Kombination aus zu verwendenden SAML Assertions, Protokollen und Bindings bezeichnet.

Neben dem durch den SP initiierten Datenabruf wird auch eine vom IDP angestoßene Datenübertragung unterstützt. Obwohl eine direkte Kommunikation zwischen IDP und SP im Rahmen des *Assertion Query/Request Profiles* unterstützt wird, tendiert SAML stark zu einer mittelbaren Kommunikation über den Client des Benutzers, bei der – wie in Abschnitt 2.1.2.7 beschrieben – reger Gebrauch von der Funktionalität des Protokolls HTTP, insbesondere der HTTP-Redirects, gemacht wird.

Bei der über den Client mittelbaren Kommunikation werden zwei Varianten unterschieden: Unter Verwendung von **SAML Artifacts** werden die zu übertragenden Nachrichten in URLs kodiert abgelegt, so dass der Client eine Webseite des SP aufruft und die Nachricht als in der Adresse des Dienstes abgelegten Parameter mitgibt (dies entspricht der Verwendung der Methode „GET“ des HTTP-Protokolls). Problematisch erweist sich hierbei die Längenbegrenzung für URLs in den weit verbreiteten Webbrowsern, insbesondere bei mobilen Endgeräten mit knapper Speicherkapazität. Aus diesem Grund wurde das **HTTP POST** Binding entwickelt, das Nachrichten theoretisch beliebiger Länge an den Server des SP so übergibt, wie üblicherweise umfangreiche ausgefüllte HTML-Formulare übertragen werden. In beiden Fällen kann der Benutzer nicht unmittelbar erkennen, welche Daten übertragen werden, auch wenn diese nicht verschlüsselt sind.

3.2.1.2. Organisatorische Aspekte und Datenschutz in SAML

Das *Organisationsmodell* von SAML sah in Version 1.x lediglich IDPs und SPs vor, die als *Asserting Party* bzw. *Relying Party* bezeichnet wurden. Mit der Anlehnung an die Liberty Alliance in Version 2.0 wurden die Begriffe IDP und SP eingeführt und Attribute Authorities unterstützt.

SAML 2.0 orientiert sich bezüglich der möglichen Föderations- und Trustmodelle stark an der Liberty Alliance; die 2005 herausgegebenen *SAML Trust Model Guidelines* [S2TRST] sind inhaltlich identisch mit den 2004 von der Liberty Alliance veröffentlichten, auf die in Abschnitt 3.2.2.3 eingegangen wird.

Die Verwaltung von Metadaten, auf deren Basis IDPs und SPs die zur Kommunikation notwendigen Daten wie Server und zu verwendende Kommunikationsprotokolle ermitteln können, wird in einem separaten Dokument beschrieben [S2META]. Ihre Umsetzung in einem föderationsweiten Kontext ist am Beispiel von Shibboleth gut zu erkennen (siehe Abschnitt 3.3.1).

[2] Der *SP first Use Case* wurde von mehreren Herstellern bereits für SAML 1.x implementiert und in Revisionen der SAML 1.1 Spezifikation erwähnt; das *Identity Provider Discovery Profile* ist jedoch erst seit Version 2.0 im Standard enthalten.

Auch im Hinblick auf Security und Datenschutz erfolgt eine starke Anlehnung an die Liberty Alliance; ein nicht zum offiziellen Standard gehörendes Dokument geht auf grundlegende Datenschutzprinzipien und einige mögliche Angriffsszenarien ein [S2PRIV]. Während für SAML 1.0 sicherheitsspezifische Schwachstellen gefunden wurden [Gro03], sind in SAML 2.0 bislang keine inhärenten Sicherheitslücken bekannt.[3]

Um die Konformität einer SAML-Implementierung mit der Standardspezifikation verifizieren zu können, gibt OASIS entsprechende *Conformance Requirements* vor [S2CONF].

3.2.1.3. Bewertung von SAML

Bei der Beurteilung von SAML ist die Intention von OASIS zu berücksichtigen, eine möglichst flexible technische Basis für den FIM-basierten Datenaustausch, jedoch keine allumfassende FIM-Lösung schaffen zu wollen.

Bezüglich der im Anforderungskatalog genannten *essentiellen* Anforderungen treten bei SAML deshalb folgende Einschränkungen auf:

- Die Notwendigkeit zur Interaktion mit dem Benutzer ([FA-Interaktion]) wird lediglich in nicht zur Standardspezifikation gehörenden Dokumenten erwähnt, aber nicht näher ausgeführt.
- Analog sind benutzergesteuerte Datenfreigaben ([DSA-ARPs]) keine zwingende Voraussetzung für SAML-Konformität; die unzureichende, lediglich informelle Empfehlung von OASIS bezüglich Datenschutzaspekten ist, dass „[vendors] *should attempt to address them in their implementations*“ (aus: [S2PRIV, Kap. 2]).

Aus diesen beiden Defiziten folgt, dass auch die *wichtigen* Anforderungen [NFA-Usability], [DSA-DefaultARPs] und [DSA-Schreibzugriff] nicht unterstützt werden.

Da die Integration von SAML in bestehende I&AM-Systeme nicht beschrieben wird, sind die ebenfalls *wichtigen* Anforderungen [FA-Konnektor], [FA-Korrelation], [FA-Schema], [NFA-Management], [ORG-Migration], [ORG-Registrierung], [ORG-SLAs] und [ORG-Supportprozesse] nicht erfüllt.

Zudem unterstützt SAML nur den Abruf, aber nicht das Schreiben von Daten, und keine Datenaktualisierungsnachrichten an SPs, so dass die *wichtigen* Anforderungen [FA-Schreibzugriff] und [FA-Updates] nicht erfüllt werden und ein deutliches funktionales Defizit darstellen.

Die ebenfalls *wichtigen* Sicherheitsanforderungen [SEC-Auditing], [SEC-IDP-Systemsicherheit] und [SEC-Integration] werden nicht durch die Spezifikation abgedeckt. Die Umsetzung der Anforderung [ORG-Datennutzung] ist nur möglich, wenn alle hierfür benötigten Dienste explizit über SAML gespeist werden.

Von den *empfehlenswerten* Anforderungen werden [FA-Pull&Push], [NFA-Modularität], [NFA-Portabilität], [SEC-Benutzerauthentifizierung] und [SEC-Übertragungswege] direkt unterstützt; die Anforderungen [FA-Accountlinking], [FA-Delegation] und [DSA-Unlinkability] können durch geeignete Implementierung und Konfiguration realisiert werden.

[3] Diese Aussage betrifft das Protokolldesign; fehlerhafte Implementierungen können selbstverständlich Sicherheitslücken aufweisen.

Insgesamt stellt SAML damit eine durchaus fundierte technische Basis dar; sie kann aufgrund ihrer Defizite – insbesondere im Hinblick auf die Integration in bestehende I&AM-Systeme und Geschäftsprozesse sowie essentielle Datenschutzanforderungen – allerdings praktisch nicht ohne Weiteres eingesetzt werden.

3.2.2. Liberty Alliance

Die Liberty Alliance (`http://www.project-liberty.org/`) wurde 2001 mit dem Ziel gegründet, offene Standards, Richtlinien und Best Practices für Federated Identity Management zu schaffen; sie umfasst mittlerweile über 160 Organisationen, zu denen neben fast allen namhaften Herstellern von Identity Management Software unter anderem auch zahlreiche Telekommunikationsdienstleister, Banken und akademische Einrichtungen gehören.

3.2.2.1. Funktionsumfang und zugrundeliegende Spezifikationen der Liberty Alliance

Die Liberty Alliance hat ihre Spezifikationen in drei große, aufeinander aufbauende Blöcke unterteilt:

1. Das **Liberty Identity Federation Framework** (ID-FF, [LAOVER]) bildet die technische Basis für den FIM-basierten Datenaustausch; ursprünglich als „Liberty Phase 1“ bezeichnet, haben sich die Versionen ID-FF 1.1 und 1.2 stark an SAML 1.x orientiert. Erweiterungen von SAML, die mit ID-FF 1.2 eingeführt worden sind, wurden in SAML 2.0 übernommen, so dass SAML 2.0 inzwischen die technische Grundlage der Liberty Alliance darstellt. Die nach wie vor gültige Dokumentation von ID-FF 1.2 weist deshalb starke Parallelen mit der SAML-Spezifikation auf, konkretisiert diese jedoch mit einer Reihe von E-Business Use Cases und XML-Codebeispielen, die ein tiefergehendes Verständnis und somit die Umsetzung durch Softwareentwickler erleichtern [LAPROT, LABIND, LAAUTH, LAMETA].

2. Das **Liberty Identity Web Services Framework** (ID-WSF, [LAWOVR]) erweitert die von ID-FF bereitgestellte Kernfunktionalität: Neben einem zu SAML analogen Discovery Service [LADISC] zur Ermittlung des IDP eines Benutzers und effizienten Protokollen für Clients (*Liberty-enabled User Agents*), deren Leistungsumfang über herkömmliche Webbrowser hinausgeht [LAEUAD], sind insbesondere die folgenden Dokumente im Rahmen dieser Arbeit relevant:

   a) Die Spezifikation des ID-WSF **Interaction Services** gibt die zu verwendenden Nachrichtenformate und Anfrageprotokolle vor, wenn im Rahmen einer FIM-Transaktion Informationen vom Benutzer abgefragt werden sollen [LAISS]. Konkrete Vorgaben zur Gestaltung von graphischen Benutzeroberflächen existieren nicht; in nicht in die formale Spezifikation aufgenommenen Dokumenten wird jedoch unter anderem auf diese Thematik im Hinblick auf die beschränkten Darstellungsfähigkeiten von mobilen Endgeräten (PDAs, Smartphones, ...) eingegangen.

   b) Im Rahmen der Spezifikation ID-WSF **Subscriptions and Notifications** wird definiert, wie SPs beim Abruf von Daten der Datenquelle optional mitteilen

können, dass sie über Änderungen an den abgerufenen Daten informiert werden möchten und wie entsprechende Benachrichtigungen syntaktisch zu kodieren sind [LASUBS].

c) Das Liberty ID-WSF **Data Services Template** spezifiziert das Anlegen, Modifizieren und Löschen beliebiger XML-basierter Daten, die existierenden Benutzerobjekten zugeordnet werden sollen [LAWDS]. Obwohl es bewusst sehr generisch und abstrakt beschrieben und primär als Schnittstelle zu den unten erläuterten ID-SIS Spezifikationen intendiert ist, lässt sich damit prinzipiell ein schreibender Zugriff von SPs auf IDPs bzw. AAs realisieren; auf die in diesem Fall notwendige, nicht triviale Rechteverwaltung wird jedoch nicht eingegangen, da lediglich generische Fehlercodes spezifiziert werden. Das Verfahren ist darüber hinaus ohne weitere Konkretisierung nicht für das SP-lokale User Provisioning von Diensten oder die Integration in vorhandene I&AM-Infrastrukturen geeignet (vgl. Abschnitt 3.7).

d) Der Liberty ID-WSF **People Service** wurde 2006 in den Standard aufgenommen und ermöglicht es Benutzern, Teile ihrer Profile selektiv für andere Benutzer freizugeben [LAPSS]. In der vorliegenden Version 1.0 dieser Spezifikation beschränkt sich der Funktionsumfang auf Benutzer beim selben IDP, die einen Dienst des selben SPs verwenden, sowie auf einfache Mengenoperationen für die Erstellung von Gruppen, beispielsweise zur gemeinsamen Verwendung einer webbasierten Kalenderapplikation.

3. Die **Liberty Identity Service Interface Specifications** (ID-SIS) zielen auf die Standardisierung ausgewählter FIM-basierter Dienste ab, liegen derzeit jedoch noch größtenteils nur als Entwürfe vor. Die Dienstpalette umfasst beispielsweise Gruppenkalender, elektronische Adressbücher und Geo-Location Services für mobile Endgeräte, auf die im Rahmen dieser Arbeit nicht näher eingegangen wird [LACBS, LAGLS, LAPRES]. Mit dem **Personal Profile** und dem **Employee Profile** sollen zwei Datenschemata standardisiert werden, die die Attribute von Identitäten, die im Rahmen privater bzw. beruflicher Dienstnutzung erfasst werden, spezifizieren [LAEmpP, LAPerP, LAEPGL, LAPPGL]. Analog zu den anderen, in Abschnitt 3.8 diskutierten Ansätzen tritt jedoch das Problem auf, dass die fest vorgegebene Auswahl an Attributen stark auf die Bedürfnisse derjenigen Organisationen ausgerichtet sind, die an der Spezifikation mitgearbeitet haben. Für Anwendungen, die nicht im Rahmen von Liberty ID-SIS standardisiert werden, reichen diese Datenmodelle deshalb im Allgemeinen nicht aus.

Der Block Liberty ID-SIS wird derzeit am stärksten weiterentwickelt; die Spezifikationen *Subscriptions and Notifications* und *Data Services Template* könnten langfristig in ID-FF und damit in SAML einfließen, da sie Funktionalitäten bieten, die den technischen Kernspezifikationen derzeit noch fehlen.

3.2.2.2. Datenschutz in der Liberty Alliance

Die Spezifikationen der Liberty Alliance betonen die Notwendigkeit einer datenschutzkonformen FIM-Umsetzung sehr stark. Entsprechende Rahmenbedingungen werden in einem „Best Practices“ Dokument erörtert, das beispielsweise auch auf unterschiedliche Regelungen in den USA und der EU eingeht [LAPRIV].

Die ursprüngliche und nach wie vor gültige wesentliche Empfehlung der Liberty Alliance ist, Benutzer vor der Übertragung personenbezogener Daten interaktiv um Erlaubnis zu fragen. Auch wenn diese Vorgehensweise trivial erscheinen mag, geht ihre konkrete Erwähnung und die Unterstützung im Rahmen des ID-WSF Interaction Services über den Umfang anderer Standards deutlich hinaus.

Die praktische Umsetzung dieser Richtlinie hat jedoch dazu geführt, dass sich Benutzer durch die bei jeder Dienstnutzung und damit sehr häufig auftretenden Nachfragen gestört fühlten. Die Liberty Alliance strebt deshalb die Möglichkeit an, dass Benutzer ihre Datenfreigaberegelungen a priori in Form von Policies konfigurieren können. Im Rahmen eines nicht zur Spezifikation gehörenden White Papers wird deshalb die Unterstützung beliebiger **Privacy Preference Expression Languages** diskutiert, die sich indirekt an den prinzipiellen Möglichkeiten von P3P (siehe Abschnitt 3.5.1) orientiert. Eine konkrete Policysprache und ihre Einbettung in eine entsprechende Privacy Management Architektur wird jedoch nicht vorgegeben und ist derzeit noch nicht geplant.

3.2.2.3. Föderations- und Trustmodelle in der Liberty Alliance

Die heute gebräuchlichen Bezeichnungen für Rollen, die Organisationen in Föderationen einnehmen können (IDP, SP, AA, TTP), wurden von der Liberty Alliance eingeführt. Während die technischen Spezifikationen auf SAML aufbauen und durchaus den Schwerpunkt bilden, werden organisatorische Aspekte von Föderationen im Rahmen nicht zum Standard gehörender Leitfäden behandelt [LATRST].

Die Liberty Alliance unterscheidet derzeit drei Arten gegenseitiger Vertrauensbeziehungen, aus denen sich implizit die Gestaltung der Föderation ableitet:

1. **Pairwise Trust**: Je zwei Organisationen, die miteinander über FIM Daten austauschen möchten, müssen explizit eine geeignete gegenseitige Vertrauensbeziehung aufbauen. Dieses ursprünglich einzige Trustmodell führte in der „Liberty Phase 1“ zum Föderationsmodell **Circle of Trust** (CoT), bei dem alle Föderationsteilnehmer untereinander SLAs abschließen mussten (vgl. Abschnitt 2.1.2.5). Die Verwendung des Begriffs CoT ist seit der Einführung der beiden nachfolgend erwähnten Trustmodelle unscharf und bezieht sich in diversen Publikationen von Dritten generell auf Liberty-Alliance-basierte Föderationen ohne Berücksichtigung des zugrundeliegenden Trustmodells.

2. **Brokered Trust**: Dieses ebenfalls bereits in Abschnitt 2.1.2.5 erläuterte Modell sieht vor, dass eine Trusted Third Party zum Einsatz kommt, mit der jeder Föderationsteilnehmer ein SLA abschließt. Eine Organisation vertraut dann jeder anderen Organisation, die wie sie selbst direkt mit dieser TTP in vertraglicher Beziehung steht. Die Vertrauensbeziehung ist somit transitiv, aber auf die TTP als einzige Zwischenstation beschränkt.

3. **Community Trust**: Bei dieser nicht präzise spezifizierten Variante wird jeder anderen Organisation vertraut, die sich als Mitglied derselben *Community* ausweisen kann. Wie sich diese Föderation bildet oder verwaltet wird, bleibt offen. Eine nahe liegende Realisierungsvariante wäre deshalb, Vertrauensbeziehungen zwischen Organisationen als uneingeschränkt transitiv zu betrachten.

Analog zu den anderen FIM-Ansätzen haben diese Vertrauensbeziehungen auf technischer Ebene lediglich Auswirkung auf die Verwaltung von Metadaten; der Datenaustausch findet auch bei der Liberty Alliance ohne Berücksichtigung des Föderationskontextes zwischen jeweils zwei Föderationsteilnehmern statt (vgl. Anforderungen [FA-Zusatzdaten], [SEC-Trust] und [ORG-Trust]).

3.2.2.4. Bewertung der Liberty Alliance Spezifikationen

Die Spezifikationen erfüllen in Kombination mit den nicht zum Standard gehörenden Richtlinien der Liberty Alliance alle *essentiellen* Anforderungen mit der Einschränkung, dass durch den Benutzer vorgegebene Attribute Release Policies ([DSA-ARPs]) zwar vorgesehen, aber nicht konkret spezifiziert sind. Ihre Implementierung ist insbesondere keine Voraussetzung für die Konformität mit den Spezifikationen [LACONF, LAIDFF, LAWSFC].

Die *wichtigen* Anforderungen werden mit folgenden Einschränkungen erfüllt:

- Die Spezifikationen und ihre Beispiele beschränken sich auf einzelne, webbasierte Anwendungen; auf die Integration mit vorhandenen I&AM-Systemen wird ebenso wie auf die Integration in bestehende Sicherheitsinfrastrukturen nicht eingegangen ([FA-Konnektor], [SEC-Integration]).
- Die Interoperabilität im Hinblick auf die pro Föderationsteilnehmer unterschiedlichen Datenformate wird nicht betrachtet ([FA-Schema]).
- Die Korrelation von Benutzerdatensätzen ([FA-Korrelation]) ist nur manuell durch den Benutzer gesteuert vorgesehen und basiert somit auf Freiwilligkeit ohne Garantie für hohe Datenqualität.
- Auf die Verwendung existierender Managementwerkzeuge und die Anbindung an bestehende Supportprozesse wird nicht eingegangen ([NFA-Management], [ORG-Supportprozesse]).
- Die administrative Vorgabe von Standardfreigaben ist nicht vorgesehen ([DSA-DefaultARPs]).
- Für die Erfüllung der Anforderung [ORG-Datennutzung] gelten dieselben Auflagen wie bei SAML.

Darüber hinaus werden die *empfehlenswerten* Anforderungen [FA-AccountLinking], [FA-Pull&Push], [NFA-Modularität], [NFA-Portabilität], [SEC-Benutzerauthentifizierung], [SEC-Übertragungswege], [DSA-Unlinkability] und [DSA-Zustimmung] erfüllt.

Insgesamt stellt die Liberty Alliance die umfangreichste und derzeit am besten geeignete, industriell standardisierte Basis für FIM-basierten Datenaustausch dar. Im Hinblick auf einen konkreten Einsatz sind jedoch insbesondere noch Lösungen für die folgenden Defizite zu erarbeiten:

- Die Interoperabilität der pro Föderationsteilnehmer eingesetzten Informationsmodelle muss gewährleistet werden, insbesondere in Kombination mit der Integration von FIM-Komponenten in bestehende I&AM-Systeme.

- Das SP-seitige Provisioning mehrerer Dienste muss unter Berücksichtigung von Abhängigkeiten und Beibehaltung existierender Managementinfrastrukturen unterstützt werden.
- Das Management von Datenfreigaben soll in Form von Attribute Release Policies erfolgen, die durch Administratoren und in geeigneter Form dabei unterstützte Benutzer vorgegeben werden.

Die Beobachtung der jüngsten Aktivitäten der Liberty Alliance lässt darauf schließen, dass in diesen Bereichen noch keine Standardisierung angestrebt wird, sondern die Bearbeitung von Rückmeldungen zu den bereits veröffentlichten Spezifikationen und das Vorantreiben von ID-SIS priorisiert werden.

3.2.3. Web Services Federation Language (WS-Federation)

Bei der Web Services Federation Language (WS-Federation, [WS-Fed]), die maßgeblich von IBM und Microsoft geprägt wurde, handelt es sich um eine konsequente Weiterentwicklung von **Microsoft Passport**,[4] bei der neben einer Erweiterung des Funktionsumfangs primär die Unterstützung dezentraler Föderationsmodelle und die Integration in den Web Services Protokollstack (WS-*) angestrebt wurden.

Passport verfolgte den Ansatz, dass Microsoft einen zentralen IDP betreibt, bei dem über die Benutzer E-Commerce-spezifische Daten wie Kontakt-, Liefer- und Kreditkarteninformationen erfasst werden, die einem SP dann zur Verfügung gestellt werden, wenn sich ein Benutzer auf seiner Webseite über Passport anmeldet. Zu diesem Zweck stellte Microsoft interessierten SPs Codefragmente zur Verfügung, mit denen ein kleines Passport-Login-Formular auf der SP-Webseite integriert werden konnte; nachdem Sicherheitslücken in der Implementierung bekannt wurden und der sehr zentrale Ansatz von Datenschutzaktivisten mehrfach heftig kritisiert wurde, setzt Microsoft das Verfahren inzwischen nur noch für die zum Microsoft Network (MSN) gehörenden SPs ein.

3.2.3.1. Funktionsumfang und zugrundeliegende Spezifikationen von WS-Federation

Der Umfang der Spezifikation von WS-Federation liegt deutlich hinter dem der anderen FIM-Industriestandards. Allerdings wurde bewusst darauf verzichtet, eine in sich geschlossene Spezifikation zu schaffen; vielmehr steht die Nutzung mehrerer anderer WS-*-Standards im Vordergrund, die über WS-Federation zusammengeführt werden:

- **WS-Security** [WS-Sec] spezifiziert die Kombination von SOAP-basierter Datenübertragung mit kryptographischen Sicherheitsmaßnahmen.
- **WSS-Kerberos** (WS-Security Kerberos Binding, [WS-Ker]) beschreibt die Verwendung von Kerberos-Tickets und X.509-Zertifikaten als Nachrichtenformate beim Datenaustausch.

[4] `http://www.passport.net/` – Microsoft Passport wurde zuerst in *dotNet Passport* und dann in *Windows Live-ID* umbenannt.

- **WS-Trust** [WS-Tru] definiert ein auf WS-Security basierendes Protokoll, um Daten von einer Gegenstelle abrufen zu können und die Vertrauensbeziehung zu dieser zu verwalten (siehe Abschnitt 3.2.3.2).
- **WS-Policy** [WS-Pol] gibt ein Rahmenwerk zur Spezifikation und Übertragung von Policies vor; es bildet in WS-Federation die Grundlage zur Verwaltung föderationsspezifischer Metadaten und wird in einer Reihe anderer Spezifikationen verfeinert [WS-PoA, WS-PAs].

Das von WS-Federation verwendete Vokabular weicht deutlich von SAML ab:

- Statt Assertions kommen **Claims** (Behauptungen) zum Einsatz, die durch Proofs-of-Possession (Beweise für die Erfüllung von Eigenschaften, typischerweise X.509-Zertifikate) in Form von **Secure Tokens** untermauert werden können. Hierdurch wird eine explizite Unterscheidung von möglicherweise falschen Benutzerangaben und durch einen Dritten sichergestellter Datenqualität ermöglicht. Inzwischen werden auch SAML Assertions als Bestandteile von Secure Tokens unterstützt.
- Service Provider werden generell als Resources bezeichnet; Secure Tokens werden sowohl IDP- als auch Resource-seitig von einem **Secure Token Service** (STS) verarbeitet.
- Benutzer bzw. deren Softwaresysteme werden als Requestors bezeichnet; dabei wird zwischen *passive requestors* (herkömmliche Webbrowser) und *active requestors* (Clients mit SOAP-Fähigkeit in Analogie zu Liberty-enabled User Agents) unterschieden [WS-FPR, WS-FAR].

WS-Federation unterstützt somit zwar prinzipiell das Informationsmodell von SAML; das Kommunikationsmodell lehnt sich jedoch stärker an das ticketbasierte Kerberos an, so dass der FIM-Datenaustausch wie in Abbildung 3.3 dargestellt abläuft:

- Der Benutzer wendet sich an den Secure Token Service seines IDPs (Schritt 1), der ein Secure Token auf Basis seines lokalen, nicht näher spezifizierten Identity Repository erstellt (Schritt 2) und an den Benutzer übermittelt (Schritt 3); analog zu SAML muss er sich dabei gegebenenfalls erst gegenüber seinem IDP authentifizieren (vor Schritt 2).
- Das Secure Token wird vom Client des Benutzers an den SP übertragen (Schritt 4).
- Zur Überprüfung der Angaben im Secure Token wendet sich der SP-seitige Service an seinen lokalen Secure Token Service (Schritt 5), der zum Aussteller des Tokens eine geeignete Vertrauensbeziehung aufgebaut haben muss und ggf. weitere lokale Datenbestände zur Beurteilung heranziehen kann (Schritt 6). Die validierten Daten werden schließlich dem Dienst zur Verfügung gestellt (Schritt 7).

Daraus ergibt sich der Vorteil, dass die SP-seitig initiierte **Delegation** vergleichsweise einfach zu realisieren ist, indem das entsprechende Token des Benutzers an einen Drittanbieter weitergeleitet wird; aus sicherheitstechnischer und datenschutzrechtlicher Sicht birgt dies jedoch die Gefahr, dass die im Token enthaltenen Daten auf diese Weise unkontrolliert in Umlauf

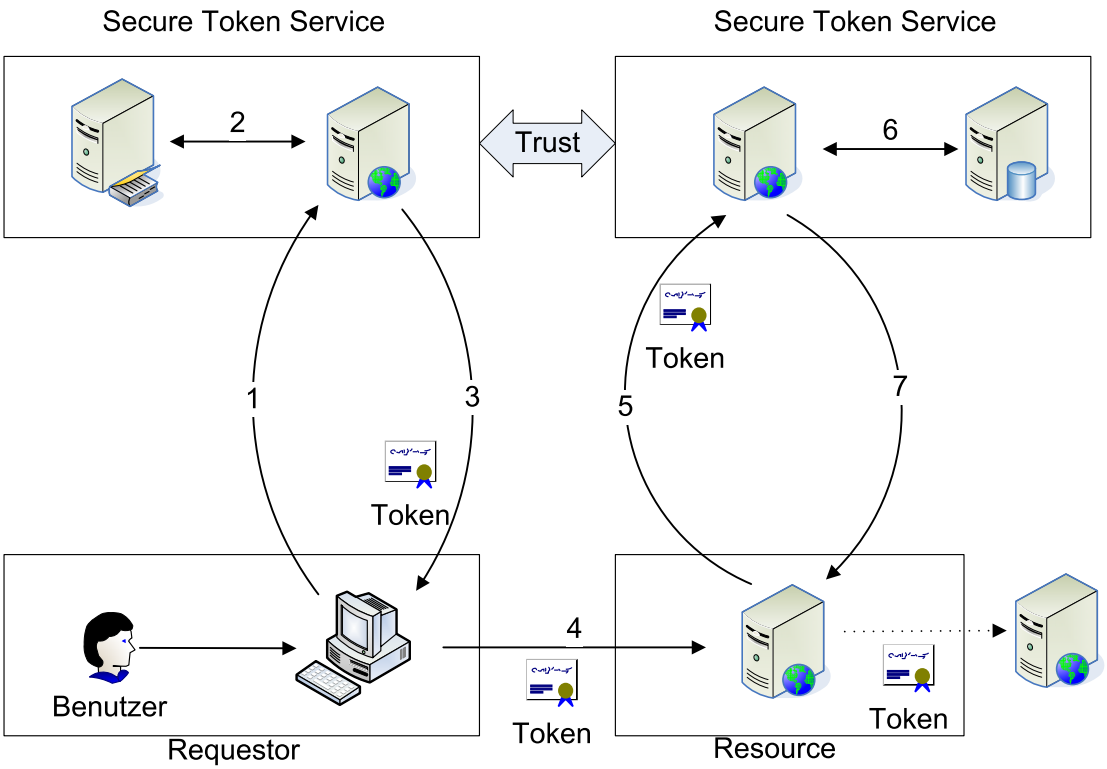


Abbildung 3.3.: Ablauf eines FIM-Datentransfers auf Basis von WS-Federation

gebracht werden könnten, so dass wiederum geeignete Schutzmechanismen implementiert werden müssen.

Das Verfahren weist insgesamt wiederum Parallelen mit Attributszertifikaten im UCIM-Umfeld auf, so dass es nicht überrascht, dass Microsoft mit CardSpace ein UCIM-Verfahren auf den Markt bringt (vgl. Szenario 2 und Abschnitt 3.9).

Auf Basis weiterer WS-*-Spezifikationen können Authentifizierungs- und Autorisierungsinformationen sowie beliebige weitere Datentypen modelliert werden. WS-Federation spezifiziert darüber hinaus einen Single-Logout-Mechanismus.

3.2.3.2. Datenschutz und organisatorische Aspekte in WS-Federation

WS-Federation wurde 2003 veröffentlicht und hebt die Berücksichtigung von Datenschutzaspekten an mehreren Stellen hervor; hinsichtlich konkreter Aussagen wird jedoch konsequent auf die Spezifikation **WS-Privacy** verwiesen, die jedoch bis heute nicht veröffentlicht und auch nicht näher angekündigt wurde. Die Umsetzung von Maßnahmen zur Unterstützung des Datenschutzes bleiben deshalb dem freien Ermessen von Softwareherstellern überlassen.

WS-Federation, WS-Trust und WS-Policy stellen generische Gerüste für die Verwaltung von Föderationsmetadaten und damit Möglichkeiten zur Instanziierung verschiedener Föderationsmodelle bereit. Die Terminologie unterscheidet sich jedoch auch hier wieder von derjenigen

der Liberty Alliance:

- Als **direct trust** wird die Situation bezeichnet, in der ein SP allen vom Benutzer gemachten Angaben vertraut, ohne sie verifizieren zu wollen.
- **Direct brokered trust** liegt vor, wenn zwischen SP und IDP eine Vertrauensbeziehung besteht und vom IDP Token für den Benutzer ausgestellt werden, die der SP überprüft.
- **Indirect brokered trust** entspricht dem Brokered-Trust-Modell der Liberty Alliance, bei dem der Dienst einer Trusted Third Party in Anspruch genommen wird.

Weitere Föderationsmodelle auf Basis dieser Spezifikationen sind denkbar, jedoch nicht explizit erläutert.

3.2.3.3. Bewertung von WS-Federation

Die Spezifikation von WS-Federation leidet generell darunter, dass an vielen Stellen auf andere WS-*-Spezifikationen verwiesen wird, die aber zur präzisen Erläuterung eines Aspekts nur wenig hilfreich sind: Zum einen ergeben sich mehrfach Verweisketten, unter denen die gewünschte Information nicht aufzufinden ist, zum anderen wird – wie im Fall von WS-Privacy – auf Dokumente verwiesen, die noch nicht veröffentlicht wurden oder noch Lücken aufweisen.

Die *essentiellen* Anforderungen [FA-Interaktion] und [DSA-ARPs] werden von WS-Federation nicht berücksichtigt.

Darüber hinaus werden die *wichtigen* Anforderungen [FA-Konnektor], [FA-Schema], [FA-Schreibzugriff], [FA-Updates], [NFA-Management], [NFA-Usability], [SEC-Integration], [ORG-Migration], [ORG-Supportprozesse] sowie daraus folgend [DSA-DefaultARPs] und [DSA-Schreibzugriff] nicht erfüllt.

Für die Erfüllung der Anforderungen [FA-Korrelation] und [ORG-Datennutzung] gelten dieselben Auflagen wie bei den Spezifikationen der Liberty Alliance.

Von den *empfehlenswerten* Anforderungen werden [FA-AccountLinking], [FA-Delegation], [NFA-Modularität], [NFA-Portabilität], [SEC-Benutzerauthentifizierung], [DSA-Attributszertifikate] und [DSA-Unlinkability] unterstützt.

Insgesamt stellt WS-Federation damit eine modulare und durchaus flexible, aber auch sehr komplexe Basis für FIM dar, deren praktische Einsatzfähigkeit aufgrund ihrer Defizite allerdings noch sehr beschränkt ist. Angesichts der kontinuierlichen Bestrebungen um Erweiterungen des WS-* Protokollstacks ist jedoch davon auszugehen, dass sich WS-Federation-basiertes FIM zukünftig noch weiterentwickeln wird; mit der Unterstützung von SAML Assertions in Secure Tokens ist darüber hinaus der Grundstein für die Interoperabilität mit SAML und den darauf basierenden FIM-Lösungen gelegt.

3.3. FIM-Forschungsansätze

In den folgenden Abschnitten werden wissenschaftliche Ansätze erläutert, die eine insbesondere mit SAML vergleichbare Zielsetzung haben, d. h. im Wesentlichen Architektur- und Pro-

tokolleigenschaften untersuchen, ohne ein entsprechendes vollwertiges Softwareprodukt, das über prototypischen Charakter hinausgeht, anzubieten.

Shibboleth ist eine wichtige Ausnahme, die mit einer bereits sehr ausgereiften Implementierung verbunden ist, anhand derer die auch in SAML bzw. den Liberty Alliance Spezifikationen vorgesehene Föderations-Metadatenverwaltung erläutert wird.

Auf weitere wissenschaftliche Veröffentlichungen, die sich mit Teilaspekten befassen und die im Rahmen dieser Arbeit verwendet, modifiziert oder bewusst nicht berücksichtigt wurden, wird themenspezifisch in den Kapiteln 4 und 5 eingegangen.

3.3.1. Shibboleth

Shibboleth[5] ist der bedeutendste Forschungsansatz und mit einer namensgleichen Open Source Implementierung verbunden, die inzwischen weltweit bei einer Vielzahl von Hochschuleinrichtungen und hochschulnahen Organisationen wie akademischen Verlagen im Einsatz ist.

Shibboleth entstand im Rahmen der US-amerikanischen Internet2-Initiative *Middleware Architecture Committee for Education* (MACE) und wird nach wie vor maßgeblich von dieser weiterentwickelt. Als Basis kommt dabei SAML 1.1 zum Einsatz, wobei eine enge Zusammenarbeit mit OASIS und der Liberty Alliance dazu geführt hat, dass viele in Shibboleth umgesetzte Erweiterungen über die Liberty Alliance in SAML 2.0 eingeflossen sind. Die für 2007 geplante Version 2.0 von Shibboleth wird deshalb auch SAML 2.0 als Grundlage verwenden, nachdem die ersten Versionen von Shibboleth noch umfangreiche Modifikationen an SAML 1.0 vorgenommen haben. Im Rahmen eines von Microsoft finanzierten Teilprojekts wird Shibboleth inzwischen auch um die Unterstützung von WS-Federation erweitert, damit beispielsweise der Onlinezugriff auf die Dienste der Microsoft Developer Network Academic Alliance (MSDNAA), z. B. kostenloser Download von Microsoft-Software für Studenten, über Shibboleth realisiert werden kann.

Im Folgenden werden aufgrund der starken Anlehnung an SAML lediglich die konkreten Ausprägungen der Föderationsverwaltungs- und Datenschutzaspekte in Shibboleth vorgestellt.

3.3.1.1. Verwaltung von Metadaten in Shibboleth

Shibboleth stellt für die Verwaltung größerer Föderationen Werkzeuge zur zentralen Pflege von Metadaten zur Verfügung. In Analogie zu den von SAML und der Liberty Alliance spezifizierten Metadatenformaten werden von jedem Identity Provider und jedem Dienst einerseits die technischen Kontaktinformationen in Form von URIs, andererseits auch organisatorische Informationen, beispielsweise über die jeweiligen Ansprechpartner, erfasst. Der folgende Codeausschnitt zeigt den Eintrag des vom LRZ in der Shibboleth-Testföderation *InQueue* betriebenen IDPs, aus dem insbesondere die URLs für Benutzerlogin (**Single Sign On Service**) und das Abrufen von SAML Assertions (**Attribute Service**) hervorgehen:

```
1 <EntityDescriptor entityID="urn:inqueue:lxsidp01.lrz-muenchen.de">
2
3    <IDPSSODescriptor>
4       <Extensions>
5          <shib:Scope>lrz-muenchen.de</shib:Scope>
```

[5] http://shibboleth.internet2.edu/

```
6         </Extensions>
7         <KeyDescriptor use="signing">
8            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
9               <ds:KeyName>lxsidp01.lrz-muenchen.de</ds:KeyName>
10           </ds:KeyInfo>
11        </KeyDescriptor>
12        <ArtifactResolutionService
13           Location="https://lxsidp01.lrz-muenchen.de/shibboleth-idp/Artifact"/>
14        <SingleSignOnService Binding="urn:AuthnRequest"
15           Location="https://lxsidp01.lrz-muenchen.de/shibboleth-idp/SSO"/>
16    </IDPSSODescriptor>
17
18    <AttributeAuthorityDescriptor>
19        <Extensions>
20           <shib:Scope>lrz-muenchen.de</shib:Scope>
21        </Extensions>
22        <KeyDescriptor use="signing">
23           <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
24              <ds:KeyName>lxsidp01.lrz-muenchen.de</ds:KeyName>
25           </ds:KeyInfo>
26        </KeyDescriptor>
27        <AttributeService
28           Location="https://lxsidp01.lrz-muenchen.de:8443/shibboleth-idp/AA"/>
29    </AttributeAuthorityDescriptor>
30
31    <Organization>
32        <OrganizationName xml:lang="en">Leibniz Supercomputing Center</OrganizationName>
33        <OrganizationURL xml:lang="en">http://www.lrz-muenchen.de/</OrganizationURL>
34    </Organization>
35    <ContactPerson contactType="technical">
36        <Name>Wolfgang Hommel</Name>
37        <EmailAddress>wolfgang.hommel@lrz-muenchen.de</EmailAddress>
38    </ContactPerson>
39
40 </EntityDescriptor>
```

Die Metadaten aller IDPs und SPs werden zu einer einzigen XML-basierten Datei zusammengefasst, von der zentralen Verwaltungsinstanz elektronisch signiert und den Föderationsteilnehmern zugänglich gemacht; sie muss von diesen – möglichst automatisiert und regelmäßig – bezogen und in die lokale Shibboleth-Installation eingespielt werden. Die einzelnen Komponenten von Shibboleth werten sie wie folgt aus:

- Zur Auswahl des für einen Benutzer zuständigen IDPs wird der **Where Are You From?** (WAYF) Service verwendet. Er überprüft anhand der Metadaten, ob die Aufforderung zur Ermittlung des IDP von einem legitimen SP stammt, und erzeugt aus ihnen eine Liste aller möglichen IDPs. Sofern sich der Benutzer für einen davon entscheidet, wird er vom WAYF-Service anhand der über den IDP gespeicherten Metadaten an dessen *Single Sign On Service* weitergeleitet.
- Analog dazu überprüfen IDPs, ob eine Anfrage von einem zur Föderation gehörenden SP stammt; die Information, wohin Benutzer nach erfolgreicher Authentifizierung zur Nutzung des Dienstes umgeleitet werden sollen, könnte ebenfalls den Metadaten entnommen werden, wird jedoch zur Flexibilisierung mittels Parametern vom SP über den WAYF an den IDP übergeben.
- SPs erkennen anhand der Metadaten die offiziellen IDPs einer Föderation und können die elektronisch signiert übermittelten SAML Assertions anhand der Zertifikatsdaten auf ihre Integrität überprüfen.

Änderungen an den Einträgen eines Föderationsteilnehmers müssen geeignet an die zentrale Verwaltungsstelle kommuniziert werden. Hierfür existiert kein vorgeschriebenes Verfahren; in der Regel erfolgt diese Kommunikation über föderationsinterne Webschnittstellen oder per E-Mail, wobei in beiden Fällen eine geeignet starke Authentifizierung des Absenders notwendig ist.

Prinzipiell könnten in den Föderationsmetadaten auch die Serverzertifikate der beteiligten IDPs und SPs festgehalten werden. Aufgrund der typischerweise auf ein bis zwei Jahre begrenzten Gültigkeitsdauer von Zertifikaten würde dies in größeren Föderationen jedoch zu einem ständigen Verwaltungsaufwand führen; in der Praxis wird deshalb bevorzugt eine föderationsweite PKI eingesetzt, so dass die von einer gemeinsamen CA ausgestellten Zertifikate von allen Föderationsteilnehmern verifiziert werden können, ohne dass sie redundant in den Metadaten geführt werden müssen.

3.3.1.2. Datenschutz in Shibboleth

Aufgrund vergleichsweise strenger Auflagen im US-amerikanischen Hochschulumfeld wurde Shibboleth mit einer starken Betonung von Datenschutzaspekten entwickelt. Shibboleth unterstützt Attribute Release Policies (ARPs) in einem proprietären, XML-basierten Format und hat maßgeblich zur Etablierung dieses Begriffs beigetragen [SHARPS].

Ein grundlegender Ansatz von Shibboleth ist die Bestrebung, in dafür geeigneten Szenarien möglichst nur Berechtigungen bzw. so wenige allgemeine Attributsauskünfte wie möglich zu erteilen. Ein Haupteinsatzgebiet von Shibboleth ist derzeit der hochschulübergreifende Zugriff auf Online-Bibliotheksbestände: Die zwischen Hochschulen und Verlagen abgeschlossenen Rahmenverträge sehen in der Regel vor, dass der Zugriff auf bestimmte Bestände nur einem eingeschränkten Nutzerkreis der Bibliothek zugänglich gemacht werden darf, beispielsweise den festangestellten Mitarbeitern einer bestimmten Fakultät. Shibboleth-Instanzen sind deshalb angehalten, nur diese Autorisierungsinformation bzw. die Fakultätszugehörigkeit an die jeweiligen SPs zu übermitteln, aber keine darüber hinaus gehenden Daten wie Name und Adresse der Benutzer. Die offensichtliche Voraussetzung, dass der SP den vom IDP gelieferten Daten vertrauen muss, wird in diesem Fall also zur delegierten Autorisierung ausgedehnt.

Shibboleth unterscheidet zwischen einer so genannten **Site-ARP**, über die Administratoren IDP-weite Voreinstellungen treffen können, und einer **User-ARP** pro Benutzer, mit der diese Vorgaben verfeinert oder überschrieben werden können. Wie in Abschnitt 3.5.3 dargestellt wird, ist die Ausdrucksmächtigkeit der Shibboleth ARP-Sprache jedoch stark begrenzt und nur für Szenarien mit diesbezüglich relativ einfachen Anforderungen geeignet.

Eine generelle Schwierigkeit bei der praktischen Verwendung von ARPs ist die Bereitstellung eines für alle Benutzer geeigneten, intuitiv zu bedienenden Managementfrontends. Der praktische Einsatz von User-ARPs wird in Shibboleth deshalb bislang stark vernachlässigt; das australische MAMS-Projekt entwickelt mit dem **Shibboleth Attribute Release Policy Editor** (ShARPE) einen vielversprechenden Lösungsansatz, der wiederum die aus dem UCIM-Umfeld bekannte Visitenkartenmetapher aufgreift, bei der Benutzer ihre personenbezogenen Daten in Form von elektronischen Visitenkarten an SPs übermitteln [MAMS].

3.3.1.3. Bewertung von Shibboleth

Shibboleth erfüllt alle *essentiellen* Anforderungen, wobei lediglich Einschränkungen bei [DSA-ARPs] aufgrund der beschränkten Ausdrucksmächtigkeit von Shibboleth-ARPs in Kauf genommen werden müssen, die sich auch auf [FA-Interaktion] auswirken (vgl. Abschnitte 3.5.3 und 5.3).

Als SAML-basierter Ansatz unterstützt Shibboleth die *wichtigen* Anforderungen [FA-Schreibzugriff] und [FA-Updates] sowie folglich [DSA-Schreibzugriff] nicht. Die Integration in bestehende I&AM-Systeme wird nur IDP-seitig betrachtet und unterliegt hinsichtlich der Anforderungen [FA-Konnektor] und [FA-Schema] wiederum Einschränkungen bezüglich der Möglichkeiten zur Konvertierung von Daten aus lokal verwendeten Formaten (vgl. Abschnitt 5.2). Ebenso wenig wie bei den anderen Ansätzen wird die Integration aus Securityperspektive betrachtet ([SEC-Integration]).

Die Ausrichtung auf hochschulspezifische Föderationen bringt Einschränkungen bezüglich der Anforderungen [ORG-Föderationsmodelle] und [ORG-SLAs] mit sich. Die Anforderungen [ORG-Datennutzung] und [ORG-Supportprozesse] werden von Shibboleth derzeit nicht berücksichtigt, für Verwaltungszwecke werden jedoch zumindest zum Teil eigene Werkzeuge bereitgestellt ([NFA-Management]).

Das von Shibboleth vorrangig verfolgte Datenschutzkonzept, bei dem möglichst nur Autorisierungen und keine personenbezogenen Daten übertragen werden, führt dazu, dass [FA-Korrelation] und [FA-Accountlinking] zwar nicht vorgesehen, aber prinzipiell möglich sind; [SEC-Deprovisioning] wird mit Shibboleth 2.0 erfüllt werden.

Die Anforderung [NFA-Usability] wird derzeit nur zum Teil erfüllt, da entsprechende Schnittstellen zu den Anwendern erst noch im Entstehen sind.

Analog zu SAML erfüllt Shibboleth die *empfehlenswerten* Anforderungen [FA-Pull&Push] und [SEC-Übertragungswege] und darüber hinaus [NFA-Modularität], [NFA-Portabilität], [SEC-ARPs], [SEC-Benutzerkreis] und [DSA-Unlinkability]. Die Anforderung [SEC-Benutzerauthentifizierung] wird im Gegensatz zu SAML nicht unterstützt, da es jedem IDP überlassen bleibt, welche Authentifizierungsmethode eingesetzt wird, ohne dass der SP darauf Einfluss hat.

Insgesamt ist Shibboleth damit eine bereits durchaus gut praktisch einsetzbare Lösung, die auch kontinuierlich weiterentwickelt wird, bislang allerdings nur im akademischen und hochschulnahen Bereich Verbreitung gefunden hat. Die im Rahmen dieser Arbeit entstandenen Prototypen und Tragfähigkeitsnachweise setzen auf Shibboleth auf und tragen damit zu einer Verringerung der Defizite insbesondere in den Bereichen IDP- bzw. SP-seitige Integration in vorhandene I&AM-Infrastrukturen und Attribute Release Policies bei (siehe Kapitel 5 und 6).

3.3.2. Browser Based Attribute Exchange (BBAE)

Nach der Veröffentlichung von SAML 1.0 wurden von IBM Research Sicherheitslücken im Protokoll nachgewiesen und Defizite bezüglich der Interaktion mit dem Benutzer im Hinblick auf Datenschutzfreigaben bemängelt [Gro03]. Mit dem Protokoll „Browser Based Attribute Exchange“ (BBAE) wurde von B. Pfitzmann und Waidner eine um Interaktionsschritte erweiterte Variante von SAML vorgeschlagen, die für die gefundene SAML-Sicherheitslücke nicht anfällig war [BBAE, PW02, PfWa03].

Durch Beheben des Sicherheitsproblems in SAML und die Anforderungen der Liberty Alliance an Benutzerinteraktionen ist BBAE inzwischen trotz seiner Innovationen obsolet und wird nicht mehr weiterentwickelt; die grundlegenden Konzepte für intuitiv benutzbare graphische Oberflächen für Datenschutzfreigaben werden im EU-geförderten PRIME-Projekt[6] vertieft

[6]PRIME = Privacy and Identity Management for Europe, `http://www.prime-project.eu/`

analysiert, an dem IBM Research ebenfalls beteiligt ist [PRUSAB, IM4EVR].

3.3.3. Tequila, Hurderos et alia

Während ihrer Entstehungszeit und als für die relative komplexe Spezifikation von SAML noch keine frei verfügbaren Implementierungen existierten, entstand im Rahmen wissenschaftlicher Projekte eine Reihe alternativer, zum Teil bewusst sehr einfach gehaltener Alternativansätze. Sie werden im Folgenden kurz umrissen und sind teilweise in Form nach wie vor gepflegter Softwarepakete verfügbar, spielen jedoch eine nur untergeordnete Rolle, da sie keine neuen Ideen umsetzen, die nicht bereits von den Industriestandards absorbiert wurden:

- **Tequila** [TEQILA] entstand an der Ecole Polytechnique Fédérale de Lausanne und weist architekturelle Ähnlichkeiten mit Shibboleth auf, da IDP- und SP-seitige Webserver um Tequila-Komponenten ergänzt werden. Tequila unterstützt die Übertragung von Authentifizierungs- und Attributsinformationen; Föderationen werden als Tequila-Zellen (engl. *cells*) bezeichnet. Das Konzept und die Open Source Software wurden ursprünglich entwickelt, um die Identity Management Systeme der Schweizer Hochschulen gemeinsam nutzen zu können; durch den landesweiten Einsatz von Shibboleth im Rahmen der SWITCH-AAI ist diese Zielsetzung nicht mehr aktuell. Es sind keine produktiven Föderationen bekannt, die Tequila einsetzen.

- **DACS**[7] entstand ursprünglich im Rahmen eines Projektes mit dem kanadischen National Forest Information System und fokussiert auf organisationsübergreifendem Single Sign-On und rollenbasierter Autorisierung nach dem klassischen RBAC-Modell (Role Based Access Control). Es ist inzwischen als eigenständiges Open Source Produkt erhältlich und setzt die Verwendung der Webserversoftware Apache bei den Teilnehmern an einer Föderation, die als *Jurisdiction* bezeichnet wird, voraus. Die Funktionalität von DACS stellt eine Teilmenge derjenigen von SAML dar, wobei die Entwickler bereits eine langfristige Annäherung der proprietären DACS-Protokolle an SAML in Erwägung ziehen.

- **Hurderos** [HURDER] hatte die Zielsetzung, LDAP-basierte Identity Repositories und Kerberos als Ausgangsbasis für FIM mit Schwerpunkt Federated User Provisioning zu verwenden (siehe auch Abschnitt 3.7), wird seit 2004 jedoch anscheinend nicht mehr weiterentwickelt und ist nur als frühe Beta-Version verfügbar. Für den Ansatz, Benutzerkonten auf diese Weise SP-seitig anzulegen, wurde der Begriff Reciprocal Identity Management (RIM) gewählt, der sich jedoch nicht durchgesetzt hat.

- **eXtensible Distributed Access Control** (X-DAC, [XDAC]) entstand 2004 am Dartmouth College und beschreibt die kombinierte Verwendung von SAML und der Policysprache XACML [XACML], um feingranulare Zugriffskontrollsteuerungen zu ermöglichen. Der Schwerpunkt liegt dabei auf der Beschreibung derjenigen Workflows, die zwischen Policy Decision und Policy Enforcement Point (PDP und PEP) notwendig sind. Analog dazu verfeinert der Ansatz **CARDEA** [CARDEA] SAML-Autorisierungsbestätigungen auf Basis von XACML.

[7] DACS = Distributed Access Control System, `http://dacs.dss.ca/`

In [XACMLD] wird ein Überblick über weitere Ansätze gegeben, die Teilaspekte verteilter Zugriffskontrolle behandeln, so dass dieser Bestandteil von FIM im Rahmen dieser Arbeit als gelöst betrachtet wird.

3.4. Aktuelle FIM-Produkte

Nachfolgend werden auf SAML, den Liberty Alliance Spezifikationen und WS-Federation basierende aktuelle FIM-Softwareprodukte vorgestellt. Die Darstellung ist bewusst knapp, da es sich um eine Momentaufnahme eines Softwaremarktes handelt, der zwar noch am Anfang ist, von dem aber bereits im Zeitraum von wenigen Jahren eine starke Vergrößerung zu erwarten ist. Die Darstellung soll deshalb primär die bisherige Akzeptanz und Umsetzung der FIM-Standards durch Softwarehersteller reflektieren.

3.4.1. Referenzimplementierungen

Zu keinem der drei Standards existieren Referenzimplementierungen durch ihre Spezifikationsgremien. OASIS und die Liberty Alliance geben Konformitätsrichtlinien vor, die sich jedoch lediglich auf den Umfang der zu erbringenden Funktionalität und nicht auf technische Details beziehen.

Als Konsequenz hat sich in den vergangenen Jahren herausgestellt, dass zahlreiche Implementierungen zwar SAML-konform, aber nicht interoperabel waren. Aus diesem Grund finden inzwischen jährliche Arbeitstreffen mehrerer großer Softwarehersteller statt, bei denen die Softwareentwickler Tests durchführen und an verbesserter Kompatibilität ihrer jeweiligen Produkte arbeiten.

Das Fehlen von Referenzimplementierungen hat somit deutlich sichtbare Konsequenzen für die Qualität der FIM-Produkte, die wiederum eine der möglichen Begründungen für das zögerliche Kundeninteresse ist (vgl. [SBP05, IMSURV]).

3.4.2. Open Source Produkte

Während die Anzahl der kommerziellen Produkte, die mindestens einen der drei industriellen FIM-Ansätze unterstützen, noch ständig zunimmt, bleibt die Anzahl verfügbarer Open Source Implementierungen bislang konstant und überschaubar:

- **OpenSAML**[8] ist eine frei verfügbare Implementierung von SAML 1.1 für die Programmiersprachen C++ und Java; sie wurde ursprünglich für Shibboleth entwickelt und wird im Rahmen von Shibboleth 2.0 für SAML 2.0 von Grund auf neu implementiert, da die Autoren mit den in OpenSAML 1.1 eingesetzten XML-Programmierbibliotheken unzufrieden sind.
- Die Firma **Ping Identity**[9] stellt als **Toolkits** bezeichnete Funktionsbibliotheken für SAML 1.1, Liberty ID-FF 1.2 und WS-Federation (als Beta-Version) für Java- und

[8] `http://www.opensaml.org/`
[9] `http://www.pingid.org/, http://www.sourceid.org/`

Windows-ASP.NET-Applikationen zur Verfügung. Da Ping Identity auch eigene kommerzielle FIM-Produkte anbietet, wurde das Liberty ID-FF 1.2 Toolkit als Liberty-konform zertifiziert.

- **Lasso**[10] ist eine in C programmierte Liberty ID-FF 1.2 Implementierung, auf deren Basis die Identity Provider Software *Authentic* von der französischen Firma Entr'Ouvert realisiert wurde, die ebenfalls als Open Source Software verfügbar ist.
- Microsoft stellt einige Beispielquelltexte zum Umgang mit WS-Federation-Nachrichten zur Verfügung, die jedoch noch keine zusammenhängende Programmierbibliothek oder Referenzimplementierung bilden.

Somit zeigt sich, dass im Bereich freier Implementierungen WS-Federation noch nur mangelhaft unterstützt wird und auch bei der Unterstützung der Version 2.0 von SAML (und damit Liberty ID-FF) ca. 2 Jahre zwischen der Verabschiedung der Spezifikation und Verfügbarkeit einer entsprechenden Implementierung liegen.

Diejenigen der im Rahmen dieser Arbeit entstandenen Werkzeugprototypen, die direkt in den FIM-basierten Datenaustausch eingreifen, wurden auf Basis von Shibboleth und damit OpenSAML realisiert, wobei die SAML-Funktionsaufrufe durch Shibboleth so gekapselt werden, dass keine direkte Verarbeitung der XML-Daten notwendig wird.

3.4.3. Kurzübersicht über kommerzielle Produkte

Viele Hersteller von Identity & Access Management Software hatten schon seit längerem so genannte *Web Access Management (WAM)* Produkte in ihrem Portfolio. Die dabei ursprünglich eingesetzten proprietären Lösungen werden sukzessive durch FIM-standardbasierte Komponenten ersetzt. Die nachfolgende Liste gibt einen knappen Überblick über den aktuellen Stand der Unterstützung der FIM-Protokolle durch aktuelle Produkte von einigen ausgewählten, international bekannten Herstellern ohne Anspruch auf Vollständigkeit:

- Vom IBM Tivoli Federated Identity Manager werden SAML 2.0, Liberty ID-FF 1.1 und WS-Federation unterstützt.
- Microsoft zielt mit dem Active Directory Federation Service (ADFS) auf eine mit dem Management von Windows-basierten Servern stark verzahnte Lösung ab, die derzeit eine Teilmenge von WS-Federation unterstützt.
- Das Produkt Netegrity Siteminder, das im WAM-Bereich lange Zeit eine marktbeherrschende Stellung hatte, wurde rasch um die Unterstützung von SAML 2.0, Liberty ID-FF 1.2 und WS-Federation erweitert.
- Der Novell Access Manager unterstützt SAML 2.0 und Liberty ID-FF 1.2.
- Das Produkt Oracle Identity Federation ist für SAML 2.0 und Liberty ID-FF 1.2 zertifiziert und unterstützt mit dem Passive Requestor Profile eine Teilmenge von WS-Federation. Oracle betont insbesondere auch die Möglichkeit zum Einsatz als Attribute Authority.

[10] `http://lasso.entrouvert.org/`

- Der RSA Federated Identity Manager unterstützt SAML 2.0.
- Der Sun Java System Federation Manager basiert auf SAML 2.0, Liberty ID-FF 1.2 und Liberty ID-WSF 1.0.

Zahlreiche weitere Hersteller haben FIM-Funktionalität für die nächsten Versionen ihrer Produkte angekündigt. Allgemein zeichnet sich eine starke Affinität zu den Spezifikationen der Liberty Alliance ab, die aber noch nicht vollständig umgesetzt werden. Darüber hinaus wird deutlich, dass SAML 2.0 wesentlich rascher integriert wird als im Open Source Bereich, und dass die breite Unterstützung aller drei Ansätze angestrebt wird, um die von den Kunden geforderte möglichst weitreichende Interoperabilität zu erreichen.

3.5. Standards für Privacy Management

Wie in Abschnitt 3.2 dargelegt wurde, ist die Berücksichtigung von Datenschutzaspekten im Rahmen von FIM-Lösungen bei den Spezifikationen der Liberty Alliance weiter fortgeschritten als bei SAML und WS-Federation. Auch diese ist jedoch unzureichend, da lediglich Interaktionsmechanismen zur Genehmigung einzelner FIM-Transaktionen vorgesehen sind, während dedizierte Steuerungs- und Kontrollmechanismen wie Attribute Release Policies fehlen und keine administrativen Eingriffe, beispielsweise zur Spezifikation von Standard-Datenfreigaben, möglich sind.

In diesem Abschnitt werden zuerst mit P3P und EPAL zwei vom World Wide Web Consortium (W3C, `http://www.w3.org/`) gepflegte Ansätze vorgestellt, die dem Bereich Privacy Management zugeordnet werden können, der sich einerseits unabhängig vom Identity Management entwickelt hat, andererseits im FIM-Umfeld berücksichtigt werden muss. Nach einer Diskussion der von Shibboleth implementierten Attribute Release Policies, die als De-facto-Standard gelten und deren Defizite das in Abschnitt 5.3 vorgestellte Werkzeugkonzept motivieren, wird ein kurzer Überblick über Privacy-Forschungsansätze gegeben, die diese Arbeit mit beeinflusst haben und zum Teil in Kapitel 5 vertieft werden.

3.5.1. Platform for Privacy Preferences (P3P)

P3P [P3P, P3PIDM] ist eine nach mehrjähriger Entwicklungszeit seit 2002 standardisierte, XML-basierte Policysprache, in der Anbieter von Online-Diensten ihre Datenschutzerklärungen (engl. *Online Privacy Statements*), die nach aktueller Gesetzgebung in vielen Ländern auf den Webseiten des Dienstes veröffentlicht werden müssen, in einer maschinenlesbaren, formalen Sprache darstellen können. Diese Privacy Policies können somit von Webbrowsern automatisch abgerufen und ausgewertet sowie mit vom Benutzer vordefinierten Bedingungen – den *Privacy Preferences* – verglichen werden.

Primäres Ziel von P3P ist, die in Prosa formulierten, teils sehr umfangreichen Erklärungen auf Webseiten weitgehend abzulösen und den Benutzern den damit verbundenen Aufwand, umfangreiche Texte mit zum Teil juristischen Passagen zu lesen, zu ersparen.

P3P ist inzwischen relativ weit verbreitet und wird auch von vielen populären Service Providern unterstützt, ist jedoch mit folgenden grundlegenden Nachteilen verbunden:

- Die Sprache ist rein deklarativ, so dass die Umsetzung der angegebenen Privacy Policies nicht garantiert oder automatisch erzwungen werden kann.
- P3P kann die in Prosa formulierten Privacy Statements nicht komplett ersetzen, da diese aus juristischen Gründen weiterhin benötigt werden; beide Versionen der Privacy Policy müssen deshalb gepflegt und konsistent gehalten werden.

Über P3P-Policies kann im Wesentlichen kommuniziert werden, *welche* Daten *zu welchem Zweck* vom SP erfasst werden und *wie lange* sie von ihm aufbewahrt werden; hierzu wird eine Menge von Benutzerattributen und Verwendungszwecken vorgegeben, die jedoch sehr E-Commerce-spezifisch ist.

P3P wird durch die Policysprache **APPEL** [APPEL] komplementiert, mit der Benutzer ihre Anforderungen an die SP-seitigen Privacy Policies spezifizieren können. Ein Ziel dabei war, dass die so formulierten Benutzerpräferenzen beispielsweise an Internet-Suchmaschinen übergeben werden können, damit diese nur solche Webseiten als Suchergebnisse anzeigen, die den Anforderungen des Benutzers entsprechen.

Das folgende Beispiel zeigt eine APPEL-Regel, nach der ein Benutzer von seinem Webbrowser alarmiert werden soll, wenn ein Dienstleister ihm bekanntwerdende Informationen über seine finanziellen Verhältnisse (P3P-Kategorie *financial*) zu Kontaktaufnahme bzw. Marketing (P3P-Verwendungszwecke *contact* bzw. *telemarketing*) verwenden möchte:

```
<appel:RULE behavior="limited" prompt="yes" description="Finanzmarketing">
  <p3p:POLICY>
    <p3p:STATEMENT>
      <p3p:PURPOSE appel:connective="or">
        <p3p:contact required="always"/>
        <p3p:telemarketing required="always"/>
      </p3p:PURPOSE>
      <p3p:DATA-GROUP>
        <p3p:DATA>
          <p3p:CATEGORIES>
            <p3p:financial/>
          </p3p:CATEGORIES>
        </p3p:DATA>
      </p3p:DATA-GROUP>
    </p3p:STATEMENT>
  </p3p:POLICY>
</appel:RULE>
```

P3P und APPEL wurden in der Forschung zwar durchaus positiv aufgenommen, gelten aber auch für ihren eigentlichen Zweck als unzureichend:

- Die Ausdrucksmächtigkeit von P3P und APPEL ist zu eingeschränkt und viele intuitive Regeln sind nur sehr umständlich auszudrücken, da beispielsweise in APPEL nur negative Regeln, aber keine Positivlisten, z. B. für erlaubte Datenverarbeitungszwecke, formuliert werden können [ABLY04, XPREF].
- Dem von P3P vorgegebenen Auswertungsprozess fehlt eine Verhandlungsphase, so dass bereits minimale Interessenskonflikte zwischen SP und Benutzer die Dienstnutzung verhindern, während eventuell beide Seiten zu Zugeständnissen bereit wären. Eine entsprechende Erweiterung von P3P [Pre05] wurde vom W3C jedoch mit der Begründung abgelehnt, die Policysprache und die mit ihr verbundenen Prozesse so einfach wie möglich halten zu wollen, um Implementierungen zu erleichtern.

Im Hinblick auf im FIM-Umfeld einsetzbare Attribute Release Policies liefern P3P und APPEL somit wertvolle Anregungen bezüglich benötigter Sprachelemente, sind aber aufgrund der vorgegebenen Workflows, der Fixierung auf ein vorgegebenes Datenmodell und des Fehlens von Sprachelementen wie Obligationen nur unzureichend geeignet.

3.5.2. Enterprise Privacy Authorization Language (EPAL)

Die Enterprise Privacy Authorization Language (EPAL) wurde von IBM entwickelt und 2003 zur Standardisierung beim W3C eingereicht [PRISER, PRIPOL, EPAL12, EPALW3]. IBM Research pflegt mit der **Platform for Enterprise Privacy Practices** (E-P3P, [EP3P]) weiterhin eine echte Teilmenge der Sprache EPAL, die insbesondere für formale Analysen wichtige Kriterien wie die algebraische Abgeschlossenheit bei der Konjunktion von E-P3P-Policies erfüllt.

Im Unterschied zu P3P, das der Veröffentlichung von Datenschutzpolicies gegenüber Benutzern dient, zielt EPAL auf die organisationsinterne Spezifikation und das sichergestellte Erzwingen (**Policy Enforcement**) von Privacy Policies ab.

EPAL beschreibt hierzu

- formal eine XML-basierte Policysprache, wobei jede Policy aus einzelnen Regeln besteht, die wiederum auf Sprachelemente zur Angabe von Benutzerkategorien (engl. *data users*, d. h. Personenkreise, die auf die Daten zugreifen wollen, nicht Kategorien der erfassten Personen), Datenkategorien, Verarbeitungsarten, Verarbeitungszwecke sowie Bedingungen und Obligationen zurückgreifen. Im Unterschied zu P3P sind die Wertemengen, z. B. für Verwendungszwecke, nicht vorgegeben und können somit flexibel szenarienspezifisch gewählt werden.

- lediglich informell den prinzipiellen Aufbau einer PDP/PEP-basierten Autorisierungsarchitektur mit entsprechenden Workflows zur Policyauswertung, die sicherstellt, dass auf personenbezogene Daten nur von dazu berechtigten Stellen innerhalb der Organisation zugegriffen werden darf.

Analog zu P3P wurden EPAL und E-P3P in der Forschung positiv aufgenommen, jedoch hinsichtlich ihrer Ausdrucksmächtigkeit und der fehlenden Berücksichtigung von Policykonflikten kritisiert, wobei auch entsprechende Abwandlungen vorgeschlagen wurden [RS06, BMR04]. Darüber hinaus wurde die theoretisch beschränkte Performanz der Autorisierungsarchitektur bemängelt, die vor jedem Datenzugriff eine erneute Anfrage an den zentralen PDP vorsieht [ABLY04].

Beim kombinierten Einsatz von P3P und EPAL ergibt sich darüber hinaus die Schwierigkeit der manuellen Konsistenzhaltung der in den beiden Sprachen formulierten Policies, da P3P die SP-internen Verarbeitungsprozesse nicht berücksichtigt und EPAL nicht auf die Kundenperspektive eingeht.

Nachdem EPAL auf den SP-internen Einsatz zugeschnitten ist, eignet sich die Sprache nicht für die Spezifikation von IDP-seitigen Attribute Release Policies; für eine nahtlose Integration von FIM und I&AM auf Seite des SP ist EPAL jedoch geeignet zu berücksichtigen.

3.5.3. Attribute Release Policies in Shibboleth

Shibboleth ist der zeitlich erste Ansatz, der ARPs konzeptionell vorgesehen und implementiert hat [SHARPS]. Die verwendete XML-basierte Policysprache ist bewusst einfach gehalten und als Provisorium gedacht, bis insbesondere graphische Benutzeroberflächen für das ARP-Management zur Verfügung stehen, von denen die Benutzbarkeit und damit inhärent auch die anzustrebende Mächtigkeit der Policies abhängen.

Bei jeder Attributsabfrage werden in Shibboleth zwei ARPs ausgewertet:

- In der so genannten Site-ARP werden die vom Administrator vorgegebenen Voreinstellungen festgehalten, die für alle Benutzer gelten.
- Für jeden Benutzer existiert optional eine User-ARP, die auf Basis eines webbasierten Managementwerkzeugs wie ShARPE (vgl. Abschnitt 3.3.1.2) verwaltet werden soll.

Aus beiden Policies wird durch Konkatenation die so genannte ***effektive* ARP** gebildet, die wie folgt ausgewertet wird:

- Ein Benutzerattribut wird nur freigegeben, wenn dafür eine explizite Freigaberegel vorliegt; Anfragen nach Attributen, für die keine Freigaberegeln definiert wurden, werden deshalb abgelehnt.
- Sofern sich Site-ARP und User-ARP widersprechen, da beispielsweise die Site-ARP die Freigabe für ein Attribut vorsieht, die in der User-ARP abgelehnt wird, so wird das Attribut nicht freigegeben. Dies entspricht dem **Policykombinationsalgorithmus *„deny overrides“***, wodurch Benutzer die administrativ vorgegebenen Freigaben nur noch weiter einschränken, aber nicht überschreiben können.

Bereits dieses nur zweistufige Konzept schränkt die Flexibilität deutlich ein, da insbesondere nur eine einzige Site-ARP vorgesehen ist, die zentral administriert werden muss; eine Verteilung, beispielsweise auf organisationsweite Vorgaben, die dezentral standort- und abteilungsspezifisch verfeinert werden, ist somit nur mit großem manuellen Aufwand realisierbar.

Jede Shibboleth-ARP enthält beliebig viele Regeln, wobei jede Regel für genau ein Tupel (Service Provider; Service) gilt. Dieses Tupel entspricht der so genannten Provider-Id, die in den Shibboleth-Föderationsmetadaten als *entityID* festgehalten wird (vgl. Beispiel in Abschnitt 3.3.1.1); alternativ kann über das Sprachelement `AnyTarget` angegeben werden, dass die Regel für alle Dienste aller SPs gelten soll; zwischen verschiedenen Föderationen kann dabei nicht unterschieden werden.

In jeder Regel können beliebig viele Benutzerattribute aufgeführt werden, für die jeweils angegeben wird, ob sie dem Dienst übermittelt werden dürfen oder nicht. Diese Angabe kann durch eine optionale Bedingung verfeinert werden, wobei lediglich Vergleichsfunktionen (z. B. Vergleich von Zeichenketten auf Basis regulärer Ausdrücke) verwendet werden können. Der Einsatz dieses Sprachelements ist beispielsweise sinnvoll, um bei Personen, die verschiedene Rollen wie Student und Mitarbeiter einnehmen, nur die jeweils höherwertige freizugeben.

Das folgende Beispiel zeigt die Freigabe beliebiger Werte des Attributs `emailAddress` an einen ausgewählten SP:

```
<Rule>
  <Target>
    <Requester>
      https://sp.example.com/service-x
    </Requester>
  </Target>
  <Attribute name="emailAddress">
    <AnyValue release="permit"/>
  </Attribute>
</Rule>
```

Shibboleth-ARPs weisen eine Reihe von Defiziten auf, die den Einsatz der eXtensible Access Control Markup Language (XACML) als ARP-Sprache im Rahmen dieser Arbeit motivierten (vgl. Abschnitt 5.3):

- Die Unterscheidung von Erfassungs-/Datenverarbeitungszwecken wird nicht unterstützt.
- Die Angabe und Auswertung von Obligationen ist nicht vorgesehen.
- Die Ausdrucksmächtigkeit für Bedingungen ist gegenüber vielen anderen Policysprachen stark eingeschränkt, beispielsweise können keine externen Daten wie Datum und Uhrzeit verwendet werden.
- Attribute können nicht gruppiert werden und müssen einzeln freigegeben werden (z.B. Vorname, Nachname, Straße, Postleitzahl und Ort statt zusammenfassend „Anschrift“).

Im Rahmen des Projekts SPADE wurde ein alternatives, auf der Simple Public Key Infrastructure (SPKI, [SPKI]) und der Simple Distributed Security Infrastructure (SDSI, [SDSI]) basierendes ARP-Format für Shibboleth implementiert [SPADE], das S-Expressions statt XML verwendet [RL97]. Dieser Ansatz bietet insbesondere die Möglichkeit zur hierarchischen Anordnung von Policies, um ein dezentrales Management von Site-ARPs zu ermöglichen, und unterstützt die Unterscheidung mehrerer Rollen pro Benutzer; allerdings ist keine Angabe von Bedingungen an die Freigabe von Attributen möglich und auch die übrigen der oben aufgeführten Defizite gelten für SPADE.

3.6. Forschungsansätze für Privacy Management

Im Umfeld der Privacy Enhancing Technologies (PET) wurde die Notwendigkeit benutzergesteuerter Datenfreigaben bereits vor dem Entstehen von FIM-Ansätzen diskutiert, wobei sich generell eine starke Affinität zu policybasierten Lösungen abzeichnet. In den folgenden Abschnitten werden einige Arbeiten zur allgemeinen Fragestellung skizziert und das Konzept der *sticky Policies* sowie der *Idemix*-Ansatz näher erläutert.

3.6.1. Arbeiten zur Notwendigkeit benutzergesteuerter Datenfreigaben

Wie schon erläutert wurde, spielt die Kontrolle einer Person über diejenigen Daten, die über sie vorliegen und verarbeitet werden, bereits organisationsintern eine zentrale Rolle im Hinblick auf die Einhaltung von Datenschutzauflagen; mit dem Aufkommen der kommerziellen

Nutzung des Internets und dem Bekanntwerden von Sicherheitslücken, die zur Ausspähung der Kundendaten von E-Commerce-Websites ausgenutzt wurden, begann auch die wissenschaftliche Auseinandersetzung mit der organisationsübergreifenden Weitergabe personenbezogener Daten in der Informatik.

Bonatti und Samarati legten 2000 ein formal spezifiziertes Rahmenwerk vor, das eine Verhandlungsphase vor der Dienstnutzung vorsieht, in der die Anforderungen des Service Providers bezüglich benötigter Daten mit denen des Benutzers abgeglichen werden [INFREL]. Der wesentliche funktionale Unterschied zu P3P besteht in der **bedarfsorientierten Dynamik** der Verhandlungsphase, so dass der SP nicht seine vollständige Policy, sondern nur die individuell benötigten Teile bekanntgeben muss.

Bohrer et al. legten 2001 mit dem *myPrivacy* genannten Ansatz die architekturelle Grundlage für ein organisationsinternes Privacy Management von Kundendaten, auf der EPAL basiert [PERSIM]; das Konzept sieht insbesondere einige fest vorgegebene, vom Benutzer optional anzugebende Bedingungen und Obligationen vor, ohne diese Begriffe explizit zu verwenden oder zu vertiefen. Die Erweiterung der Anforderung an Policysprachen um **generische Obligationen** erfolgte erst parallel zum Entstehen von EPAL 2003 im Rahmen von Arbeiten, die auch von HP Research aufgegriffen wurden [IPPBAC, Mont04b, Mont04a], nachdem der Begriff von Bettini et al. geprägt wurde [BJWW02a, BJWW03, BJWW02b].

Diese Arbeiten haben die Gemeinsamkeit, schwerpunktmäßig die Seite des Service Providers zu betrachten und die benutzerseitigen Anforderungen nicht zu vertiefen; sie werden deshalb im Rahmen dieser Arbeit als komplementär zu IDP-seitigen Attribute Release Policies betrachtet.

B. Pfitzmann geht im Rahmen des BBAE-Ansatzes (siehe Abschnitt 3.3.2) auf konkrete Usabilityaspekte bei der Gestaltung von graphischen Oberflächen zur Datenfreigabesteuerung ein [BBAEPR]. Analog zu den früheren Richtlinien der Liberty Alliance liegt der Schwerpunkt dabei auf der interaktiven Genehmigung der Freigabe aktuell angeforderter Benutzerdaten; der Einsatz von ARPs wird in Erwägung gezogen, aber mit der Begründung nicht vertieft, dass viele Benutzer vermutlich damit überfordert sind, a priori Datenfreigaberegeln zu formulieren, und deshalb Interaktivität bevorzugen würden. Die praktische Umsetzung der Liberty Alliance Spezifikationen hat gezeigt, dass dieses Argument durchaus zutrifft, ARPs aber mindestens zur optionalen Speicherung bereits genehmigter FIM-Transaktionen benötigt werden, um eine den Benutzern lästig werdende ständig wiederkehrende Interaktion bezüglich derselben Dienste und Daten zu vermeiden (vgl. Abschnitt 3.2.2.2).

3.6.2. Sticky Policies

Der Begriff *sticky Policies* bezeichnet das Konzept, Daten und die sie betreffenden Policies untrennbar miteinander zu verknüpfen, und wurde von den Forschungsabteilungen von HP und IBM geprägt [STICKY, Mont04c, MTCB05].

Der Ansatz wurde ursprünglich entwickelt, um Privacy Policies besser versionieren zu können: Er stellt sicher, dass Daten nur unter genau denjenigen Auflagen verarbeitet werden, unter denen sie erfasst wurden, auch wenn sich die Policies zwischenzeitlich geändert haben; diese Eigenschaft wird insbesondere bei langlebigen Prozessinstanzen wie beispielsweise der Aufbewahrung von Patientenakten benötigt.

Beim organisationsübergreifenden Datenaustausch haben sticky Policies den Vorteil, dass der Empfänger der Daten explizit auf Einschränkungen bezüglich erlaubter Verwendungszwecke und entsprechende Obligationen hingewiesen wird, wodurch zumindest unbeabsichtigtem Missbrauch vorgebeugt werden kann.

Die Übertragung von sticky Policies und ihre geeignete Auswertung durch einen Policy Enforcement Point auf Empfängerseite sind in den existierenden FIM-Ansätzen derzeit noch nicht vorgesehen; in dieser Arbeit wird die Unterstützung von sticky Policies als Anforderung an das ARP-Konzept in Abschnitt 5.3 betrachtet, wobei die Policies selbst zusammen mit den SAML Attribute Assertions übertragen werden können, die der Empfänger entsprechend auswerten muss.

3.6.3. Idemix

Idemix ist ein Ansatz von IBM Research, der zur annullierbaren anonymen oder pseudonymen Dienstnutzung im UCIM-Umfeld konzipiert wurde [IDEMIXa, IDEMIXb].

Die personenbezogenen Daten des Benutzers werden dabei eingangs nur einem Treuhanddienst zur Verfügung gestellt, der dem Benutzer ein Pseudonym zuweist, mit dem dieser den gewünschten Dienst regulär nutzen kann. Lediglich bei Missbrauchs- oder Notfällen kann der Dienstleister vom Treuhanddienst die Herausgabe der dort über den Benutzer gespeicherten Daten verlangen.

Im Rahmen von Idemix wurde darüber hinaus der Einsatz kryptographischer Methoden untersucht, auf deren Basis der Treuhanddienst dem Benutzer analog zu UCIM-Diensten Attributszertifikate ausstellen kann, die dem Dienstleister zur Bestätigung ausgewählter Eigenschaften des Benutzers vorgelegt werden können, ohne dessen Anonymität zu gefährden: Beispielsweise kann dem Dienstleister versichert werden, dass der Benutzer im Besitz eines Führerscheins ist, ohne dass ihm dieser mit allen darin enthaltenen Angaben vorgelegt werden muss.

Insgesamt kann Idemix somit als Identity Provider mit Schwerpunkt auf pseudonymer Dienstnutzung betrachtet werden, wobei mit der möglichen Herausgabe der personenbezogenen Daten durch den Treuhanddienst organisatorische und juristische Implikationen verbunden sind, die noch nicht abschließend untersucht worden sind.

Da der Schwerpunkt dieser Arbeit nicht auf pseudonym nutzbaren Diensten liegt, wird der Idemix-Treuhanddienst im Weiteren lediglich als Sonderfall von IDPs betrachtet.

3.7. Ansätze für Federated User Provisioning

Wie in Kapitel 2 gezeigt wurde, benötigt eine Vielzahl von Diensten lokal gespeicherte Benutzerprofile; neben Legacy-Diensten, die zentrale Benutzerdatenbestände aus technischen Gründen nicht nutzen können, gehören hierzu insbesondere sehr systemnahe Dienste wie die Bereitstellung von CPU-Kapazitäten im Umfeld des Grid-Computings.

Die Nutzung solcher Dienste über FIM ist folglich nur möglich, wenn diese Daten nicht nur zum Service Provider übertragen, sondern dort auch in die jeweiligen Zielsysteme eingespeist werden; analog zum im Abschnitt 2.1.1.3 vorgestellten User Provisioning in I&AM-Systemen wird diese Zielsetzung im FIM-Kontext als *Federated User Provisioning* (FUP) bezeichnet.

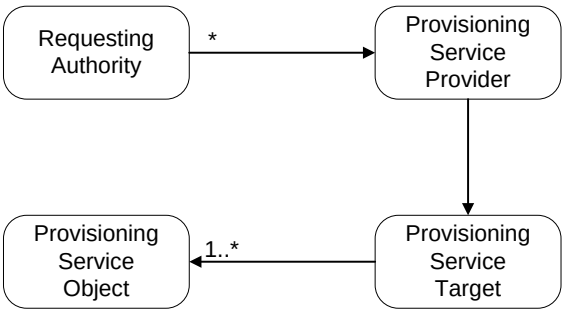


Abbildung 3.4.: Grobe Architektur und Terminologie der Service Provisioning Markup Language

Im Folgenden werden erste Lösungsansätze, die potentiell dazu eingesetzt werden könnten, die Funktionalität der in Abschnitt 3.2 vorgestellten FIM-Standards um FUP zu ergänzen, skizziert.

3.7.1. Service Provisioning Markup Language (SPML)

Die Service Provisioning Markup Language (SPML, [SPML20]) ist wie SAML ein Standard der OASIS und spezifiziert eine XML-basierte Sprache, mit der Anfragen zum Anlegen, Modifizieren, Löschen und Suchen von Benutzerprofilen und entsprechende Antworten formuliert werden können. Die 2003 veröffentlichte Version 1.0 wurde unter anderem um Bulkoperationen zur Unterstützung mehrerer Profile pro Operation erweitert, so dass seit 2006 Version 2.0 vorliegt.

Die Architektur von SPML sieht wie in Abbildung 3.4 dargestellt vor, dass so genannte Requesting Authorities (RA) SPML-Anfragen an einen als Provisioning Service Provider (PSP) bezeichneten Dienst stellen, der sie an das betroffene Provisioning Service Target (PST) weiterleitet, von dem mindestens ein Provisioning Service Object (PSO) verwaltet wird.

SPML wurde ursprünglich für den organisationsinternen Einsatz konzipiert und wird erst seit der weiteren Verbreitung von SAML im FUP-Kontext diskutiert. Eine massive grundlegende Einschränkung besteht darin, dass SPML **kein Autorisierungskonzept** aufweist, so dass nicht geregelt wird, welche RAs welche Arten von Anfragen an PSPs stellen dürfen; die Spezifikation überlässt diesen Aspekt explizit den Softwareherstellern, wodurch keine organisationsübergreifende Interoperabilität gewährleistet wird.

Während SPML 1.0 die Arten anzuschließender Dienste durch die feste Vorgabe eines Informationsmodells, das beispielsweise Name und E-Mail-Adresse des Benutzers enthielt, eingeschränkt hat, wurde SPML 2.0 wesentlich flexibilisiert, so dass eigene Datenmodelle verwendet werden können und das von SPML 1.0 verwendete nur noch als Vorschlag dient.

Aufgrund des Ansatzes, Benutzerprofile direkt beim jeweiligen Dienst anzulegen, ergeben sich im Wesentlichen die folgenden Schwierigkeiten:

- SPML stellt eine Funktionalität bereit, die die erläuterten FIM-Protokolle logisch ergänzt; durch die mangelnde Integration von SPML mit diesen Protokollen müssten praktisch jedoch beide Lösungen parallel betrieben oder es muss auf die übrige FIM-Funktionalität verzichtet werden.

- Die SPML Request Authority muss die zu speisenden Provisioning Targets und ihre Anforderungen sowie Abhängigkeiten im Detail kennen, um entsprechende Anfragen korrekt formulieren zu können; dies betrifft neben dem notwendigen Namensraum für Objekte auch Dienstabhängigkeiten und dienstspezifische Datenschemata. Der Service Provider muss somit einen tiefen Einblick in seine internen Strukturen gewähren, was im Allgemeinen unerwünscht ist und mit einem äußerst komplexen organisationsübergreifenden Change Management verbunden wäre.

- SPML berücksichtigt ebenso wenig wie die FIM-Standards das potentielle Vorhandensein eines SP-lokalen I&AM-Systems, das durch das direkte Provisioning eines Dienstes schlichtweg umgangen werden würde.

SPML bietet sich somit neben organisationsinternem User Provisioning primär für Outsourcingszenarien an, in denen der als SPML RA fungierende Kunde volle Kontrolle über die bereitgestellten Dienste und Ressourcen haben soll und eine feingranulare Autorisierung unabhängig von SPML intern vornimmt. Es stellt darüber hinaus ein standardisiertes, herstellerunabhängiges Protokoll für den Einsatz in Konnektoren dar (siehe Kapitel 4).

3.7.2. Web Services Provisioning (WS-Provisioning)

Vergleichbar mit dem Verhältnis von WS-Federation zu SAML stellt WS-Provisioning eine von IBM und Microsoft vorgeschlagene Alternative zu SPML dar, die auf dem Web Services WS-*-Protokollstack aufbaut [WS-Pro].

WS-Provisioning lehnt sich dabei bewusst so stark an SPML 1.0 an, dass die dort definierten Use Cases und Fachbegriffe explizit übernommen wurden.

Der Ansatz weist somit dieselben Probleme wie SPML auf wird derzeit nicht aktiv weiterentwickelt; im Rahmen dieser Arbeit wird er deshalb als eingeschränkte Alternative zu SPML mit bevorzugtem Einsatz in Szenarien mit starker WS-*-Affinität betrachtet.

3.7.3. Grid-Middleware

Das User Provisioning im Grid-Umfeld, das auch im Rahmen von Szenario 4 in Kapitel 2 diskutiert wurde, unterscheidet sich durch die folgenden Einschränkungen deutlich von generischem FUP:

- Bei den bereitzustellenden Diensten handelt es sich derzeit primär um CPU- und Datenspeicherkapazitäten, die einerseits sehr (betriebs-)systemnah sind und andererseits lediglich minimale Benutzerprofile (z. B. Username und Passwort, ggf. dienstübergreifend einheitliche numerische User-ID) erfordern.

- Die selektive partielle Verschmelzung realer Organisationen zu einer virtuellen Organisation ist mit der Delegation von Rechten verbunden, so dass aus logischer Sicht eine VO-interne User-Provisioning-Lösung ausreicht.

Die Durchführung des User Provisionings kann dabei prinzipiell den Aufgaben der eingesetzten Grid-Middleware zugeordnet werden, auch wenn in bestehenden Grids wie DEISA noch eine davon unabhängige Infrastruktur aufgebaut wurde (vgl. Szenario 4). Dies ist im Wesentlichen auf die bislang noch sehr einfach gehaltenen technischen Lösungen zurückzuführen:

- In der exemplarisch gewählten Middleware *Globus Toolkit 4* muss ein so genanntes Mappingfile zwischen Grid-Benutzern und lokal angelegten Kennungen gepflegt werden. Das Anlegen von Kennungen und die Pflege des Mappingfiles geschieht auf Anfrage manuell durch einen Administrator oder wie in DEISA durch Administrations-Skripte automatisch in regelmäßigen Abständen. Diese Vorgehensweise schränkt die mögliche Dynamik stark ein, kommt jedoch dem vorherrschenden Bedürfnis nach lokaler Hoheit über die Ressourcen („Locality over globality“) entgegen.
- Alternativ dazu können *alle* über ein Grid eingebrachten Programmabläufe (sog. Grid Jobs) unter *einer* gridspezifischen Kennung pro Service Provider ausgeführt werden, wobei eine vom Dienst unabhängige externe Instanz für das Accounting individueller Benutzer zuständig ist. Bei dieser Variante verliert der SP jedoch die unmittelbare Kontrolle über zugelassene Benutzer auf Ebene der von ihm angebotenen Dienste.

In Entwicklung befindliche Ansätze sehen vor, dass einer middlewarespezifischen unpersönlichen Kennung eingeschränkte administrative Rechte gegeben werden, mit der Kennungen für neue Gridbenutzer bei Bedarf dynamisch eingerichtet werden können; dabei besteht insbesondere die Bestrebung, weitere Benutzerinformationen auf Basis einer ans Grid-Umfeld angepassten Version von Shibboleth namens GridShib zur Verfügung zu stellen [GRDSHB, BBF+06].

3.8. Ansätze für interoperable Informationsmodelle

Der FIM-basierte Austausch von Identitätsinformationen setzt wie jeder andere zielorientierte Kommunikationsprozess ein gemeinsames Verständnis von Syntax und Semantik der übertragenen Datenelemente voraus. Während die FIM-Standards die Datenformate von Authentifizierungsinformationen exakt vorgeben und die Übertragung von Autorisierungsinformationen im Wesentlichen lediglich um einen gemeinsamen Namensraum für geschützte Dienste ergänzt werden muss, leidet die organisationsübergreifende Übermittlung allgemeiner Attributsauskünfte häufig am Fehlen eines gemeinsamen Informationsmodells.

Die historische, untereinander nicht koordinierte Entwicklung der Softwarekomponenten für organisationsinternes Identity Management durch verschiedene Hersteller hat dazu geführt, dass viele I&AM-Produkte bei einer Standardinstallation eigene Datenmodelle, beispielsweise in Form von LDAP-Schemata, verwenden. In der Regel unterscheiden sich hier beispielsweise die *Namen* von Benutzerattributen, die *Syntax* z. B. von Datumsangaben, und die *Semantik* von Attributen, beispielsweise hinsichtlich der Erfassung des ersten im Gegensatz zur Erfassung aller Vornamen einer Person in einem Attribut.

Diese herstellerbedingten Differenzen bei der Modellierung der Stamm- und Kontaktdaten von Benutzern sind manuell meist trivial zu korrigieren, verhindern aber de facto den unmittelbaren Einsatz der in Abschnitt 3.2 diskutierten FIM-Protokolle, da keines davon die Anforderung [FA-Schema] erfüllt, die eine entsprechende Datenkonvertierung ermöglichen würde. Dieses Problem wird in der Praxis dadurch verschärft, dass viele Organisationen eigene Ergänzungen an den von den Softwareherstellern vorgegebenen Datenmodellen durchführen, und dass die Semantik, beispielsweise von Rollenbezeichnungen wie „Projektleiter“, je nach Organisation völlig unterschiedlich sein kann, so dass daraus bei jedem Föderationsteilnehmer z. B. unterschiedliche Berechtigungen abgeleitet werden müssen.

Im nachfolgenden Abschnitten werden deshalb einerseits Standardisierungsbemühungen um einheitliche Informationsmodelle betrachtet und andererseits Ansätze zur möglichst weitgehend automatisierten Konvertierung von in unterschiedlichen Formaten vorliegenden Identitätsdaten skizziert.

3.8.1. Standardisierte LDAP-Objektklassen

Wie in Abschnitt 2.1.1 erläutert wurde, werden in I&AM-Systemen bevorzugt LDAP-basierte Verzeichnisdienste und nicht z. B. relationale Datenbanken als Identity Repositories eingesetzt. Durch das Ziel, Endgeräte wie organisationsinterne Benutzerarbeitsplätze möglichst direkt mit dem zentralen Datenbestand zu koppeln, hat sich schon früh der Bedarf an einem plattform- und betriebssystemunabhängigen LDAP-Schema zur grundlegenden Verwaltung von Benutzern und deren Zugangsdaten für Rechner ergeben.

Die Internet Engineering Taskforce (IETF) hat in den Jahren 1998 und 2000 deshalb die LDAP-Objektklassen `posixAccount` [RFCPXA] und `inetOrgPerson` [RFCIOP] in Form von RFCs (Requests for Comments, entspricht IETF-Standardspezifikationen) herausgegeben, mit denen neben systemnahen Einstellungen wie dem Pfad zum Home-Directory des Benutzers auch Kontaktinformationen wie E-Mail-Adresse und Telefonnummer festgehalten werden können. Während sich `posixAccount` weitgehend durchgesetzt hat, eignet sich `inetOrgPerson` meist nur mit Erweiterungen für vollwertiges Identity Management, da beispielsweise zur Personenkorrelation häufig benötigte Attribute wie *zweiter* bzw. *weitere Vornamen* und *Geburtsname* fehlen.

Im Rahmen der US-amerikanischen Internet2-Initiative entstand ferner die LDAP-Objektklasse `eduPerson` [EDUPER], die zur Verwaltung von Hochschulangehörigen verwendet werden kann. Die Kombination aus `inetOrgPerson` und `eduPerson` hat sich insbesondere durch den Einsatz von Shibboleth inzwischen zur organisationsübergreifenden Datenübertragung im Hochschulumfeld durchgesetzt; dabei werden außerhalb der USA Attribute wie `nickname` (Spitzname) nur selten verwendet, wohingegen beispielsweise Studiengangsinformationen wie Haupt- und Nebenfächer fehlen und wie andere lokal benötigte Attribute durch Schemaerweiterung ergänzt werden müssen. Für den Einsatz im deutschen und europäischen Hochschulumfeld wurden deshalb Arbeitskreise gegründet, die zum Ziel haben, ein auf `eduPerson` basierendes, an die regionalen Gegebenheiten angepasstes Schema zu spezifizieren (vgl. [DEEP, SCHAC]).

3.8.2. Liberty Alliance Profile

Wie bereits in Abschnitt 3.2.2.1 erwähnt wurde, arbeitet die Liberty Alliance an der Standardisierung der so genannten Personal und Employee Profiles, die auf Anwendungen für private Endkunden bzw. Business-to-Business Applikationen zugeschnitten sind.

Neben allgemein üblichen Stamm- und Kontaktinformationen sind in diesen Datenmodellen Attribute wie `GreetMeSound` (URL einer Audiodatei, mit deren Abspielen der Benutzer beim Beginn der Dienstnutzung begrüßt werden soll) vorgesehen, die die Ausrichtung auf die Liberty ID-SIS Dienste verdeutlichen. Als weitere Besonderheit werden Daten redundant vorgehalten, um die Auswertung der Daten durch Applikationen zu erleichtern; beispielsweise wird neben dem Geburtsdatum auch explizit das daraus ableitbare Alter der Person als separates Attribut gespeichert und muss entsprechend konsistent gehalten werden.

Die Liberty Alliance verfolgt insgesamt die in sich abgeschlossene Strategie, neben dem Informationsmodell (ID-WSF Profile) auch die Funktions- und Kommunikationsmodelle (ID-SIS Spezifikationen) der unterstützten Anwendungen vorzugeben. Die Verwendung und Erweiterung dieser Profile in anderen Szenarien ist möglich, hierzu liegen jedoch noch keine Erfahrungen vor.

3.8.3. Weitere Standardisierungsbemühungen

Das von P3P (vgl. Abschnitt 3.5.1) vorgegebene Datenmodell ist zwar aufgrund seiner E-Commerce-spezifischen Ausrichtung ebenso wenig universell einsetzbar wie die anderen erläuterten Ansätze, geht jedoch über die rein syntaktische Spezifikation der Attribute hinaus, indem Wertemengen – beispielsweise für Datenverarbeitungszwecke – samt Semantik vorgegeben werden. Dadurch wird einerseits die Interoperabilität erleichtert, andererseits sind diese Vorgaben je nach Szenario zwangsweise unvollständig, so dass wiederum nichtstandardisierte Erweiterungen vorgenommen werden müssen.

Auch in anderen Bereichen, die nicht direkt mit Identity Management in Zusammenhang gebracht werden, existieren zum Teil standardisierte Ansätze zur Modellierung von Benutzern. Beispielsweise spezifiziert die Distributed Management Task Force (DMTF) im Rahmen des **Common Information Models** (CIM) unter anderem das CIM User Schema.[11] Es bietet neben einer Vielzahl von Attributen insbesondere auch Konzepte zur Verwaltung von Gruppen- und Rollenzugehörigkeiten und stellt somit neben den IETF-Standards eine gute Ausgangsbasis für szenarienspezifische Anpassungen dar.

Die Abschnitte 3.8.1–3.8.3 zusammenfassend ist anzumerken, dass die organisationsinterne Verwendung standardisierter Schemata den organisationsübergreifenden Datenaustausch erleichtern kann, aufgrund der Vielzahl möglicher Kombinationen aus herstellerspezifischen und -unabhängigen Schemata und notwendigen Erweiterungen aufgrund additiver lokaler Anforderungen jedoch keine Voraussetzung dafür sein darf.

Bei der Erarbeitung föderationsweiter Datenmodelle stellen die erwähnten herstellerunabhängigen Datenmodelle eine solide, neutrale Ausgangsbasis dar, so dass der Fokus auf szenarienspezifischen Erweiterungen liegen kann; es ist davon auszugehen, dass mit zunehmender Reife

[11] `http://www.dmtf.org/standards/cim/`

von FIM weitere branchenspezifische Standards wie `eduPerson` für das Hochschulumfeld und CIM für das Management vernetzter Rechner geschaffen werden.

Damit verbleibt jedoch weiterhin die Herausforderung, die Daten zwischen dem organisationsinternen und dem föderationsweiten Format zu konvertieren, da im Allgemeinen nicht von einer durchgehenden Homogenität ausgegangen werden kann.

3.8.4. Vorgehensweisen in föderierten Datenbanken

Als Alternative zur im Identity Management Umfeld derzeit häufig gewählten Strategie, für organisationsübergreifenden Datenaustausch auf ein standardisiertes, herstellerunabhängiges Datenmodell zurückzugreifen, bieten sich Techniken aus dem Datenbankbereich an.

Insbesondere im Umfeld föderierter Datenbankenmanagementsysteme (FDBMS), die sich gegenüber den ebenfalls verteilten, so genannten parallelen Datenbanken durch ihre Heterogenität auszeichnen, werden Techniken zur gemeinsamen Nutzung in unterschiedlichen Formaten vorliegender Daten bereits seit längerer Zeit untersucht.

Die FIM-spezifische Problemstellung ist dabei bei Weitem nicht so komplex wie beispielsweise bei zentralen Unternehmensdatenbanken mit Milliarden abgewickelter Transaktionen, die im Rahmen von Firmenfusionen konsolidiert und integriert werden müssen.

In der Literatur wird allgemein zwischen den folgenden beiden Lösungsansätzen unterschieden, für die jeweils verschiedenste, an dieser Stelle nicht näher diskutierte Realisierungsvarianten existieren:

1. Bei der klassischen **Schema-Integration** wird in einem technisch wie organisatorisch aufwendigen Prozess ein gemeinsames Datenschema gefunden und in allen angeschlossenen Datenbanken implementiert [BLN86, CRE87]. Dieser Prozess muss bei jedem Hinzufügen einer neuen Datenbank oder bei Änderungen an einer bestehenden Datenbank wiederholt werden; im Worst Case ist der Aufwand dafür exponentiell [SS05].

   Im Hinblick auf die angestrebte hohe Dynamik von Föderationen ist dieser Ansatz nur sehr bedingt brauchbar, da der Aufwand zur Integration neuer Föderationsteilnehmer insbesondere für die Bestandsmitglieder minimal sein sollte.

2. Bei der **Schema-Koordination** wird eine Abbildungstabelle (engl. *Attribute Correspondence Matrix*) erstellt, auf deren Basis die Anfragen an die einzelnen Datenbanken des FDBMS so umformuliert werden, dass sie deren lokale Datenschemata verwenden; analog dazu werden die von jeder beteiligten Datenbank gelieferten Antworten wieder zurück in das Schema des Anfragestellers konvertiert [SCFDBM]. Der manuelle Aufwand beim Hinzufügen weiterer Datenbanken reduziert sich somit im Wesentlichen auf die Definition eines Mappings zwischen deren Datenschemata und einem virtuellen Gesamtschema, das zur Formulierung der Anfragen verwendet wird [DLC03].

   Dieser Ansatz ist im Hinblick auf FIM mit einem einmaligen Implementierungsaufwand für die Datenkonvertierungskomponente verbunden, die Komplexität bei der Anwendung steigt dafür jedoch nur noch linear mit der Anzahl hinzukommender Föderationsteilnehmer.

Aufgrund der Heterogenität der I&AM-Lösungen und der praktischen Unmöglichkeit, ein einziges Datenschema für alle Föderationen und alle lokal eingesetzten Softwarekomponenten zu verwenden, ist der zweite Ansatz im Rahmen von FIM klar vorzuziehen. In Abschnitt 5.2 wird das Konzept für ein entsprechend an FIM angepasstes Werkzeug, das flexibel in die Föderationsverwaltung integriert werden kann, vorgestellt.

3.8.5. Ontologiebasierte Ansätze

Ontologien haben unter anderem das Ziel, über die explizite formale Spezifikation von gegenseitigen Abhängigkeiten und Beziehungen neben der Syntax auch die Semantik von Datenmodellen zu definieren. Als **Ontology Mapping** wird die Aufgabe bezeichnet, zwei oder mehr Ontologien aufeinander abzubilden; dies kann stark vereinfacht mit der im vorangegangenen Abschnitt beschriebenen Schema-Koordination verglichen werden.

Auch Forschungsarbeiten im Umfeld des Identity Managements befassen sich zunehmend mit dem Einsatz von Ontologien, die beispielsweise für das P3P-Datenmodell, allgemeine Autorisierungsinformationen und das Vokabular für in Policies verwendeten Bedingungen definiert worden sind (siehe [P3PSEM, PARADI, ADdV$^+$05]). Die ontologiebasierte Steuerung der von I&AM-Konnektoren zwischen Quell- und Zielsystem durchgeführten Konvertierung von Attributsnamen wird von Abeck und Emig untersucht [ELBA07] und hat zum Ziel, den manuellen Aufwand bei der szenarienspezifischen Konfiguration von Konnektoren diesbezüglich zu minimieren.

Im Rahmen der in dieser Arbeit entwickelten Konzepte wird auf die Verwendung von Ontologien jedoch aus folgenden Gründen nicht näher eingegangen:

- Die Ansätze zur automatisierten Erstellung von zuverlässigen, korrekten Ontology Mappings sind bislang nur unter sehr restriktiven Randbedingungen ausgereift, deren Einhaltung im Einzelfall zu prüfen wäre.
- Der Aufwand zur manuellen Erstellung von Ontology Mappings ist größer als derjenige zur Spezifikation entsprechender Konvertierungsregeln zwischen Datenschemata, die nur eine Teilmenge der Ontologien darstellen.
- Die Hauptanwendungsgebiete von Ontologien, z. B. Reasoning und Knowledge Mining, werden im Kontext dieser Arbeit nicht benötigt.
- Auch das Ableiten einer gemeinsamen Ontologie für alle Föderationsteilnehmer würde nur einen Teil des Problems lösen, da zu integrierende, proprietäre Systeme praktisch gar nicht und viele andere Systeme nur mit beträchtlichem Aufwand an ein gemeinsames, homogenes Datenmodell angepasst werden könnten.

Das in Abschnitt 5.2 vorgestellte Werkzeugkonzept verwendet entsprechend keine Ontologien, kann jedoch mit zunehmender Reife entsprechender Verfahren angepasst oder erweitert werden.

3.8.6. Enterprise Application Integration (EAI)

Das Gebiet der Enterprise Application Integration (EAI) befasst sich mit der Zusammenführung heterogener Anwendungen und deren Nutzdaten unter starker Geschäftsprozessorientierung. Im Unterschied zur herkömmlichen Datenintegration, die die Nutzung eines gemeinsamen Datenmodells durch alle Softwarekomponenten erzwingen sollte, wird dabei verstärkt auf Adapter zwischen den Systemen gesetzt, deren Funktionalität mit I&AM-Konnektoren vergleichbar ist, ohne dass eine Beschränkung auf Identitätsinformationen vorliegt.

Die technische Umsetzung erfolgt dabei in der Regel über ein EAI-herstellerspezifisches Zwischenformat, das eine Obermenge der unterstützten Datenformate darstellt; zur Programmierung der Adapter zwischen dem EAI-System und den anzuschließenden Applikationen werden Frameworks und Funktionsbibliotheken bereitgestellt, deren Komplexität diejenige der entsprechenden Schnittstellen von Meta-Directories (vgl. Abschnitt 2.1.1.5) bei Weitem übertrifft.

EAI setzt somit primär auf Methoden, die sich im Hinblick auf Identity Management mit den bereits im I&AM-Umfeld eingesetzten decken und bei FIM zu den in Abschnitt 2.2.1.2 diskutierten Problemen führen. Aus diesem Grund wird in den Kapiteln 4 und 5 nicht auf EAI zurückgegriffen.

3.9. Entwicklungen beim User-Centric Identity Management

Das in Abschnitt 2.1.3 diskutierte UCIM wird als jüngste Identity Management Disziplin derzeit am stärksten vorangetrieben. Nachfolgend werden die aktuellen UCIM-Ansätze und ihr Bezug zu FIM-Protokollen knapp vorgestellt:

- **Microsoft Cardspace** (vgl. Szenario 2) findet durch seine direkte Integration in die Betriebssystemfamilie Microsoft Windows eine weite benutzerseitige Verbreitung und erleichtert die Verwendung durch eine intuitiv bedienbare graphische Benutzeroberfläche, die mit keinem Installationsaufwand verbunden ist. Cardspace bietet alle in dieser Arbeit betrachteten UCIM-Funktionalitäten (siehe Abschnitt 2.1.3) und deckt die zwar von Microsoft definierten, aber breit diskutierten und allgemein anerkannten „7 Laws of Identity“ ab, die auf einen herstellerunabhängigen, interoperablen Ansatz mit starker Integration der Benutzer in die Datenaustauschprozesse abzielen [LAWS]. Cardspace wird deshalb im Folgenden als Referenz für UCIM-Ansätze betrachtet und bringt die aus Szenario 2 abgeleiteten Anforderungen an FIM ein.

- Das **Digital Identity eXchange** (DIX, [DIX]) Protokoll wird von der IETF spezifiziert und gibt eine Reihe von nur sehr knapp beschriebenen Use Cases vor, die auf UCIM-Systeme im Allgemeinen angewendet werden können [DIXUSE]. Als Implementierung mit Schwerpunkt auf der Bereitstellung der SP-seitigen Komponenten für verschiedene Plattformen liegt **SXIP** vor [SXIPOV, SXIPIN, SXIP20].

  Ursprünglich wurde DIX als leichtgewichtige, UCIM-spezifische Alternative zu SAML konzipiert, nähert sich mit wachsenden Anforderungen aber immer stärker an eine Erweiterung von SAML um neue Nachrichtentypen, Bindings und Profile an, die ausschließlich auf webbasierte Anwendungen (und nicht Web Services) spezialisiert ist.

Als Identity Provider (ursprünglich als DIX Homesite bezeichnet) kommt dabei eine vom Benutzer betriebene Webanwendung zum Einsatz, deren URL beim Service Provider (ursprünglich DIX Membersite) manuell eingegeben werden muss; sie ist für die Speicherung der Benutzerattribute und das Erzeugen von Antwortnachrichten an den Service Provider im entsprechenden Format (ursprünglich DIX-spezifisch, inzwischen SAML Assertions) zuständig.

DIX erweitert SAML um zwei Nachrichtentypen: Mittels „**DIX Store Request**“ und „**DIX Store Response**“ kann ein schreibender Zugriff auf den beim IDP hinterlegten Datenbestand realisiert werden, wobei der Benutzer diesem Zugriff explizit zustimmen muss, so dass die Anforderungen [FA-Schreibzugriff] und [DSA-Schreibzugriff] erfüllt werden.

Die DIX-Spezifikationen sind jedoch noch unvollständig und stark im Fluss: Als nächster Schritt ist die Fusion mit den unten genannten OpenID-Spezifikationen geplant, so dass zum zukünftigen Funktionsumfang und praktischen Einsatz noch keine Aussagen getroffen werden können.

- **OpenID** [OpenID] ist ein weiterer Ansatz, der ursprünglich bewusst sehr einfach gehalten wurde, mit laufender Weiterentwicklung jedoch ständig komplexer wird. Er sieht vor, dass jeder Benutzer eindeutig über den URL seiner persönlichen Webseite identifiziert wird und gibt in Version 1.0 neun Benutzerattribute vor, die vom SP abgefragt werden konnten.

  In Version 2.0 ist die Anzahl abzufragender, nach wie vor fest vorgegebener Attribute auf über 50 gestiegen, wobei dazu auch Metadaten wie der Zeitpunkt der Authentifizierung des Benutzers gehören. Seit der Standardisierung von SAML 2.0 erfolgt eine kontinuierliche Annäherung an SAML; die architekturelle Ähnlichkeit mit SXIP, bei der die Benutzer auf ihrer Webseite den „OpenId Server“ betreiben, motivierte die anstehende Zusammenführung mit DIX.

- Mit **LID**[12] und **XDI/XRI** [XDI] existieren zwei weitere Ansätze, die jedoch explizit nur auf Single Sign-On bzw. die Identifizierung von Identitäten ausgelegt sind.

  Die Vielzahl von Ansätzen, die Benutzer auf Basis von URLs identifizieren, hat dazu geführt, dass SPs, die mehrere Varianten unterstützen wollten, zusätzlich zu einem Eingabefeld für den URL auch eine Auswahlliste für das Verfahren benötigten; als Alternative wurde mit **Yadis** [YADIS] ein SP-seitiges Loginmodul entwickelt, das eine einheitliche Schnittstelle zum Benutzer darstellt und intern mehrere Protokolle wie OpenID und LID unterstützt.

  Insbesondere kann auch der Ansatz **mIDm** [MIDM] mit Yadis verwendet werden, der für die Identifikation von Benutzern zwar ebenfalls URLs verwendet, die jedoch nicht manuell beim SP eingegeben werden müssen, sondern als Suffix des bei HTTP übermittelten Clientnamens (i.d.R. Name und Version des verwendeten Webbrowser) mitgeschickt werden. mIDm hat jedoch noch keine weite Verbreitung gefunden, da die clientseitige Konfiguration noch nicht von allen Webbrowsern unterstützt wird und die Verwendung unterschiedlicher Rollen oder Pseudonyme bei mehreren parallel genutzten Webdiensten nicht möglich ist.

[12] `http://lid.netmesh.org/`

Insgesamt hat sich somit eine recht große Zahl von UCIM-Ansätzen gebildet, deren Funktionsumfang sich jedoch stark ähnelt und noch relativ beschränkt ist, so dass sich daraus nur wenige Anregungen für FIM ergeben. Es ist darüber hinaus zu erwarten, dass die UCIM-Protokolle mittelfristig noch stärker konsolidiert werden, wobei insbesondere SAML Assertions ein großes Potential als gemeinsames Datenaustauschformat aufweisen, so dass mittelfristig ein interoperabler Einsatz von FIM und UCIM möglich erscheint.

3.10. Zusammenfassung und Bewertung

Die vorgestellten Industrie- und De-facto-Standards SAML, Liberty Alliance, WS-Federation und Shibboleth spiegeln den aktuellen Stand der Technik im FIM-Umfeld wider und sind bereits durchaus für den praktischen Aufbau von Identitätsföderationen einsetzbar.

In den Abschnitten 3.2 und 3.3 wurde jedoch gezeigt, dass einige der in Kapitel 2 erarbeiteten *essentiellen* Anforderungen nur mit zum Teil größeren Einschränkungen, viele der *wichtigen* Anforderungen nicht und nur wenige der *empfehlenswerten* Anforderungen erfüllt werden. Abbildung 3.5 zeigt zusammenfassend die Bewertung der eingehend untersuchten FIM-Ansätze anhand einer Übersichtstabelle.

Somit bleiben **Defizite** insbesondere in den folgenden Bereichen bestehen:

1. Auf **Datenschutzaspekte** wird trotz der Bemühungen der Liberty Alliance noch nur unzureichend eingegangen, wodurch insbesondere die praktische Umsetzbarkeit und Akzeptanz von FIM leidet. Die Steuerung von Datenfreigaben durch den Benutzer in Form von Attribute Release Policies wurde zwar in Shibboleth umgesetzt, bleibt jedoch noch deutlich hinter ihren Möglichkeiten zurück. Die in Abschnitt 3.5 vorgestellten Lösungen zum Privacy Management können nicht direkt in FIM-Transaktionen angewendet werden, so dass erst entsprechende IDP- und SP-seitige Schnittstellen geschaffen werden müssen, die in den Abschnitten 5.3 und 5.4 konzipiert werden.

2. Die **Integration** von I&AM- und FIM-Komponenten bleibt sowohl IDP- als auch SP-seitig weitgehend offen:

   - IDP-seitig wird die Existenz eines Identity Repositories vorausgesetzt, aus dem die für FIM-Transaktionen benötigten Daten bezogen werden können, ohne dass die Auswirkungen z. B. auf die **Sicherheitsinfrastruktur** oder die **IT Service Supportprozesse** berücksichtigt werden.
   - SP-seitig wird von allen Ansätzen lediglich die Anbindung eines einzigen Dienstes betrachtet, wodurch **vorhandene I&AM-Systeme umgangen** und potentielle **Dienstabhängigkeiten ignoriert** werden. Die in Abschnitt 3.7 diskutierten Provisioningansätze sind in ihrer aktuellen Form noch nicht adäquat für FIM.

   In Kapitel 4 wird deshalb ein integrierendes Architekturkonzept erarbeitet, das die sowohl IDP- als auch SP-seitig vorhandene Infrastruktur und die dahinter stehenden Prozesse berücksichtigt; zur SP-seitigen Umsetzung wird eine von den aktuellen FIM-Ansätzen noch nicht bereitgestellte Werkzeugkomponente benötigt, die in Abschnitt 5.4 spezifiziert wird.

Abbildung 3.5.: Ergebnisse der Analyse auf Basis des Kriterienkatalogs

3. Mit der Notwendigkeit eines **einheitlichen Informationsmodells** bleibt ein grundlegendes Problem verteilter Systeme bestehen, da bei den Föderationsteilnehmern bereits vorhandene I&AM-Systeme in der Regel heterogen sind. In Abschnitt 3.8 wurden verschiedene Ansätze für das Ermitteln eines föderationsweiten Informationsmodells vorgestellt; eine flexible bidirektionale Konvertierung lokaler Datenbestände in föderationsspezifische Formate ist in den FIM-Ansätzen jedoch noch nicht vorgesehen, so dass in Abschnitt 5.2 eine entsprechende Komponente konzipiert wird, wobei insbesondere das effiziente föderationsweite Management der dezentralen Konvertierungsprozesse betont wird.

Bei den aufgeführten Problemen hat sich in den letzten Jahren gezeigt, dass sich dafür zwar durchaus ein Bewusstsein gebildet hat, aber noch keine signifikanten Fortschritte erzielt wurden, da von Softwareherstellern gewünschte Detailverbesserungen Vorrang vor einer funktionalen Weiterentwicklung haben. Auch die UCIM-Ansätze liefern zu diesen Schwierigkeiten keine Lösungen, obwohl sie zum Identity Management im Allgemeinen durchaus signifikante Beiträge leisten, beispielsweise hinsichtlich der Benutzbarkeit und SP-gesteuerten Schreibzugriffen auf die beim IDP hinterlegten Benutzerprofile.

Kapitel 4.

Konzept für eine integrierte I&AM- und FIM-Architektur

Inhalt dieses Kapitels

Auf Basis der in Kapitel 3 vorgestellten FIM-Ansätze und der Analyse ihrer Defizite wird im Folgenden ein Architekturkonzept vorgestellt, das insbesondere zu Verbesserungen in den Bereichen

- **Integration von I&AM und FIM** unter Berücksichtigung von **IT-Securityinfrastrukturen** und IT Service Management Prozessen, insbesondere Unterstützung des **Change Managements**,
- **Interoperabilität** im Hinblick auf föderationsweit **heterogene Datenmodelle** und
- **organisationsübergreifendes Privacy Management** aus Benutzer- und Administratorperspektive

führt und dessen Zielsetzung in Abschnitt 4.1 näher erläutert wird. In Abschnitt 4.2 wird ein sehr knapper Überblick über die Gesamtarchitektur gegeben, deren Bestandteile im Anschluss detaillierter erläutert werden.

Neben der systematischen Integration von I&AM- und FIM-Komponenten, die in den Abschnitten 4.3 und 4.4 strukturiert anhand ihrer Aufgaben und Schnittstellen dargestellt werden, um eine **„Black-Box"-Betrachtung** zu ermöglichen, wird eine Reihe im Rahmen dieser Arbeit **neu konzipierter FIM-Komponenten** eingesetzt, die hier motiviert und in Kapitel 5 detailliert spezifiziert werden („White-Box"-Betrachtung).

Die gegenseitigen **Abhängigkeiten** von I&AM- und FIM-Komponenten, mit denen sich die Spezifikationen der existierenden FIM-Ansätze wie in Kapitel 3 erläutert nicht ausreichend auseinandersetzen, sind Gegenstand der Diskussion in Abschnitt 4.5, die wiederum die Randbedingungen für die in Abschnitt 4.6 erläuterte **methodische Integration von FIM-Komponenten in bestehende I&AM-Infrastrukturen** vorgibt.

Neben den für Identity Management spezifischen Herausforderungen bei der Integration müssen zur Sicherstellung der praktischen Realisierbarkeit weitere Aspekte betrachtet werden: In Abschnitt 4.7 wird auf die Auswirkungen für bestehende IT-Securityinfrastrukturen eingegangen; die hierbei gewählte Integrationsperspektive ergänzt Literatur zur Sicherheit von FIM-Komponenten und -Protokollen um den wesentlichen Aspekt des Zugriffs auf lokale, ursprünglich in der Regel nicht für externe Zugriffe geschaffene Identity Repositories. Die Auswirkungen auf die organisationsinternen IT Service Support Prozesse werden in Anlehnung an die Klassifizierung nach ITIL in Abschnitt 4.8 am Beispiel des Change Managements diskutiert, das bereits einen essentiellen Schwerpunkt im I&AM-Umfeld darstellt.

Auf Basis der erläuterten Zusammenhänge lassen sich analog zu den aus dem zeitgemäßen Software Engineering bekannten *Design Patterns* so genannte **Architekturmuster** ableiten, die in Abschnitt 4.9 zu exemplarischen Lösungen für typische Szenarienbestandteile ausgearbeitet werden. Ihre Kombination zu **Referenzarchitekturen** für die FIM-spezifischen organisatorischen Rollen wie Identity Provider und Service Provider in Abschnitt 4.10 sowie eine **Bewertung der Gesamtarchitektur auf Basis des Kriterienkatalogs** in Abschnitt 4.11

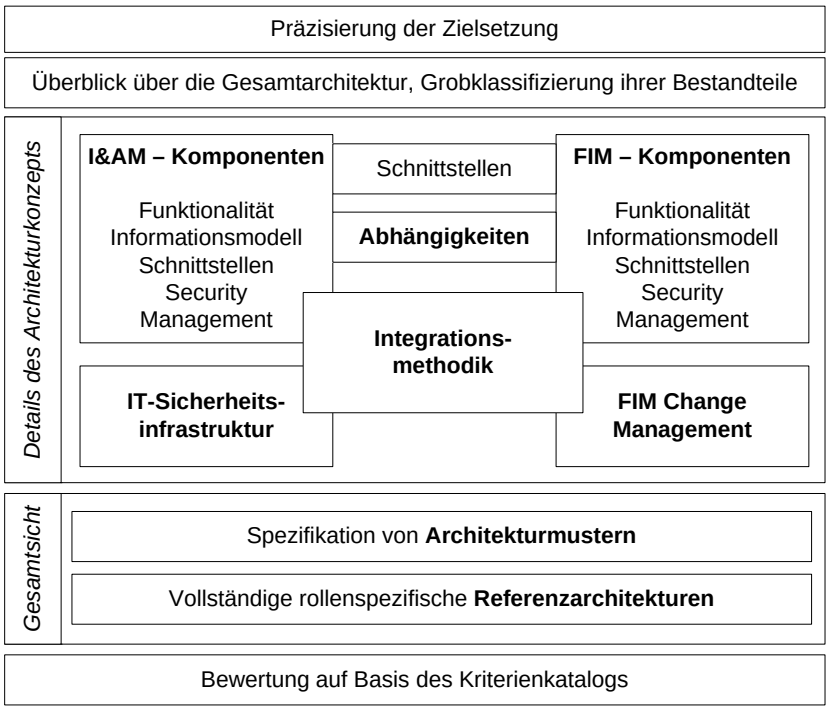


Abbildung 4.1.: Vorgehensmodell in diesem Kapitel

schließen das Kapitel ab. Das für dieses Kapitel angewendete Vorgehensmodell ist zusammenfassend in Abbildung 4.1 dargestellt.

4.1. Präzisierung der Zielsetzung des Architekturkonzepts

Zur Verdeutlichung der Ziele des in dieser Arbeit geschaffenen Architekturkonzepts wird in Abschnitt 4.1.1 zuerst die **Ausgangssituation aus einer szenarienunabhängigen Perspektive** mit dem Schwerpunkt auf der Integration von I&AM-Systemen und FIM-Komponenten konkretisiert. Diese Darstellung umfasst ausgewählte, in Kapitel 3 analysierte Problemstellungen vor dem Hintergrund eines praktischen Einsatzes der existierenden FIM-Ansätze auf Basis eines bereits bestehenden I&AM-Systems.

Als Kontrast dazu und als designiertes Fernziel wird in Abschnitt 4.1.2 der **hypothetische Idealzustand bei vollständiger Integration** von I&AM- und FIM-Komponenten skizziert; er zeichnet sich dadurch aus, dass alle in Kapitel 2 postulierten Anforderungen vollständig erfüllt werden; die bereits größtenteils erfüllten Anforderungen werden dabei nicht alle explizit erwähnt, um primär die noch ungelösten Fragestellungen zu betonen.

Zwangsweise kann diese Arbeit nur selektive Beiträge erbringen, die näher an dieses Ziel heranführen; in Abschnitt 4.1.3 werden die **Bereiche und der Umfang der eigenen Tätigkeiten** erläutert und gegen bewusst nicht vertiefend betrachtete Forschungsfelder abgegrenzt.

4.1.1. Ausgangssituation aus Integrationsperspektive

Dieser Abschnitt beschreibt diverse Schwierigkeiten bei der praktischen Einführung eines der in Kapitel 3 beschriebenen FIM-Ansätze ohne Bezug zu einem konkreten Szenario; er dient der zusammenfassenden Verdeutlichung bestehender Defizite bei der Integration von FIM-Komponenten in I&AM-Systeme.

4.1.1.1. Föderationsweite Betrachtung

Die Entscheidung für die FIM-basierte Unterstützung organisationsübergreifender Geschäftsprozesse ist mit der Auswahl eines konkreten Produktes verbunden, da die verschiedenen FIM-Protokolle und zum Teil die herstellerspezifischen Implementierungen desselben FIM-Ansatzes untereinander nicht ausreichend kompatibel sind (siehe Abschnitt 3.4.1). Für die Teilnahme an verschiedenen Föderationen kann somit der Einsatz unterschiedlicher FIM-Software notwendig werden.

Eine Föderation ist durch die zwischen ihren teilnehmenden Organisationen instanziierten Vertrauensbeziehungen charakterisiert (vgl. Abschnitt 2.1.2.5); die bestehenden FIM-Ansätze gehen jedoch von homogenen Vertrauensverhältnissen aus, d. h. jeder Föderationsteilnehmer vertraut jedem anderen uneingeschränkt. Eine Differenzierung, beispielsweise hinsichtlich der garantierten Servicequalität je nach der von einem Identity Provider gelieferten Datenkategorien ist in den FIM-Ansätzen nicht vorgesehen und kann in den existierenden Implementierungen höchstens statisch eingeschränkt werden, so dass die von Trust & Reputation Management ermöglichte Dynamik nicht genutzt werden kann.

Für die Verwaltung von Föderationen werden einfache Werkzeuge bereitgestellt, die wichtige Aspekte wie die sichere und zuverlässige Übermittlung von Metadaten an die Verwaltungsinstanz nicht abdecken. Im Allgemeinen wird die Existenz einer gemeinsamen Public-Key-Infrastruktur (PKI) vorausgesetzt, die beispielsweise bei Kooperationen von Hochschulen mit Industriepartnern erst geschaffen und parallel zu existierenden PKIs betrieben werden muss; alternativ müssen alle sicherheitsrelevanten Metadaten wie Serverzertifikate in einem aufwendigen Prozess in die Föderationsmetadaten integriert werden. Änderungen an den Metadaten eines Föderationsteilnehmers müssen ebenfalls manuell eingearbeitet werden.

Die erfolgreiche Abwicklung von FIM-Transaktionen setzt ein föderationsweit gemeinsames Datenmodell voraus, das neben der Konzeption eines entsprechenden Namensraums, beispielsweise für Benutzer- und Dienstidentifikatoren, insbesondere die syntaktische und semantische Spezifikation von auszutauschenden Benutzerattributen umfasst. Die fehlende Vorgabe einer Methodik zur Erarbeitung eines gemeinsamen Datenschemas führt zur Verwendung multilateral anerkannter Vorarbeiten (siehe Abschnitt 3.8) als größten gemeinsamen Nenner oder zum aufwendigen Entwurf eines neuen Datenmodells, der häufig durch wenige, aufgrund ihrer politischen Stellung ausgezeichneten Föderationsteilnehmer dominiert wird und somit nicht alle Interessen ausgewogen berücksichtigt.

Darüber hinaus sind die Möglichkeiten zur zentralen Verwaltung von Föderationen stark eingeschränkt; beispielsweise können Vorgaben, welche Daten übertragen werden dürfen bzw. müssen, nur dezentral umgesetzt werden. Die Einhaltung derartiger Randbedingungen müssen wie die übrigen im Rahmen von SLAs vereinbarten Dienstgüteparameter unabhängig vom FIM-Ansatz dezentral überwacht werden.

4.1.1.2. IDP-spezifische Betrachtung

Die Integration der FIM-Komponenten beim IDP führt zu zwei unmittelbaren technischen Problemen: Die der Föderation zur Verfügung zu stellenden Daten liegen im Allgemeinen nicht im föderationsspezifischen Datenformat vor und sind im Identity Repository eines I&AM-Systems hinterlegt, das bewusst nicht für externe Zugriffe konzipiert worden ist.

Organisationen, die in der Rolle eines IDPs fungieren sollen, haben deshalb in Anbetracht fehlender Integrationskonzepte lediglich die Möglichkeit, die entsprechenden Datenbestände in ein neues Identity Repository, das den datenschemaspezifischen Anforderungen der Föderation entspricht, zu replizieren; dieser Vorgang, der neben dem Initialaufwand auch mit den Kosten für den laufenden Betrieb verbunden ist, muss für die Teilnahme an weiteren Föderationen wiederholt werden. Die so geschaffenen weiteren Identity Repositories müssen darüber hinaus in die übrigen Geschäftsprozesse wie das Security Management und das Change Management integriert werden. Die daran Beteiligten müssen sich aufgrund des Mangels an zielgerichteter Dokumentation intensiv mit dem jeweils gewählten FIM-Ansatz auseinandersetzen.

Das Management der Identitäten, deren Daten über FIM bereitgestellt werden, beispielsweise deren Ergänzung um föderationsspezifische Attribute, muss IDP-seitig mit herkömmlichen Werkzeugen durchgeführt werden; eine Kontrolle, welche Daten über welche Benutzer bereits von außen abgerufen worden sind, kann maximal über die Auswertung von Protokolldateien der FIM-Komponenten erfolgen, so dass diese Information auch nicht ohne weiteres den betroffenen Benutzern im Sinne der informationellen Selbstbestimmung zur Verfügung gestellt werden kann.

Die Möglichkeiten zur Beschränkung abrufbarer Daten sind stark begrenzt: Die nur selektive Speisung föderationsspezifischer Identity Repositories in der Granularität einzelner Benutzer ist bei größerer Benutzeranzahl aufgrund des damit verbundenen manuellen Aufwands nicht bewältigbar. Der Einsatz von Attribute Release Policies ist in den FIM-Standards noch nicht vorgesehen und bei Implementierungen wie Shibboleth mit den Nachteilen verbunden, dass administrativ vorgegebene Policies nicht dezentral oder hierarchisch gepflegt werden können und insbesondere für Benutzer keine geeigneten Frontends zur Pflege der eigenen Policies zur Verfügung stehen; ferner sind Policysprachelemente wie flexible Bedingungen und Obligationen nicht verfügbar.

Aus Benutzerperspektive ist darüber hinaus der Einsatz von Attributszertifikaten sowie die Unterstützung unterschiedlicher Rollen, auch im Hinblick auf mögliche Antwortvarianten auf Anfragen von SPs, ungeklärt. Bei auftretenden technischen Problemen bleibt offen, ob sich der Benutzer an den Service Desk des jeweiligen SPs oder seines IDPs werden soll.

4.1.1.3. SP-spezifische Betrachtung

Analog zur Situation bei IDPs stellt sich für SPs das Problem, dass die Benutzerdaten im föderationsspezifischen Format geliefert werden. Schwerwiegender ist jedoch, dass alle FIM-Ansätze vorsehen, dass die Dienste direkt über FIM gespeist werden; dies setzt einerseits FIM-fähige Dienste voraus und bedeutet andererseits ein Umgehen des SP-seitig lokal vorhandenen I&AM-Systems und entsprechender Sicherheitskomponenten, die bislang exklusiv für die Kanalisierung von Autorisierungsinformationen über berechtigte Benutzer zuständig waren.

Dadurch können Dienstabhängigkeiten und Korrelationsmechanismen für Benutzerdatensätze nur genutzt werden, wenn sie in jedem Dienst explizit implementiert sind. Da auf Benutzerdaten beim IDP nur zugegriffen werden kann, während der Benutzer online ist und den Dienst nutzt, und derzeit vorherrschend noch kein Schreibzugriff auf die beim IDP gespeicherten Daten möglich ist, müssen SP-seitig lokale Benutzerdatenbestände vorgehalten werden. Deren Konsistenz ist bei der Verwendung in asynchron instanziierten Prozessen wie dem Rechnungswesen jedoch nur gewährleistet, wenn der verwendete FIM-Ansatz entsprechende Updatemechanismen zur Verfügung stellt; dies trifft derzeit nur auf die Liberty Alliance mit den in Abschnitt 3.2.2 genannten Einschränkungen zu.

Während die FIM-basierte Nutzung von Diensten für Bestandskunden auf Basis der Verknüpfung von Benutzerprofilen bei IDP und SP ([FA-AccountLinking]) bereits weitgehend unterstützt wird, ergibt sich für neue Benutzer die Schwierigkeit, den Nutzungsbedingungen, beispielsweise den allgemeinen Geschäftsbedingungen des SPs, a priori in geeigneter Form zustimmen zu müssen; über FIM nutzbare Dienste müssen ggf. erst um diesen Aspekt erweitert werden.

Aufgrund der direkten Einspeisung der mittels FIM übertragenen Daten in die jeweiligen Dienste muss für das Management des FIM-spezifischen bzw. des ganzen Benutzerdatenbestands auf die in den jeweiligen Dienst integrierten Werkzeuge zurückgegriffen werden; eine Weiterverwendung dieser Daten im Rahmen anderer Prozesse ist nicht ohne Weiteres möglich.

4.1.2. Idealzustand bei vollständig realisierter Integration

Nachfolgend wird der Idealzustand gezeigt, der durch eine vollständige Verschmelzung von I&AM-Systemen mit FIM-Komponenten erreicht werden kann. Dieser Zustand ist beim heutigen Stand der Technik unrealistisch und wird auch durch die in dieser Arbeit geschaffenen Ergänzungen und Verbesserungen nicht vollständig erreicht; seine Beschreibung dient deshalb einerseits zur Formulierung von Randbedingungen an eigene Entwicklungen, d. h. er zeigt Ziele auf, die nicht blockiert werden dürfen, und andererseits zur Motivation weiterer Arbeiten, die auf dieser aufbauen.

4.1.2.1. Föderationsweite Betrachtung

Im Idealfall reflektiert die initiale Bildung einer Föderation lediglich eine lose Kopplung von Organisationen auf Basis gemeinsamer Kriterien frei wählbarer Granularität (z. B. alle deutschen Hochschulen), die eine FIM-basierte Kommunikation prinzipiell ermöglicht. Eine Föderation wird somit nicht für genau einen Zweck geschaffen, sondern legt den Grundstein für eine enge Zusammenarbeit beliebiger Teilmengen der Föderationsteilnehmer auf Basis dedizierter Service Level Agreements, die auf dienstespezifische technische Konfigurationen entsprechender Vertrauensbeziehungen abgebildet werden. Für die Aus- und Bewertung der realen Dienstgüte im Betrieb können insbesondere Methoden des Trust & Reputation Managements angewendet werden, die eine angemessene Dynamik bei niedrigem manuellem Aufwand ermöglichen.

Die Föderationsverwaltung beschränkt sich beispielsweise bei der Aufnahme neuer Föderationsteilnehmer auf die Eintragung der URLs der neuen FIM-Komponenten; die notwendigen Metadaten werden automatisch ausgetauscht und in die Föderationsmetadaten integriert,

wobei ein manueller Eingriff nur notwendig ist, wenn ein neuer Teilnehmer an einer den technischen Systemen noch nicht bekannten, aber von der Föderation akzeptierten PKI beteiligt ist.

Optional können föderationsweit gültige Policies spezifiziert werden, die beispielsweise die grundlegenden Datenfreigaben und Protokollierungsregeln festlegen und somit ein föderationsweites Datenschutz- und Sicherheitskonzept ermöglichen, dessen Einhaltung zentral unterstützt und sichergestellt werden kann.

Die Einigung auf das zu verwendende föderationsweite Datenmodell bleibt eine manuell durchzuführend Aufgabe, die jedoch durch Werkzeuge, beispielsweise auf der Basis von Schemakoordinationstechniken (vgl. Abschnitt 3.8) weitgehend unterstützt wird.

4.1.2.2. IDP-spezifische Betrachtung

Die IDP-seitige Integration der FIM-Komponenten wird durch eine Möglichkeit zur transparenten Konversion zwischen dem föderationsweit und dem lokal eingesetzten Datenschema erleichtert. Alle bereits vorhandenen Komponenten können deshalb mit dem bisherigen Datenmodell weiterverwendet werden; die Einführung zusätzlicher Identity Repositories ist nicht notwendig.

Die Zugriffe auf den lokalen Datenbestand werden über eine weitere Komponente kanalisiert und kontrolliert, um föderationsweite und IDP-spezifische Policies umzusetzen. Alle FIM-Komponenten bieten geeignete Schnittstellen, beispielsweise zur Integration in bestehende IT-Sicherheitsinfrastrukturen.

Benutzer werden bei der Verwaltung ihrer Daten und Datenfreigaben umfassend unterstützt: Neben einer intuitiv und effizient nutzbaren Möglichkeit zur Spezifikation flexibler Attribute Release Policies, die bei Bedarf um interaktive Nachfragen während der Dienstnutzung ergänzt werden, werden die Benutzer vom IDP auf verschiedene Varianten zur Beantwortung von Anfragen durch SPs hingewiesen und können die über sie abgerufenen Daten jederzeit zentral einsehen. Neben vom IDP vorgegebenen und im Rahmen von Self Service pflegbaren Attributen werden der Import und Export von Attributszertifikaten sowie die selektive Delegation von Berechtigungen an andere Benutzer, beispielsweise für Vertretungsfälle, unterstützt. Die Zuständigkeiten bei auftretenden Problemen sind klar geregelt.

4.1.2.3. SP-spezifische Betrachtung

Über FIM gelieferte Daten werden wie beim IDP in das lokal verwendete Format konvertiert und in das I&AM-System des SP eingespeist; vorhandene Werkzeuge zur Berücksichtigung von Dienstabhängigkeiten und zur Korrelation von Benutzerdatensätzen können somit unverändert weiterverwendet werden. Das Einspeisen der Daten wird von einer FIM-Komponente überwacht, die neben einer Schnittstelle zur lokalen Sicherheitsinfrastruktur die Möglichkeit zur Umsetzung föderationsweiter und SP-spezifischer Richtlinien erlaubt. Die Daten werden durch IDP-seitige Updatemechanismen in einem Pushverfahren automatisch konsistent gehalten und können mit den bestehenden Managementwerkzeugen in anderen Prozessen auch verwendet werden, wenn der Benutzer den Dienst gerade nicht nutzt.

Über einen Schreibzugriff auf das beim IDP gespeicherte Benutzerprofil können diesem Informationen über die Dienstnutzung durch seine Benutzer übermittelt werden, die diese optional

zentral einsehen können. Der Schreibzugriff, der analog zu den Datenfreigaben IDP- und benutzerseitig eingeschränkt werden kann oder bei Bedarf zu Interaktionen führt, dient darüber hinaus optional als Ersatz der lokalen Speicherung von benutzerspezifischen Daten beim SP, sofern dieser kein lokales I&AM-System verwendet, da er beispielsweise nur einen einzigen, nur wenig komplexen Dienst anbietet.

Bevor die zur Nutzung eines Dienstes benötigten Identitätsdaten übertragen werden, muss der Benutzer den entsprechenden Nutzungsrichtlinien zustimmen; sofern der Dienst anonym oder pseudonym verwendet werden kann, wird dem SP ein entsprechend randomisiert erzeugter Identifikator mitgeteilt, über den kein Rückschluss auf die reale Person möglich ist.

4.1.3. Vorgehensweise und Umfang

Die im Rahmen dieser Arbeit konzipierten eigenen Beiträge werden wie folgt motiviert:

1. **I&AM-Systeme werden als gegeben vorausgesetzt** und gelten als bereits hinreichend ausgereift, so dass keine fundamentalen Eingriffe erforderlich sind bzw. notwendig gemacht werden sollten. Die zugrundeliegenden Konzepte und existierenden konkreten Implementierungen werden durch hinreichende Literatur und Dokumentation gestützt, obwohl sich der überwiegende Teil wissenschaftlicher Veröffentlichungen im Hinblick auf Identity Management stark auf UCIM und nur am Rand auf I&AM bezieht (vgl. z. B. [Ric05]). Insbesondere fehlt eine für das hier vorgestellte Konzept notwendige gesamtheitliche architekturelle Betrachtung von I&AM-Systemen, so dass diese in Abschnitt 4.3 aufgegriffen wird, um I&AM-Komponenten hinsichtlich ihrer Funktionalität und Schnittstellen, u. a. zu IT-Sicherheitskomponenten, darzustellen.

2. FIM-Systeme sind noch im Entstehen und nicht ausreichend untersucht worden; insbesondere reicht der Umfang bereits spezifizierter FIM-Komponenten nicht aus, um alle gestellten Anforderungen zu erfüllen, wodurch die Erweiterung bestehender Komponenten und die **Einführung neuer Architekturelemente** notwendig werden. Die Modularität aller bekannten FIM-Ansätze erlaubt dabei eine nahtlose Integration neuer Komponenten, ohne die Kompatibilität mit den Standards zwingend zu gefährden.

Das vorliegende Architekturkonzept orientiert sich aus den folgenden Gründen primär an SAML und Shibboleth:

- Die Spezifikationen der Liberty Alliance basieren auf SAML, wodurch die grundlegende Übertragbarkeit eigener SAML-basierter Konzepte sichergestellt ist. Die Erweiterungen der Liberty Alliance lassen sich grob in zwei Kategorien einteilen: Zum einen werden beispielsweise mit den *ID-WSF Subscriptions and Notifications* Funktionalitäten vorgestellt, die analog zu einigen aus dem UCIM-Umfeld stammenden Konzepten berücksichtigt werden müssen; zum anderen spielen die insbesondere in den *Liberty Identity Service Interface Specifications (ID-SIS)* standardisierten Applikationen im Rahmen dieser Arbeit nur eine untergeordnete Rolle, da es sich um Anwendungen von FIM, aber nicht um FIM-Konzepte per se handelt.

- Durch die Verwendung von SAML Assertions in Secure Tokens ist ebenfalls eine grundlegende Interoperabilität mit WS-Federation möglich. Die hier vorgestellten Konzepte lassen sich vollständig auf WS-Federation übertragen; auf eine redundante Darstellung in der Terminologie von WS-Federation wird jedoch verzichtet.

- Shibboleth basiert einerseits auf SAML, implementiert andererseits jedoch Konzepte der Liberty Alliance, beispielsweise im Hinblick auf Benutzerinteraktionen und ARPs. Die Open Source Software eignet sich deshalb zur konkreten Demonstration bestehender Defizite und ermöglicht Erweiterungen, die insbesondere in Kapitel 6 als Tragfähigkeitsnachweise der in Kapitel 5 konzipierten FIM-Werkzeuge dienen.

Die in diesem Kapitel gewählte Vorgehensweise reflektiert das Ziel, FIM-Komponenten nahtlos in bestehende I&AM-Systeme zu integrieren:

- In einer grundlegenden Analyse werden die prinzipiell verfügbaren I&AM- und FIM-Komponenten auf Basis ihrer **Schnittstellen** in ihr jeweils engeres Umfeld, beispielsweise hinsichtlich Security- und Managementinfrastruktur, eingeordnet. Diese Betrachtung ist notwendig, um das Ziel der Integration bestehender Komponenten nicht zu verfehlen, und bildet die Grundlage für die vertiefenden Untersuchungen in den nachfolgenden Schritten.

- Auf Basis einer **Top-down**-Vorgehensweise werden die zur Umsetzung der FIM-Funktionalität notwendigen Komponenten miteinander kombiniert und methodisch in die gegebene I&AM-Infrastruktur integriert. Diese Integration reflektiert im Wesentlichen die Schnittmenge der beiden vorangegangenen Betrachtungen und stellt ein wichtiges Teilergebnis der Gesamtarchitektur dar.

- Die kombinierte I&AM- und FIM-Architektur wird hinsichtlich ihrer technischen Einbettung in das IT Service Management untersucht; die Schwerpunkte liegen dabei auf der **IM-spezifischen Betrachtung des IT-Security Managements und des Change Managements**, deren Komplexität aufgrund der organisationsübergreifenden Prozesse deutlich zunimmt. Diverse organisatorische und juristische Aspekte werden lediglich angedeutet, da eine adäquate vollständige Analyse der damit verbundenen komplexen Fragestellungen den Rahmen dieser Arbeit sprengen würde.

Der Umfang des vorgelegten Architekturkonzepts orientiert sich an der Realisierung der folgenden Teilziele:

- **Integration** der bekannten I&AM- und FIM-Komponenten vor dem Hintergrund der Bereitstellung generischer FIM-Funktionalität; für das Konzept wird eine **Anwendungsmethodik** spezifiziert, die in Kapitel 7 exemplarisch auf eines der in Kapitel 2 vorgestellten Szenarien angewandt wird.

- Erläuterung der Einzelschritte im Hinblick auf die in Kapitel 2 gestellten Anforderungen und die sich daraus ergebenden Verbesserungen gegenüber den in Kapitel 3 analysierten Defiziten.

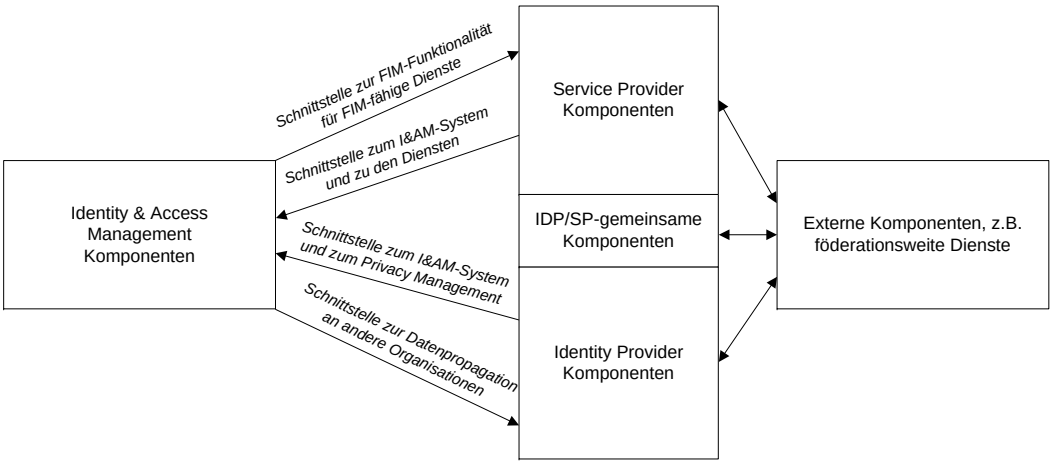


Abbildung 4.2.: Prinzipielles Zusammenspiel der Komponentenblöcke

- **Spezifikation der Schnittstellen** zwischen den Komponenten; diese werden zum Teil über neu eingeführte Komponenten realisiert, deren Details in Kapitel 5 spezifiziert werden.
- Verbesserung des **Privacy Managements** beim organisationsübergreifenden Datenaustausch unter Berücksichtigung von organisationsinternen Privacy Management Systemen.
- Verdeutlichung der **Zusammenhänge mit Netz- und Systemsicherheitskomponenten**, ohne deren Berücksichtigung eine praktische Realisierung nicht möglich ist, da angemessene Maßnahmen zur Datensicherheit im Rahmen des Datenschutzes zwingend erforderlich sind und ihr Fehlen ein inakzeptables Risiko darstellen würde.
- Diskussion der Auswirkungen auf den laufenden Betrieb, insbesondere bezüglich des Change Managements, um die **Nachhaltigkeit** der gefundenen Lösung sicherzustellen.
- Sicherstellung von **Anwendbarkeit und Wiederverwendbarkeit** beim Aufbau neuer Identity Management Systeme durch Spezifikation von Architekturmustern und Referenzarchitekturen.

Abbildung 4.2 zeigt das prinzipielle Zusammenspiel der vier Komponentenblöcke, die im Rahmen dieses Konzepts vertieft werden: Ein Identity & Access Management System wird als Grundlage angesehen, wobei durchaus auf die speziell für FIM relevanten Aspekte und benötigten Komponenten eingegangen wird. Die organisatorischen FIM-Rollen des Services Providers und des Identity Providers unterscheiden sich auch in der technischen Realisierung sehr deutlich voneinander, so dass nur wenige der FIM-Komponenten sowohl bei IDP als auch bei SP eingesetzt werden. In beiden Fällen sind die Schnittstellen von den FIM-Komponenten zum I&AM-System in ihrer bidirektionalen Ausprägung zu untersuchen. Darüber hinaus spielen externe Komponenten eine nicht unwesentliche Rolle; hierzu gehören einerseits föderationsweite

Dienste, andererseits sind Benutzer und deren Clientsoftware maßgeblich an der Bearbeitung vieler FIM-Transaktionen beteiligt.

Die folgenden Aspekte gehören bewusst nicht zum Umfang dieses Konzepts:

- Erläuterungen zum Design und zur Konfiguration einzelner Komponenten vor dem Hintergrund der intuitiven und effizienten Benutzbarkeit aus Benutzerperspektive, beispielsweise zur Gestaltung graphischer Oberflächen für Self Services und ARP-Management. Diese sind zwar eine zwingende Voraussetzung für den umfassenden praktischen Einsatz, jedoch Gegenstand anderer einschlägiger Arbeiten. Komponenten, die eine entsprechende Interaktion mit den Benutzern ermöglichen, werden deshalb nur auf ihre prinzipielle Funktionalität reduziert dargestellt.
- Kriterien zur Entscheidung über die Eignung konkreter Softwareprodukte für den praktischen Einsatz; wie bereits in Kapitel 2 erläutert wurde, kann hierzu der Anforderungskatalog herangezogen und ergänzt werden. Unter der Voraussetzung der Erfüllung der genannten Anforderungen kann das hier vorgestellte Architekturkonzept angewandt werden.
- Auf die explizite Untersuchung anonym oder pseudonym nutzbarer Dienste wird verzichtet; neben den in Kapitel 2 genannten speziellen Anforderungen stellen sie nur einen Teil der übrigen Anforderungen, so dass eine entsprechende Teilmenge des Architekturkonzepts angewendet werden kann.
- Im Rahmen des Konzepts werden keine konkreten Dienste betrachtet; stattdessen soll eine prinzipielle Eignung für alle Dienste, die an I&AM-Systeme gekoppelt werden können, sichergestellt werden. Dies bedeutet, dass sich aus konkreten Szenarien ergebende Randbedingungen bei der Instanziierung der vorgestellten Architektur berücksichtigt werden können und müssen.
- Die physische Positionierung von Komponenten, beispielsweise vor dem Hintergrund der Einbruchssicherheit oder unter Brand- und Katastrophenschutzaspekten, wird nicht betrachtet; diesbezüglich können jedoch andere Konzepte umgesetzt werden, die nicht FIM-spezifisch sind.
- Die zum Einsatz kommenden, nicht sicherheitsspezifischen Netzwerkkomponenten und deren Hochverfügbarkeit werden nicht betrachtet, sondern als gegeben vorausgesetzt.

Die Zielsetzung für die neu entworfenen FIM-Komponenten und deren Umfang werden in Kapitel 5 erläutert.

4.2. Überblick über die resultierende Gesamtarchitektur

Abbildung 4.3 gibt einen Überblick über die in dieser Arbeit konzipierte Gesamtarchitektur für integriertes I&AM und FIM; die einzelnen Komponenten sind über Pfeile miteinander verbunden, die Kommunikationsbeziehungen in der Richtung des Verbindungsaufbaus repräsentieren.

Die gezeigten Komponenten lassen sich wie folgt grob in vier Kategorien einteilen:

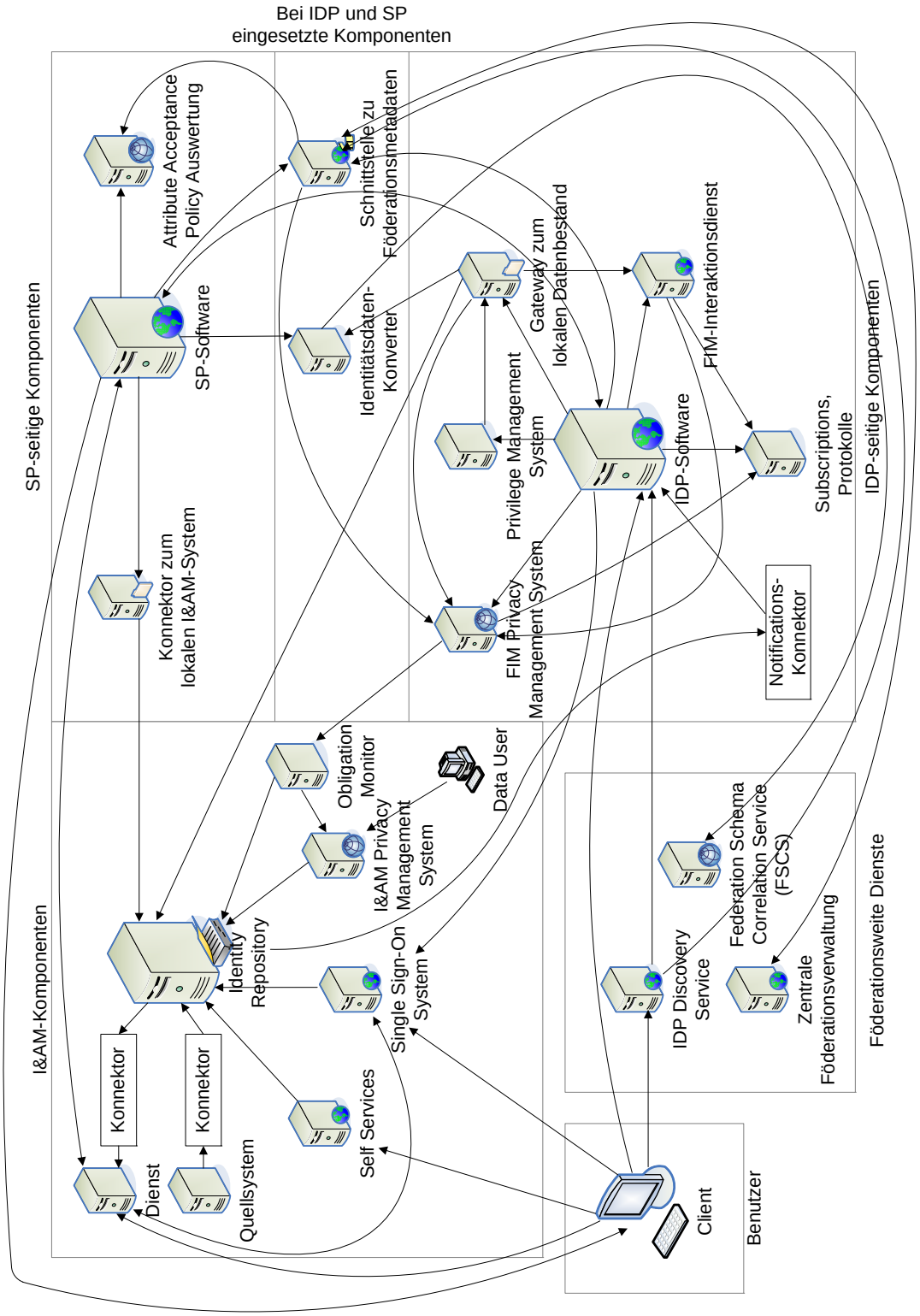


Abbildung 4.3.: Überblick über die Gesamtarchitektur

1. Links oben werden die zum organisationsinternen **I&AM-System** gehörenden Komponenten gezeigt. Sie umfassen neben einem Identity Repository, das über Konnektoren mit Quell- und Zielsystemen verbunden ist, insbesondere webbasierte Self Services für die Benutzer, ein organisationsinternes Single Sign-On System und ein I&AM Privacy Management System, dessen so genannter Obligation Monitor auch im Rahmen von FIM verwendet wird.

2. Rechts oben sind die FIM-Komponenten für den Einsatz bei **Service Providern** dargestellt; die Koordination aller FIM-Transaktionen wird dabei von der so genannten SP-Software übernommen, die von einem Konnektor zum lokalen I&AM-System und dem Identitätsdatenkonverter unterstützt wird, um über FIM akquirierte Datensätze im richtigen Format ins lokale Identity Repository einzupflegen. Zur Sicherstellung der Datenqualität werden Attribute Acceptance Policies eingesetzt, die optional auch föderationsweit vorgegeben werden können. Sowohl der Identitätsdatenkonverter als auch die Schnittstelle zu den Föderationsmetadaten greifen auf externe Dienste zurück, die den lokalen Administrationsaufwand minimieren.

3. Rechts unten sind die für **Identity Provider** relevanten FIM-Komponenten eingezeichnet. Die IDP-Seite stellt den Komplexitätsschwerpunkt dar; dies ist jedoch primär auf die Anzahl der verschiedenen Aufgaben und Komponenten zurückzuführen – die Häufung eingezeichneter Kommunikationsbeziehungen ist eine Konsequenz aus der IDP-seitig verstärkt notwendigen Interaktion mit dem Benutzer, auf die in Abschnitt 4.4 näher eingegangen wird.

   Prinzipiell werden alle FIM-Transaktionen IDP-seitig über die so genannte IDP-Software abgewickelt; analog zur SP-Software nutzt sie einen Gateway zum lokalen Datenbestand für den Zugriff auf das Identity Repository. Für die Unterstützung des Datentyps „Autorisierungsbestätigung“ wird ein Privilege Management System integriert. Ein FIM Privacy Management System übernimmt die Auswertung der Attribute Release Policies und bildet die Schnittstelle zum organisationsinternen Privacy Management System. Auf Basis eines Notifications-Konnektors und einer Subscriptions-Datenbasis können Änderungen an den Daten zeitnah an Service Provider propagiert werden. Analog zu diesen werden der Identitätsdatenkonverter und die Schnittstelle zu den Föderationsmetadaten genutzt.

   Echte Teilmengen dieser IDP-Komponenten sind auch bei Attribute Authorities und Authorization Providern vorhanden; für diese beiden Rollen werden separate Referenzarchitekturen vorgestellt.

4. Links unten sind **externe Komponenten** dargestellt. Neben den Benutzerclients gehören hierzu auch die föderationsweiten Dienste wie die zentrale Föderationsverwaltung und ein IDP Discovery Service, der den für einen Benutzer zuständigen IDP ermittelt.

Bei der Abbildung ist das ihr zugrundeliegende hohe Abstraktionsniveau zu berücksichtigen: Beispielsweise wurde auf die Darstellung der eingesetzten Securitykomponenten sowie der Repositories und Managementinfrastruktur für die policybasierten Komponenten verzichtet; diese Aspekte werden bei der detaillierteren Beschreibung jeder der verwendeten Komponenten in den nachfolgenden Abschnitten berücksichtigt. Um ihren zielgerichteten Einsatz in

der Gesamtarchitektur zu verdeutlichen, werden anschließend aufgabenspezifische Architekturmuster und Referenzarchitekturen spezifiziert, die zu dieser Gesamtarchitektur kombiniert werden können. Abbildung 4.4 zeigt die Komponenten in derselben relativen Positionierung, wobei jeweils eingezeichnet ist, ob es sich um eine neue, modifizierte, konfigurationsseitig angepasste oder unverändert übernommene Komponente handelt.

4.3. I&AM-Komponenten

Die nahtlose Integration aller I&AM- und FIM-Komponenten setzt ein Verständnis ihrer Aufgaben, Funktionsweise und Schnittstellen voraus. In diesem und dem folgenden Abschnitt werden die für das Architekturkonzept relevanten Komponenten deshalb näher analysiert, wobei die sich ergebenden und zu berücksichtigenden Abhängigkeiten in Abschnitt 4.5 vertieft werden.

In den folgenden Unterabschnitten werden die I&AM-Komponenten hinsichtlich ihrer **Ziele**, **Funktionalität**, **Datenmodelle** und **Kommunikationsschnittstellen** beschrieben. Ebenso werden die Kombination mit **IT-Sicherheitsmechanismen** sowie die Maßnahmen und Methoden für die **Hochverfügbarkeit** und das **Management** der Komponenten beschrieben, um einen umfassenden Blick auf jede Komponente zu ermöglichen, für den in dieser Gesamtheit noch keine Vorarbeiten existieren. Im Hinblick auf das FIM-spezifische Zusammenspiel der Komponenten werden dabei auch die im Rahmen dieses Architekturkonzepts getroffenen **Designentscheidungen** begründet.

Durch diese systematische Strukturierung soll verdeutlicht werden, dass beispielsweise die Berücksichtigung von Sicherheitsmaßnahmen eine wichtige Teilaufgabe bei der Inbetriebnahme jeder einzelnen Komponente ist, die bei der Konzeption einer szenarienspezifischen Architekturinstanziierung a priori und nicht erst nachträglich zu berücksichtigen ist; diese Darstellungsform darf jedoch nicht darüber hinweg täuschen, dass für den Betrieb der resultierenden IM-Gesamtarchitektur dennoch integrierte Sicherheits- und Managementarchitekturen und keine Insellösungen benötigt werden.

Anmerkungen zu den nachfolgenden Graphiken:

- Semantik der Pfeile:
  - Die Pfeilspitzen weisen in Richtung des Verbindungsaufbaus.
  - Die Pfeile sind in der Regel mit dem Namen des eingesetzten Kommunikationsprotokolls beschriftet. Dabei werden die folgenden Abkürzungen eingesetzt:
    - **WS**: Web-Service-basierte Kommunikation, z. B. Protokoll SOAP
    - **R**: Interaktive Weiterleitung des Benutzers per Redirect über das Protokoll HTTPS
- Semantik der Firewallsymbole:
  - Ein großes Firewallsymbol, durch das mindestens ein Pfeil hindurchgeht, stellt einen explizit vorgesehenen Firewall dar, dessen Einsatz empfohlen wird.

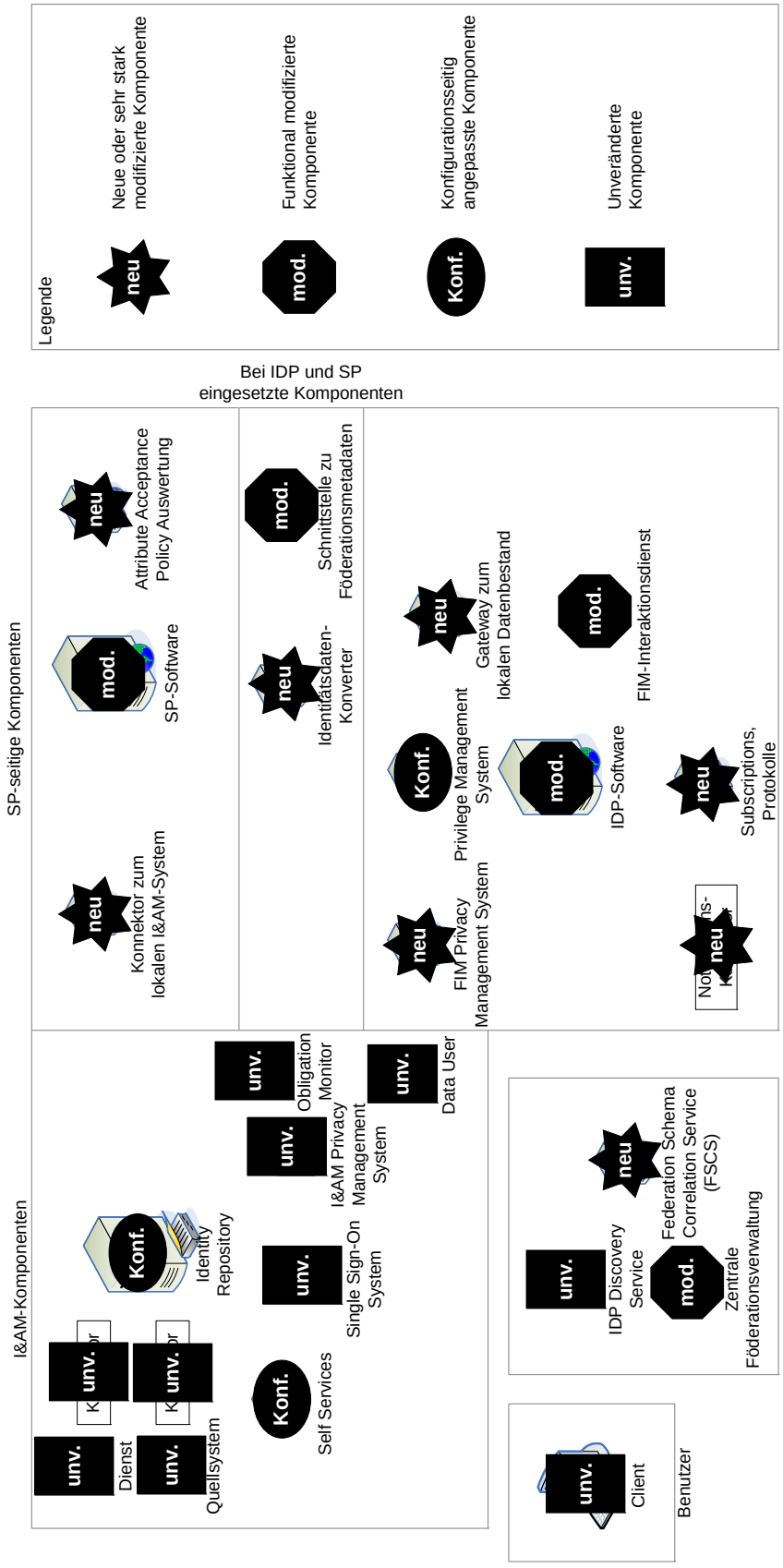


Abbildung 4.4.: Überblick über neue und modifizierte Komponenten

- Ein kleines Firewallsymbol, das zwar neben einem oder mehreren Pfeilen platziert, aber einer oder mehreren Verbindungen klar erkennbar zugeordnet ist, stellt einen optionalen Firewall dar, der einen zusätzlichen organisationsinternen Schutz bringen kann, im Normalfall aber nicht zwingend erforderlich ist; in der Praxis sind diese Firewalls bereits häufig in Form von Routern mit Paketfilterfähigkeiten an Netzwerkübergängen vorhanden und sollten entsprechend konfiguriert werden.
- Zur Verbesserung der Übersichtlichkeit werden Firewalls nur den jeweiligen Kernkomponenten einer Graphik zugeordnet und in der Peripherie vernachlässigt; dies bedeutet, dass Komponenten, die an anderer Stelle ausführlicher beschrieben werden, in der Regel ohne ihre Firewallarchitektur eingezeichnet werden.

Auf weitere Besonderheiten wird ggf. in den jeweiligen Komponentenbeschreibungen hingewiesen.

4.3.1. Identity Repositories

Identity Repositories sind der Kern eines I&AM-Systems. Bezüglich des Einsatzes von FIM dienen sie primär der Speicherung von Identitätsdaten; wie in Szenario 3 gezeigt wurde, werden beim organisationsinternen Einsatz darüber hinaus Informationen über Kunden, Verträge sowie Berechtigungen zur Nutzung der organisationsinternen Systeme und von einzelnen Diensten benötigte Profildaten abgelegt.

In *einem* I&AM-System können mehrere Identity Repositories eingesetzt werden, wenn dieselben Daten oder Teilmengen davon in unterschiedlichen Formaten vorgehalten werden sollen; mehrere Identity Repositories mit disjunkten oder sich nur partiell überlappenden Datensätzen deuten hingegen auf eine noch nicht abgeschlossene organisationsinterne Integration hin und werden nur insofern berücksichtigt, als dass andere Komponenten ggf. auf mehr als ein Identity Repository zugreifen können müssen. Zur Realisierung von Identity Repositories werden überwiegend Directory Services in Form von LDAP-Servern eingesetzt; nachfolgend wird auch der Einsatz relationaler Datenbankmanagementsysteme berücksichtigt, deren Verbreitungsgrad für diesen Einsatzzweck jedoch immer weiter abnimmt.

4.3.1.1. Funktionalität

Als Datenbasis stellen Identity Repositories Funktionen zum Anlegen, Modifizieren, Löschen und Auslesen von Datensätzen bereit. Jeder Datensatz wird durch einen Schlüssel eindeutig identifiziert (vgl. Abschnitt 2.1.2.4); das Modifizieren des Schlüssels ist bei LDAP als eigene Funktion realisiert, die als Umbenennen bezeichnet wird.

Auf I&AM ausgelegte LDAP-Serverprodukte generieren bei jeder Änderung am Datenbestand eine Ereignisnachricht, die beispielsweise von den unten beschriebenen Konnektoren ausgewertet werden kann; bei relationalen Datenbanken entspricht dies einer Unterstützung von *Triggern*, die an so genannte *stored procedures* gekoppelt sind und weitere Aktionen initiieren können.

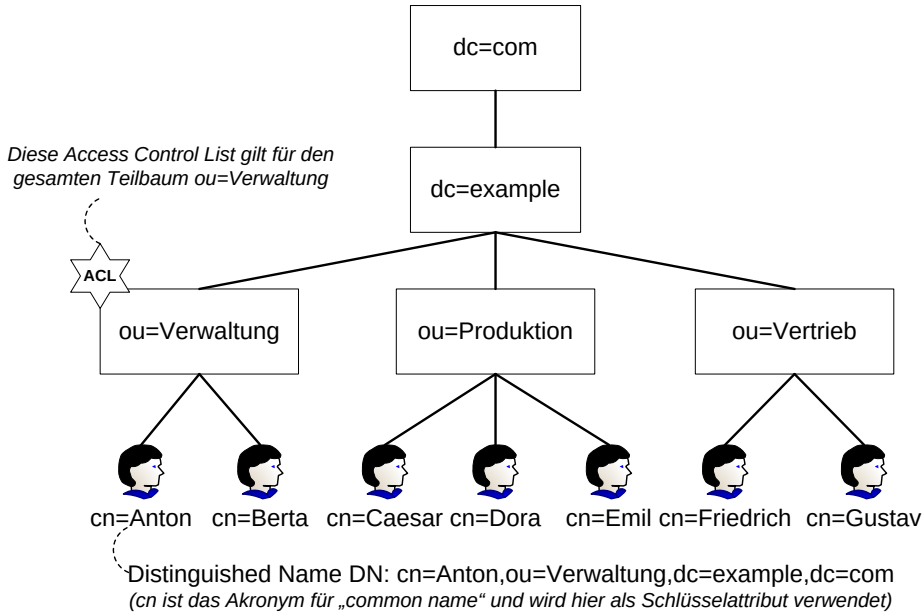


Abbildung 4.5.: LDAP-Datenmodell: Exemplarischer Directory Information Tree

4.3.1.2. Datenmodell

Die Datenmodelle von LDAP-Servern und relationalen Datenbanken unterscheiden sich grundlegend und werden getrennt skizziert.

LDAP-Server speichern Daten objektorientiert; das Design eines entsprechenden Datenmodells beginnt mit der in Abschnitt 2.1.2.4 erläuterten syntaktischen Beschreibung der Attribute, die zu einem Objekt gehören können oder müssen. In einem weiteren Schritt muss die hierarchische Anordnung der Objekte im so genannten Directory Information Tree (DIT) festgelegt werden. Somit ist es beispielsweise wie in Abbildung 4.5 dargestellt möglich, Mitarbeiterobjekte hierarchisch anhand ihrer Abteilungszugehörigkeit anzuordnen. Der Zugriff auf einzelne Datensätze setzt somit neben der Kenntnis ihrer Attribute, deren Beschreibung in Form von Metadaten abgerufen werden kann, auch Wissen über ihre Positionierung im DIT voraus, das beispielsweise in Konnektoren vorhanden sein muss und nicht explizit im LDAP-Server hinterlegt werden kann.

Wie in Abschnitt 2.1.2.4 erläutert existieren verschiedene Möglichkeiten für die Modellierung z. B. mehrerer Anschriften einer Person; beispielsweise können multi-valued Attribute verwendet werden, mehrere Attribute in einem Objekt für Anschriften vorgesehen werden oder dedizierte Adressobjekte im DIT unterhalb der jeweiligen Personenobjekte platziert werden. Dies ermöglicht einerseits Optimierungen für bestimmte Suchanfragen, kann jedoch andererseits zu einer deutlich höheren Komplexität, beispielsweise von Konnektoren, führen.

In relationalen Datenbanken werden Datensätze in Tabellenform organisiert; zur Vermeidung redundanter Datenspeicherung und daraus resultierender potentieller Konsistenzprobleme wird das Datenmodell in der Regel in eine Normalform gebracht, so dass beispielsweise Anschriften in einer eigenen Tabelle abgelegt werden und über ein Schlüsselattribut mit dem

Personendatensatz verknüpft werden. Der Zugriff setzt somit eine Kenntnis der Tabellen- und Spaltennamen voraus; diese syntaktischen Informationen können als Metadaten ausgelesen werden.

4.3.1.3. Kommunikationsschnittstellen

Das standardisierte, TCP/IP-basierte Protokoll LDAP ist hersteller- sowie plattformunabhängig und stellt alle genannten Funktionen bereit; für Bulkoperationen wie den Im- bzw. Export großer Datenmengen kommen Textdateien im ebenfalls standardisierten LDIF-Format (LDAP Data Interchange Format) zum Einsatz. Das Protokoll LDAP steht auch in verschlüsselten Varianten zur Verfügung (LDAPS bzw. LDAP+TLS).

Das Auslesen von in LDAP-Servern gespeicherten Datensätzen geschieht ausschließlich über Suchanfragen,[1] denen der Wurzelknoten des zu durchsuchenden DIT-Teilbaums, die gewünschte Suchtiefe und ein geeigneter Suchfilter übergeben werden muss. Über eine LDAP-Verbindung können beliebig viele Suchanfragen angestoßen werden, die optional vom Server nicht nur sequentiell, sondern auch parallel bearbeitet werden können; dabei wird jeder Suchanfrage ein numerischer Identifikator zugewiesen, anhand dessen Anfragen und asynchron eintreffende Antworten korreliert werden können. Schreibende Zugriffe erfordern die genaue Kenntnis der Position des betroffenen Objekts, die durch seinen so genannten Distinguished Name (DN) ausgedrückt wird (vgl. Abbildung 4.5).

Der Zugriff auf relationale Datenbanken setzt hersteller- bzw. produktspezifische Protokolle voraus, die in der Regel IP-basiert sind; die proprietären Treiber werden meist in standardisierte Datenbankframeworks eingebunden, beispielsweise JDBC für die Programmiersprache Java. Anfragen werden in der Structured Query Language (SQL) gestellt, die zwar standardisiert ist, von vielen Herstellern aber mit leichten Abweichungen implementiert wird, die in Clientsystemen berücksichtigt werden müssen. Die Kommunikation mit der Datenbank erfolgt in der Regel unverschlüsselt; mehrere Hersteller bieten inzwischen Zusatzmodule für verschlüsselte Kommunikation an, die aber überwiegend im Auslieferungszustand nicht aktiviert und zum Teil mit zusätzlichen Lizenzkosten verbunden sind.

4.3.1.4. Kommunikationspartner

Identity Repositories zeichnen sich dadurch aus, dass viele andere Systeme zumindest lesend darauf zugreifen können: Zum einen werden sie von ans I&AM-System angeschlossenen Diensten verwendet, die nicht über das User Provisioning angebunden sind; zum anderen können *alle* der nachfolgend erläuterten I&AM-Komponenten darauf zugreifen.

Für FIM-Komponenten erfolgt der Zugriff über die in Abschnitt 4.4 beschrieben FIM-Konnektoren.

4.3.1.5. Interne Sicherheitsmechanismen

Der Verbindungsaufbau mit einem LDAP-Server ist zwangsweise mit einer Authentifizierungsphase verbunden, die als LDAP-Bind bezeichnet wird. Dabei wird jedoch zwischen einem *an-*

[1] In LDAP existiert keine Operation „Lesen“ – diese wird durch das „Suchen“ impliziert.

onymous bind und einem LDAP-Bind als individueller Benutzer unterschieden, d. h. LDAP-Server sind prinzipiell auch für eine anonyme, unauthentifizierte Nutzung geeignet, um beispielsweise öffentlichen lesenden Zugriff auf elektronische Telefonbücher zu ermöglichen.

Die Authentifizierungsmöglichkeiten beim LDAP-Bind sind äußerst flexibel; neben der am häufigsten eingesetzten Authentifizierungsmethode über Benutzername und Passwort sind beispielsweise je nach Hersteller auch Clientzertifikate und Kerberostickets möglich.

Für alle im LDAP-Server gespeicherten Teilbäume und Objekte können Access Control Lists (ACLs) definiert werden, die regeln, welche Benutzer Zugriff haben; je nach Produkt sind dabei Einschränkungen der Zugriffsart, z. B. auslesend oder löschend, bis zur Granularität einzelner Attribute realisierbar (vgl. Abbildung 4.5).

Zum Zugriff auf relationale Datenbanken ist in der Regel eine Benutzername-/Passwortkombination erforderlich, wobei je nach Produkt unauthentifizierte Zugriffe über die Vergabe leerer Passwörter realisiert werden können; über so genannte *Views* kann die Sichtbarkeit von Tabellenspalten und damit von Benutzerattributen gesteuert werden. Darüber hinaus kann die Verwendung von SQL-Befehlen wie *insert* und *delete* pro Benutzer und Datenbanktabelle eingeschränkt werden.

4.3.1.6. Einbettung in die Sicherheitsinfrastruktur

Ein Identity Repository ist eine Softwarekomponente, die in der Regel auf einer dedizierten Servermaschine betrieben wird. Somit ergeben sich folgende Sicherheitsmaßnahmen, die analog für vergleichbare Komponenten gelten:

- Zugriffe und Aktivitäten können in nahezu beliebiger Granularität mitprotokolliert werden. **Protokolldateien** können zentral gesammelt und im Rahmen von Auditingmaßnahmen ausgewertet werden. Der anzustrebende Detaillierungsgrad ist ein Kompromiss aus ableitbaren Erkenntnissen und zu verarbeitenden Datenmengen – auch vor dem Hintergrund datenschutzrechtlicher und anderer juristischer Randbedingungen wie Compliance-Anforderungen (vgl. [ZRF05]).

- Der Netzwerkzugang zum System kann über **Paketfilterfirewalls** auf Clientsysteme, deren IP-Adressen bekannt sind, eingeschränkt werden. In der Regel werden Identity Repositories in einer Sicherheitszone für organisationsinterne Serversysteme positioniert, auf die keine Zugriffe von außerhalb der Organisation möglich sind, und die auch von Mitarbeiternetzen geeignet abgeschirmt ist, sofern das Identity Repository nicht beispielsweise als organisationsinternes E-Mail-Adressbuch eingesetzt werden soll. Die Kommunikationswege zu anderen benötigten, aber nicht I&AM- oder sicherheitsspezifischen Komponenten, beispielsweise zu Backup-, DNS- und NTP-Servern, können ebenfalls über Firewalls abgesichert werden.

- Die **verschlüsselte Kommunikation** basiert in der Regel auf hybriden Verschlüsselungsverfahren,[2] wobei die Authentizität des Public Keys des Servers durch ein von einer Certificate Authority signiertes Zertifikat beglaubigt wird. Für die Ausstellung

[2] Hybride Verschlüsselungsverfahren verwenden asymmetrische Verschlüsselungsverfahren zur Authentifizierung des Kommunikationspartners und zur Vereinbarung eines Sitzungsschlüssel für die effizientere symmetrische Verschlüsselung der Nutzdaten.

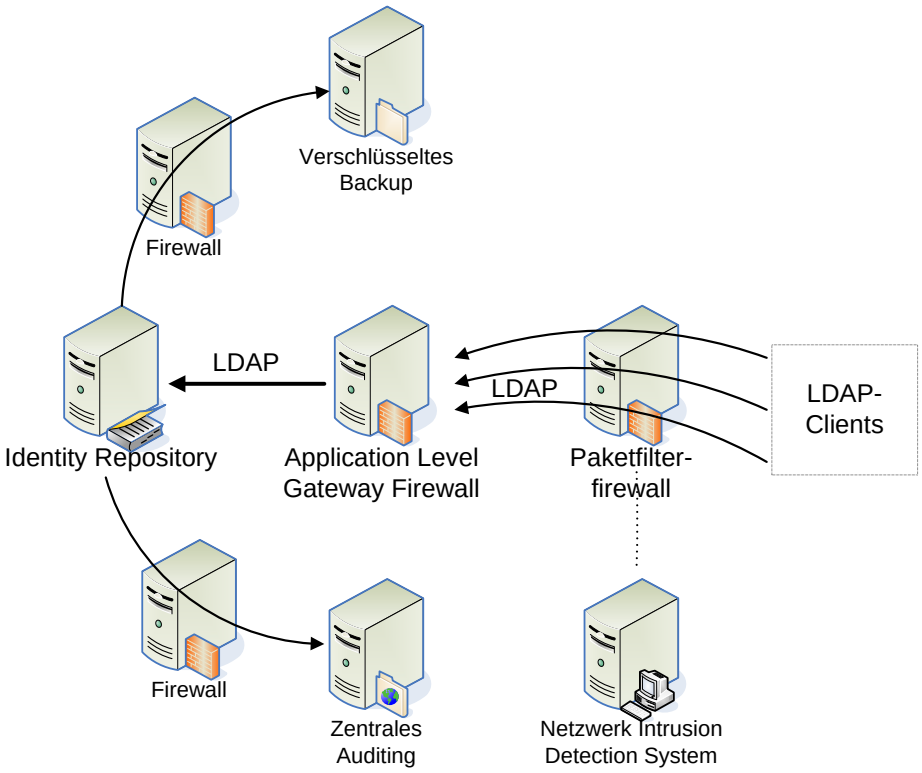


Abbildung 4.6.: Abschottung der I&AM-Komponente Identity Repository durch Firewalls

der Zertifikate für interne Server kann eine organisationsinterne PKI aufgebaut werden; alternativ können Zertifikate aus einer bekannten öffentlichen PKI eingesetzt werden, deren Verwendung sich insbesondere für von außen erreichbare Systeme empfiehlt, damit die Zertifikate auch von extern Zugreifenden ohne großen Zusatzaufwand verifiziert werden können.

- **Intrusion-Detection-Systeme** (IDS) können sowohl in lokal installierten Varianten (hostbasierte IDS) als auch netzwerkweit (netzbasierte IDS) wie bei anderen Serversystemen eingesetzt werden.

- Weitere Sicherheitsmaßnahmen wie Virenscanner können uneingeschränkt verwendet werden.

- Softwareupdates für den Dienst und das Betriebssystem können mit der allgemeinen Randbedingung durchgeführt werden, dass ein Neustart des Servers oder Dienstes mit einem typischerweise mehrminütigen Dienstausfall verbunden ist.

- Backups der Konfigurations- und Nutzdaten, die zum Schutz der Verfügbarkeit des Dienstes beitragen, sollten aufgrund des sensiblen Charakters insbesondere der Nutzdaten nur in verschlüsselter Form erfolgen.

Für LDAP-Server besteht darüber hinaus wie in Abbildung 4.6 dargestellt die Möglichkeit, in die Netzwerkverbindung mit den Clients einen Firewall der Kategorie **Application Level Gateway (ALG)** einzuschleifen. Der Client baut dabei eine Verbindung zum ALG auf, der wiederum eine Verbindung zum LDAP-Server herstellt; Anfragen des Clients können somit vom ALG ebenso wie Antworten des LDAP-Servers einer inhaltlichen Analyse unterzogen werden, bevor sie zur jeweiligen Gegenstelle weitergeleitet oder verworfen werden. Als ALGs können beispielsweise die unten beschriebenen virtuellen Verzeichnisdienste eingesetzt werden. Für Datenbanken besteht diese Möglichkeit aufgrund der verwendeten proprietären Protokolle im Allgemeinen nicht.

4.3.1.7. Hochverfügbarkeit

Die Hochverfügbarkeit zielt einerseits auf die Vermeidung von Dienstausfällen, z. B. bei Hardwaredefekten oder Softwareaktualisierungen, und andererseits auf die Sicherstellung der Dienstqualität bezüglich der Überlastung einzelner Servermaschinen bei einer hohen Anzahl paralleler Anfragen ab.

Sowohl LDAP-Server als auch Datenbanksysteme können auf folgende Arten hochverfügbar gemacht werden, die auch für viele der anderen erläuterten Komponenten verwendbar sind:

- **Replikate**: Es werden mehrere Servermaschinen verwendet, die dieselben Nutzdaten aufnehmen. Die Nutzdaten müssen zu diesem Zweck beispielsweise über Konnektoren oder herstellerspezifische Protokolle zwischen den Servern synchronisiert werden. Hierbei ist abhängig von den Fähigkeiten der eingesetzten Software zu unterscheiden, ob Schreibzugriffe nur auf einer der Maschinen, die als Master bezeichnet wird, durchgeführt werden dürfen, oder auf mehreren bzw. allen (**Multi-Master-Fähigkeit**).
- **High-Availability-Clustering** (HA-Clustering): Hierbei werden identisch konfigurierte Servermaschinen eingesetzt, die sich im Bedarfsfall gegenseitig ersetzen können; da nur jeweils eine Maschine Anfragen entgegen nimmt, kann mit dieser Technik keine Lastverteilung erreicht werden. Es handelt sich um ein so genanntes Hot-Standby-Verfahren, da alle am Cluster beteiligten Maschinen ständig in Betrieb sind und den Dienst innerhalb sehr kurzer Zeit übernehmen können.

Im Fall von Replikaten werden entweder die zugreifenden Clients so konfiguriert, dass sie üblicherweise das in der Netzwerktopologie für sie am günstigsten gelegene Replikat verwenden, oder es wird eine Lastverteilung beispielsweise über **DNS Round Robin** Verfahren realisiert, bei denen der zuständige DNS-Server zyklisch bei jeder Anfrage auf das nächste Replikat verweist. Bei einer HA-Clusterlösung übernimmt die jeweils gerade aktive Maschine die im DNS eingetragene IP-Adresse.

Eine Ergänzung zu Replikaten stellen **Service Load Balancer (SLBs)** dar; sie verteilen eingehende Anfragen an ein Replikat, das auf Basis seiner Verfügbarkeit und aktuellen Auslastung bestimmt wird. Sofern die Auslastung nicht ermittelt werden kann, kommen Heuristiken, randomisierende Verfahren oder klassische Round-Robin-Verfahren zum Einsatz.

SLBs und DNS-Round-Robin-Verfahren eigenen sich bei LDAP-Servern nur bedingt, da diese im Unterschied zu modernen relationalen Datenbanken **keine Transaktionssicherheit** bieten: Da die Synchronisation zwischen den Replikaten einige Sekunden dauern kann, könnte

somit beispielsweise der Fall eintreten, dass eine an einem Replikat durchgeführte Änderung bei einem nachfolgenden Lesezugriff auf ein anderes Replikat verloren geht (so genanntes *lost update*). Diese Verfahren bieten sich somit primär für reine Lesezugriffe an, bei denen keine hundertprozentige Datenaktualität benötigt wird. Zudem sind SLBs selbst wiederum redundant auszulegen, um keinen Single Point of Failure darzustellen.

4.3.1.8. Managementschnittstellen

Die Konfiguration eines Identity Repository erfolgt in der Regel kombiniert über lokale Konfigurationsdateien und herstellerspezifische, webbasierte Managementfrontends, die konfigurationsrelevante Daten in speziell geschützten Bereichen des Identity Repository ablegen. Diese Frontends unterstützen die Administratoren auch über die Protokolldateien hinaus bei eventuell notwendigen Fehlerfällen.

Der Status des Dienstes und Statistiken über seine Auslastung können bei vielen Produkten nicht nur über ein Webfrontend, sondern auch über SNMP abgerufen werden, wodurch eine einfache Anbindung an zentrale Monitoringsysteme ermöglicht wird.

Das Management der für den Zugriff autorisierten Benutzer läuft über das Identity Repository selbst; den jeweiligen Identitätsobjekten werden entsprechende Rollen und Berechtigungen zugewiesen, die z. B. zu den definierten Access Control Lists passen müssen. Ein Accounting der Nutzung des Identity Repository findet in der Regel nicht statt, da die syntaktische und semantische Auswertung von Anfragen und z. B. LDAP-Suchfiltern zu komplex ist; die Anzahl eingetragener Identitäten bzw. pro Abrechnungsperiode authentifizierter Benutzer spielt vielmehr für die Lizenzgebühren zahlreicher kommerzieller Produkte eine Rolle.

4.3.1.9. Begründung der Verwendung in der Gesamtarchitektur

Identity Management hat das explizite Ziel, eine einheitliche Sicht auf den gesamten Benutzerdatenbestand zu bieten; Identity Repositories bilden dabei die Grundlage von I&AM-Systemen und bieten die Möglichkeit, nicht nur die Daten aus verschiedenen Quellsystemen korreliert zu aggregieren, sondern bei Bedarf auch zusätzlich benötigte Daten zu jeder Identität zu hinterlegen. Wie in Abschnitt 4.5.1 gezeigt wird, ist ein Identity Repository eine zwingende Voraussetzung für die Nutzung der gesamten FIM-Funktionalität.

4.3.2. Konnektoren

Die bereits in Abschnitt 2.1.1.3 skizzierten Konnektoren verbinden jeweils zwei an der I&AM-Architektur beteiligte Systeme, zu denen neben I&AM-Komponenten auch Datenquellen und an ein User Provisioning System angeschlossene Dienste gehören können. Die Anzahl der Konnektoren ist somit proportional zur Anzahl der organisationsintern beteiligten Systeme, die keine integrierte Schnittstelle zum zentralen Datenbestand haben.

4.3.2.1. Funktionalität

Die wesentliche Aufgabe eines unidirektionalen Konnektors ist die kontinuierliche Synchronisation der in seinem Zielsystem gespeicherten Daten mit denjenigen seines Quellsystems.

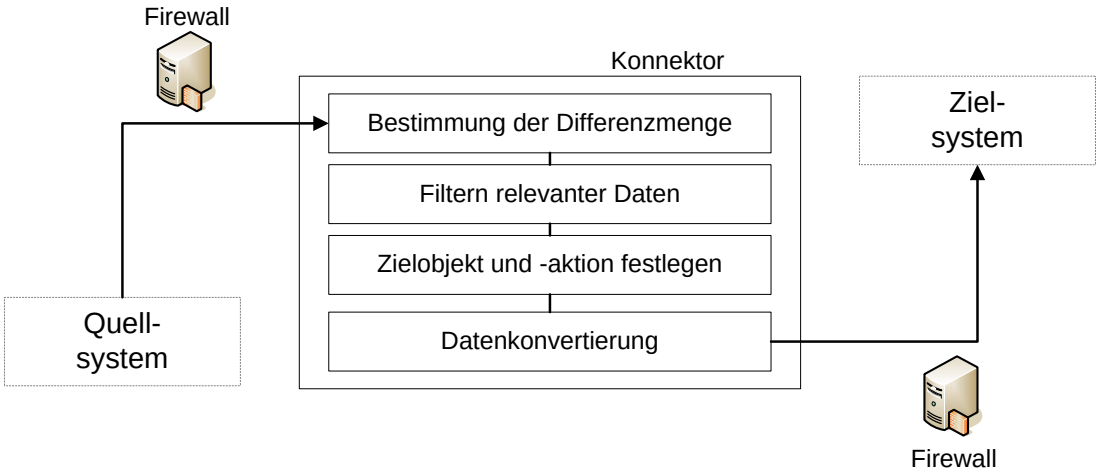


Abbildung 4.7.: Verarbeitungsschritte bei I&AM-Konnektoren

Unter Vernachlässigung von Optimierungsmöglichkeiten kann ein bidirektionaler Konnektor als logische Einheit zweier entgegengesetzt gerichteter unidirektionaler Konnektoren betrachtet werden.

Die Funktionalität ist durch den folgenden internen Arbeitsablauf gegeben, der auch in Abbildung 4.7 skizziert ist:

1. Aktivwerden des Synchronisierungsprozesses, das beispielsweise durch ein eingetretenes Änderungsereignis in einem Identity Repository, zeitgesteuert oder beim Start des Konnektors ausgelöst wird.
2. Der zu synchronisierende Datenbestand wird bestimmt; dieser wird dem Konnektor entweder in der Nachricht über das Änderungsereignis mitgeteilt, ist über Zeitstempel der Datensätze zu erkennen oder muss durch eine Differenzmengenbildung des aktuellen Datenbestandes mit dem Stand der letzten Synchronisation ermittelt werden. Die zu wählende Variante hängt von der Flexibilität der Datenquelle und der Positionierung des Konnektors ab: Ein ins Zielsystem integrierter Pull-Konnektor (vgl. Abschnitt 2.1.1.3) hat in der Regel keinen Zugriff auf Ereignisnachrichten der Datenquelle, wodurch dieser Vorverarbeitungsschritt deutlich aufwendiger wird.
3. Die ermittelten Differenzdatenbestände werden hinsichtlich ihrer Relevanz analysiert; Attribute im Quellsystem, die für das Zielsystem nicht benötigt werden, können mittels eines sogenannten Attributsfilters verworfen werden.
4. Anhand der Schlüsselattribute werden der im Zielsystem betroffene Datensatz und die entsprechend notwendige Aktion bestimmt; wurde im Quellsystem beispielsweise ein Datensatz angelegt, der im Zielsystem schon mit abweichenden Attributen existiert, kann im Konnektor eine Modifikations- statt einer Additionsoperation notwendig oder eine Fehlerbehandlung ausgelöst werden.
5. Die Daten werden in das im Zielsystem benötigte Format konvertiert; die Programmierung der Konvertierungsschritte erfolgt je nach Hersteller in einer proprietären Skript- oder einer herkömmlichen Programmiersprache wie Java.

6. Die konvertierten Daten werden ins Zielsystem geschrieben oder im Konnektor gepuffert, falls dieses temporär nicht verfügbar ist.

Je nach Flexibilität der eingesetzten Software kann eigener Programmcode integriert werden, über den beispielsweise weitere externe Datenquellen mit einbezogen werden können, um dynamisch Daten ins Zielsystem einspeisen zu können, die im Quellsystem nicht enthalten sind. Ebenso muss Programmlogik zur schlüsselattributsunabhängigen Korrelation von Datensätzen, z. B. auf Basis von Vor- und Nachname sowie Geburtsdatum der erfassten Person, in der Regel zusätzlich implementiert werden.

4.3.2.2. Datenmodell

Aufgrund ihrer Aufgabe unterstützen Konnektoren mindestens die Datenmodelle des jeweiligen Quell- und Zielsystems. Programmierbare Konnektorenframeworks setzen analog zu EAI-Ansätzen (vgl. Abschnitt 3.8.6) häufig auf ein internes Datenformat, das typischerweise XML-basiert ist und so die Transformation ins Zielformat erleichtern soll.

Da die Unterstützung für die Datenmodelle und die Konvertierungsregeln bei allen aktuell verfügbaren Produkten fest in den Konnektor integriert werden, eignet sich ein Konnektor für die Verwendung mit genau einer Kombination aus Quell- und Zielsystemen. Wie in Abschnitt 2.2.1.2 beschrieben eignen sich I&AM-Konnektoren daher nicht für den skalierbaren organisationsübergreifenden Einsatz.

4.3.2.3. Kommunikationsschnittstellen und Kommunikationspartner

Konnektoren kommunizieren mit ihren Quell- und Zielsystemen über deren gegebenenfalls proprietäre Schnittstellen. Um von Quellsystemen oder Identity Repositories generierte Nachrichten über Änderungen am Datenbestand verarbeiten zu können, werden Konnektoren häufig in die Datenquelle integriert; das eingesetzte Kommunikationsprotokoll ist in diesen Fällen herstellerabhängig.

Für die Anbindung von Zielsystemen bietet sich neben deren nativen Protokollen auch die in Abschnitt 3.7.1 vorgestellte Service Provisioning Markup Language (SPML) an, sofern diese vom jeweiligen Zielsystem unterstützt wird; der Konnektor würde in diesem Fall als Requesting Authority (RA) agieren und mit einem vom Zielsystem bereitzustellenden Provisioning Service Provider (PSP) kommunizieren.

Die Möglichkeit zur Anbindung von Quellsystemen mittels SPML beschränkt sich zwangsweise auf Systeme, die für die Speisung von Diensten geschaffen worden sind und SPML in der Rolle als RAs unterstützen. Der Einsatz von Konnektoren wird in diesem Fall auch nur dann benötigt, wenn das Zielsystem nicht SPML-fähig ist; der Konnektor würde somit als PSP agieren und über ein herkömmliches Protokoll mit dem Provisioning Service Target (PST) kommunizieren.

Von mehreren Konnektoren benötigte Programmlogik, beispielsweise für die Untersuchung der übertragenen Daten auf Plausibilität, wird bevorzugt auf dedizierte Server ausgelagert (siehe Abschnitt 4.3.9) und kann beispielsweise über RPC, Java-RMI oder Web Services angebunden werden.

4.3.2.4. Interne Sicherheitsmechanismen

Die von Herstellern ausgelieferten Standardkonnektoren verfügen neben der Authentifizierung von Quell- und Zielsystemen über keine expliziten Sicherheitsmechanismen, erhalten in den Zielsystemen jedoch meist nahezu uneingeschränkte Lese- und Schreibrechte. Fehler in der Programmlogik wirken sich deshalb auf die Zielsysteme ebenso direkt aus wie unerwünschte Änderungen in Quellsystemen, die beispielsweise kompromittiert worden sind und von einem Angreifer kontrolliert werden.

Neben umfassenden Tests von Konnektoren vor der Produktivführung und ständiger Überwachung des Regelbetriebs können somit nur zusätzlich implementierte Plausibilitätsprüfungen dazu beitragen, dass lediglich berechtigte und erwünschte Änderungen in den Zielsystemen vorgenommen werden.

4.3.2.5. Einbettung in die Sicherheitsinfrastruktur

Bei der Integration von Konnektoren in Quell- bzw. Zielsysteme können die für diese Systeme definierten Sicherheitsmaßnahmen übernommen werden (siehe Abschnitt 4.3.1.6). Diese gelten auch analog, wenn ein Konnektor auf einer dedizierten Maschine betrieben wird. Dabei muss darauf geachtet werden, in beteiligten Paketfilter-Firewalls Verbindungen zum Quell- und Zielsystem sowie zu eventuell benötigten externen Werkzeugen (siehe Abschnitt 4.3.2.3) zuzulassen. Die eingesetzten Firewalls dienen dabei primär dem Schutz der Quell- und Zielsysteme und nur sekundär dem Schutz der Konnektoren.

4.3.2.6. Hochverfügbarkeit

In Quell- oder Zielsysteme integrierte Konnektoren müssen zur Sicherstellung der Hochverfügbarkeit in jeder Instanz ihres Wirtssystems installiert werden; eine Ausnahme bilden Konnektoren, die schreibend auf Identity Repositories zugreifen, sofern dieses nicht die Eigenschaft hat, Master zu sein (vgl. Abschnitt 4.3.1.7).

Es ist zu beachten, dass ein Neustart des Konnektors, beispielsweise nach Softwareaktualisierung oder Konfigurationsänderung, lediglich mit einer sehr kurzen Betriebsunterbrechung im Sekundenbereich verbunden ist, von der andere Dienste nicht direkt betroffen sind. Änderungen, die sich während des Ausfalls eines Konnektors ergeben, werden nach dessen Neustart abgearbeitet.

Konnektoren, die auf dedizierten Servermaschinen betrieben werden, können auf Basis der in Abschnitt 4.3.1.7 beschriebenen HA-Clusteringtechnik hochverfügbar gemacht werden; da ein einzelner Konnektor zeitgemäße Hardware üblicherweise nicht auslastet, können mehrere Konnektoren pro Maschine betrieben oder es kann auf Hardware-Virtualisierungstechniken, die den Betrieb mehrerer virtueller pro physischer Maschine erlauben, zurückgegriffen werden.

4.3.2.7. Managementschnittstellen

Die Konfiguration und Fehleranalyse erfolgt typischerweise über webbasierte Managementfrontends, die vom Hersteller des Konnektorenframeworks mitgeliefert werden.

Ein praktisches Defizit stellt das Fehlen von Monitoringschnittstellen in vielen Produkten dar; der Ausfall von Konnektoren wird in diesen Fällen häufig erst bemerkt, wenn ausbleibende Datenänderungen im Zielsystem auffallen. Es ist jedoch davon auszugehen, dass Konnektoren zukünftig ebenfalls zentral, beispielsweise über SNMP, überwacht werden können.

4.3.2.8. Begründung der Verwendung in der Gesamtarchitektur

Kein I&AM-System kommt ohne Konnektoren aus, da die manuell und parallel zu den anderen Systemen durchgeführte Pflege sämtlicher Personendaten in einem Identity Repository im offensichtlichen Widerspruch zu den Zielen des organisationsinternen Identity Managements stehen würde. Die hier dargestellte Funktionalität ergibt sich aus den derzeit verfügbaren Produkten zahlreicher Hersteller; in Kombination mit den anderen I&AM-Komponenten können somit sehr flexibel szenarienspezifische I&AM-Architekturen entwickelt werden.

4.3.3. Meta-Directories

Ein Meta-Directory stellt wie in Abschnitt 2.1.1.5 erläutert und in Abbildung 4.8 dargestellt eine Kombination aus Identity Repository und damit verbundenen Konnektoren dar. Aufgrund dieser Eigenschaft gelten die in den beiden vorangehenden Abschnitten getroffenen Aussagen.

Es ist zu beachten, dass kommerzielle Meta-Directory-Produkte nahezu ausschließlich einen LDAP-basierten Verzeichnisdienst als Identity Repository einsetzen und relationale Datenbanken nur noch sehr selten Verwendung finden. Bei kommerziellen Produkten steht zum Management des Identity Repository und der Konnektoren darüber hinaus ein gemeinsames, in der Regel webbasiertes Managementfrontend zur Verfügung.

4.3.4. Virtuelle Verzeichnisdienste

Die ebenfalls in Abschnitt 2.1.1.5 bereits skizzierten virtuellen Verzeichnisdienste agieren darauf zugreifenden Clients gegenüber wie reguläre LDAP-basierte Identity Repositories; sie verfügen jedoch, ggf. abgesehen von Caches, über keine eigenen Datenbestände, sondern beantworten wie in Abbildung 4.9 dargestellt Anfragen durch dynamische Zugriffe auf externe Datenquellen wie beispielsweise Identity Repositories.

4.3.4.1. Funktionalität

Die LDAP-Clients zur Verfügung gestellte Funktionalität entspricht der in Abschnitt 4.3.1.1 für Identity Repositories beschriebenen, wobei jedoch keine Änderungsbenachrichtigungen unterstützt werden.

Die clientseitig angestoßenen Operationen werden jedoch nicht auf einem lokalen Datenbestand ausgeführt, sondern an die jeweiligen Quellsysteme des virtuellen Verzeichnisdienstes weitergeleitet:

- Eingehende Anfragen können an mehr als ein Quellsystem weitergeleitet werden, woraufhin die einzelnen Antworten zu einem Gesamtresultat kombiniert werden, das dem

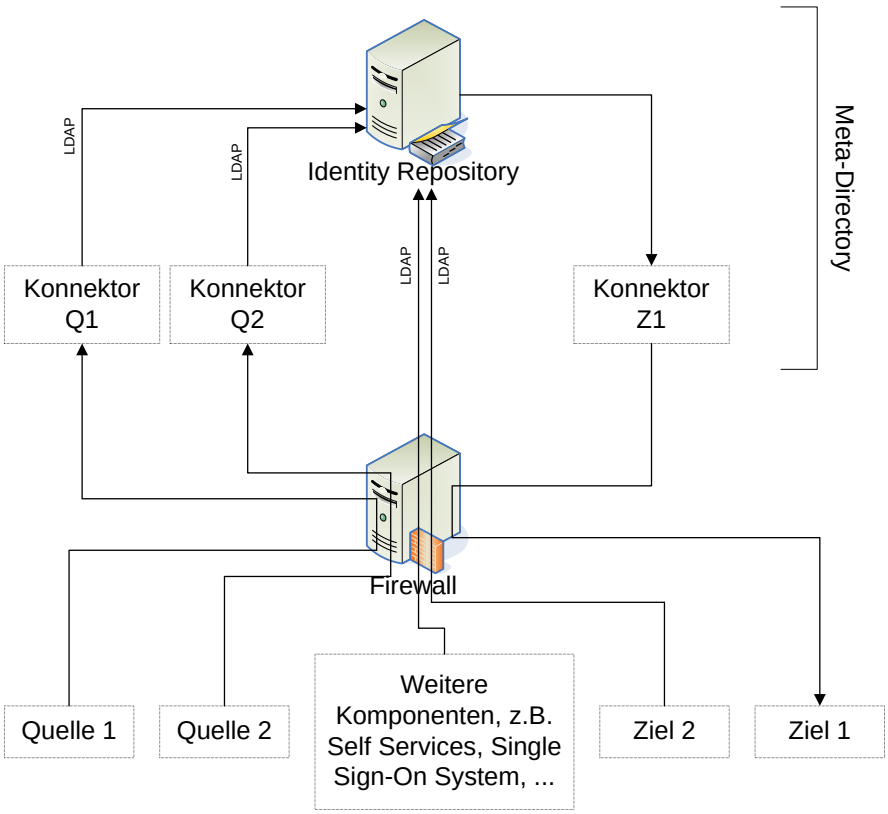


Abbildung 4.8.: Meta-Directory als logische Einheit aus Identity Repository und Konnektoren

Client zurückgegeben wird. Virtuelle Verzeichnisdienste ermöglichen somit aus Clientperspektive die **redundanzfreie Zusammenführung mehrerer Datenbestände**.

- Alternativ besteht die Möglichkeit, Anfragen zum Zweck einer **Lastverteilung** auf verschiedene identische Quellsysteme zu verteilen. Dieser Ansatz ist jedoch nur sinnvoll, wenn es sich typischerweise um komplexe Anfragen handelt, deren Beantwortung ressourcenintensiv ist; andernfalls würde anstelle der Datenquellen lediglich der virtuelle Verzeichnisdienst zum Flaschenhals werden.

- Die von Clients eingehenden Anfragen und die von den Quellsystemen gelieferten Antworten müssen vom virtuellen Verzeichnisdienst im Allgemeinen hinsichtlich der zum Einsatz kommenden Datenmodelle konvertiert werden. Dazu stehen Mechanismen zur Verfügung, die denen von Konnektoren entsprechen.

- Die notwendige Transformation von Anfragen und Antworten kann zu einer **Inhaltsanalyse** im Stil von Application Level Gateway Firewalls ausgebaut werden; nicht erlaubte Anfragen können verworfen werden und unerwünschte Bestandteile der Antworten von Quellsystemen können aus der Gesamtantwort an den Client herausgeschnitten werden (engl. *Content Filtering*).

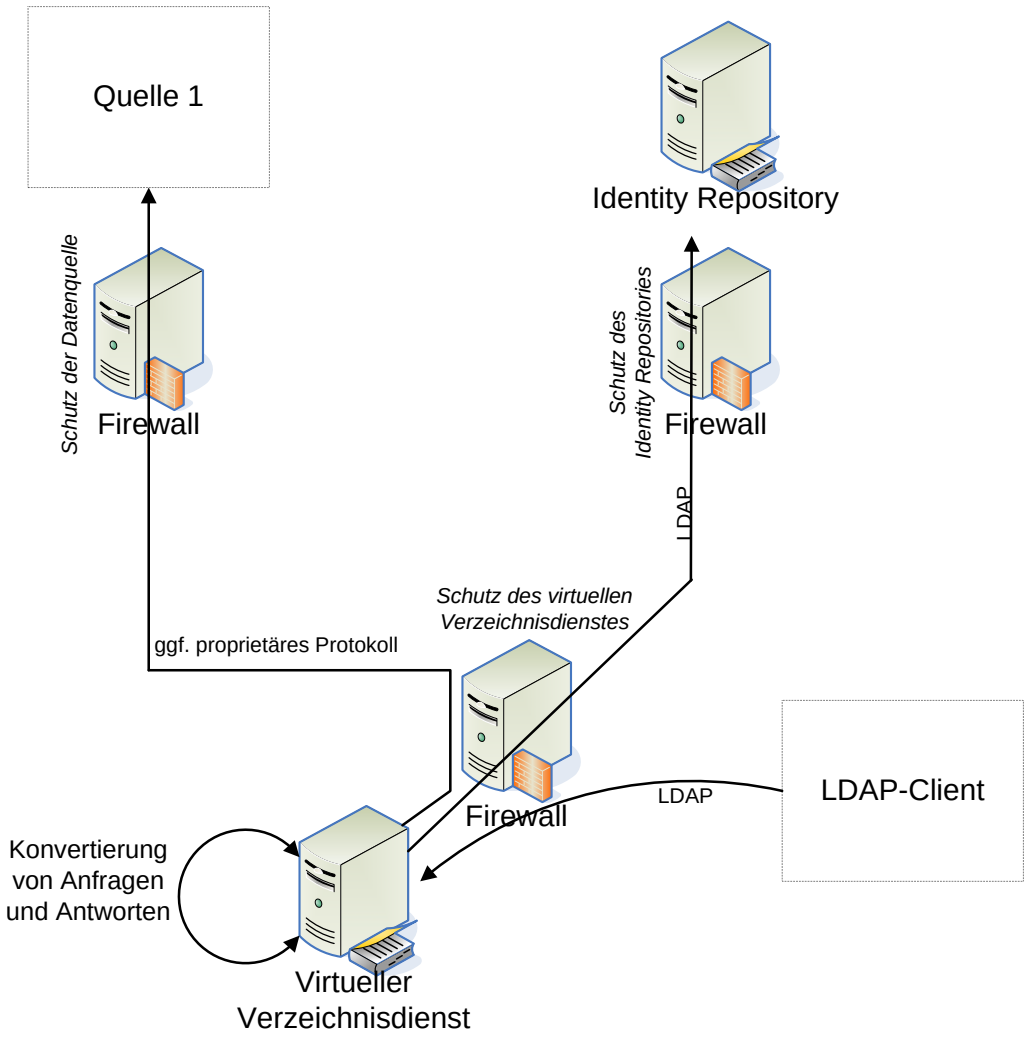


Abbildung 4.9.: Virtueller Verzeichnisdienst zur redundanzfreien Zusammenführung von Datenbeständen

Dabei ist zu berücksichtigen, dass die mögliche Dynamik durch eine bei den heutigen Produkten zwingend statische Konfiguration des virtuellen Verzeichnisdienstes beschränkt ist und dass die zur Laufzeit durchgeführten Anfragen an die Quellsysteme in Kombination mit der Datentransformation und der optionalen Inhaltsanalyse **deutliche Auswirkungen auf die Performanz** haben; ebenso hängt die Vollständigkeit einer von einem virtuellen Verzeichnisdienst gelieferten Antwort von der **Verfügbarkeit der Quellsysteme zum Zeitpunkt der Anfrage** ab.

4.3.4.2. Datenmodell

Für die von virtuellen Verzeichnisdiensten unterstützten Datenmodelle gelten im Wesentlichen dieselben Aussagen wie für Konnektoren (siehe Abschnitt 4.3.2.2). Davon abweichend präsentieren sich virtuelle Verzeichnisdienste ihren Clients gegenüber immer als LDAP-Server, für die analog zu den Ausführungen in Abschnitt 4.3.1.2 ein entsprechendes Datenmodell samt Directory Information Tree festgelegt werden muss. Dieses orientiert sich in der Regel an den Anforderungen der Clients, da virtuelle Verzeichnisdienste häufig dann zum Einsatz kommen, wenn die Clients LDAP-fähig sind, jedoch das von einem bereits vorhandenen Identity Repository eingesetzte Datenmodell nicht verwenden können, da sie nicht entsprechend flexibel konfigurierbar sind.

4.3.4.3. Kommunikationsschnittstellen und Kommunikationspartner

Das Kommunikationsverhalten virtueller Verzeichnisdienste entspricht dem von Meta-Directories, wobei der Datenaustausch mit den Quellsystemen jedoch nicht bei Änderungen an den Datenbeständen, sondern bei jeder clientseitigen Anfrage stattfindet.

4.3.4.4. Interne Sicherheitsmechanismen

Virtuelle Verzeichnisdienste bieten prinzipiell dieselben Sicherheitsmechanismen wie LDAP-basierte Identity Repositories (siehe Abschnitt 4.3.1.5).

Darüber hinaus ist zu unterscheiden, ob die dynamischen Anfragen an die Quellsysteme im Sicherheitskontext einer Pseudokennung für den virtuellen Verzeichnisdienst durchgeführt werden, oder ob die Anmeldeinformationen, mit der sich Clients zum virtuellen Verzeichnisdienst verbinden, an die Quellsysteme durchgereicht werden, um dort eine detailliertere Rechtedifferenzierung zu ermöglichen. Während die letztere Variante aus Sicherheitsperspektive sehr vorteilhaft ist, bedeutet sie in der Praxis einen erheblichen Mehraufwand bei der Konfiguration der Quellsysteme, dessen Notwendigkeit in konkreten Szenarien individuell ermittelt werden muss.

4.3.4.5. Einbettung in die Sicherheitsinfrastruktur

Für virtuelle Verzeichnisdienste können dieselben Sicherheitskonzepte wie für Identity Repositories angewendet werden (siehe Abschnitt 4.3.1.6).

Dabei ist zu beachten, dass die Speisung von Identity Repositories möglicherweise ausschließlich von den Datenquellen initiiert wird, während virtuelle Verzeichnisdienste bei der Weiterleitung von Anfragen immer selbst die Verbindungen zu den Datenquellen aufbauen; sofern eingesetzte Paketfilterfirewalls nicht nur die Verbindungsendpunkte, sondern auch den Richtung des Verbindungsaufbaus, z. B. über die Kombination aus SYN- und ACK-Flag im Header von TCP-Paketen, einschränken, müssen diese entsprechend konfiguriert werden.

4.3.4.6. Hochverfügbarkeit

Virtuelle Verzeichnisdienste können wie Identity Repositories hochverfügbar gestaltet werden; die Replikation entspricht in diesem Fall dem parallelen Betrieb mehrerer analog konfigurierter virtueller Verzeichnisdienste, wobei keine Einschränkungen hinsichtlich der Eigenschaft, Mastersystem zu sein, existieren.

4.3.4.7. Managementschnittstellen

Das Management von virtuellen Verzeichnisdiensten erfolgt analog zu dem von Meta-Directories, wobei sich die Administration des virtuellen Identity Repository auf die Konfiguration des den Clients präsentierten Datenmodells beschränkt.

4.3.4.8. Begründung der Rolle in der Gesamtarchitektur

Wie in Abschnitt 4.5.1 gezeigt wird, spielen virtuelle Verzeichnisdienste im Rahmen von FIM nur eine untergeordnete Rolle, da typischerweise die Möglichkeit zur Speicherung zusätzlicher, d. h. in den Quellsystemen nicht vorgesehener Datenfelder fehlt und eine unerwünscht starke Abhängigkeit von der aktuellen Verfügbarkeit der Quellsysteme vorhanden ist. Virtuelle Verzeichnisdienste stellen jedoch ein mächtiges, wenn auch häufig unterschätztes Werkzeug für I&AM-Architekturen dar, deren Funktionalität im Rahmen des Identitätsdatenkonverters, der in Abschnitt 4.4.12 vorgestellt wird, auf FIM übertragen wird.

4.3.5. Provisioningsysteme

Wie in Abschnitt 2.1.1.5 beschrieben verhalten sich Provisioningsysteme komplementär zu virtuellen Verzeichnisdiensten, da sie Änderungen der Datenbestände in Quellsystemen in einem Push-Verfahren an die angeschlossenen Zielsysteme weiterleiten, ohne die Daten in einem eigenen Identity Repository vorzuhalten.

4.3.5.1. Funktionalität

Provisioningsysteme können bezüglich ihrer Funktionalität mit komplexen Konnektoren verglichen werden, die mehr als ein Quell- und ein Zielsystem unterstützen. Änderungen, die sich in einem der Quellsysteme ergeben, werden dabei selektiv an die angeschlossenen Zielsysteme propagiert und hierzu konvertiert sowie gegebenenfalls gepuffert, falls ein Zielsystem temporär nicht verfügbar ist.

4.3.5.2. Datenmodell und Kommunikationsverhalten

Bezüglich der unterstützten Datenmodelle, Kommunikationsschnittstellen und Kommunikationspartner gelten dieselben Aussagen wie für Konnektoren; insbesondere findet kein Zugriff auf Provisioningsysteme durch Clients statt. Die Datenflüsse von Quell- zu Zielsystemen werden über das Provisioningsystem jedoch analog zu Meta-Directories kanalisiert und gegenüber Lösungen mit individuellen Konnektoren von jedem Quell- zu jedem Zielsystem klar strukturiert.

4.3.5.3. Interne Sicherheitsmechanismen und Einbettung in die Sicherheitsinfrastruktur

Das Sicherheitsverhalten von Provisioningsystemen entspricht dem in den Abschnitten 4.3.2.4 und 4.3.2.5 für Konnektoren erläuterten; da Provisioningsystem in der Regel auf dedizierten Servern betrieben werden, sind darüber hinaus die in Abschnitt 4.3.1.6 erläuterten Maßnahmen einsetzbar.

Da ein Provisioningsystem lediglich mit seinen Quell- und Zielsystemen und der Managementinfrastruktur kommunizieren können muss, kann es in einem entsprechend abgeschotteten organisationsinternen Netzwerk platziert werden; für die Verwendung von Firewalls gelten dieselben Aussagen wie bei den Konnektoren.

4.3.5.4. Hochverfügbarkeit

Da ein paralleler Betrieb mehrerer Provisioningsysteme für dieselben Datenquellen und -ziele nicht sinnvoll wäre, kann nur das in Abschnitt 4.3.1.7 beschriebene HA-Clusteringverfahren eingesetzt werden.

Sofern zum Zweck der Lastverteilung mehrere Provisioningsysteme eingesetzt werden sollen, sind diese isoliert voneinander zu betrachten. In der Regel sollten sie bei ansonsten gleicher Konfiguration für disjunkte Mengen von Zielsystemen zuständig sein, da eine disjunkte Aufteilung der Quellsysteme, ggf. in Kombination mit partiell überlappenden Zielsystemen, zu einer ungleich höheren Komplexität beispielsweise bei der Korrelation von Datensätzen und bei der Fehlersuche führen würde.

4.3.5.5. Managementschnittstellen

Provisioningsysteme weisen dieselben Managementeigenschaften wie Konnektoren auf (vgl. Abschnitt 4.3.2.7). Das Framework des Provisioningsystems, in das seine einzelnen Konnektoren eingebettet werden, kann darüber hinaus in der Regel über Schnittstellen wie SNMP überwacht werden.

4.3.5.6. Begründung der Rolle in der Gesamtarchitektur

Provisioningsysteme haben eine starke Berechtigung in I&AM-Systemen, an die Dienste, die nicht LDAP-fähig sind, angeschlossen werden müssen; im FIM-Kontext sind sie deshalb vor allem SP-seitig relevant. In diesem Architekturkonzept wird auf Provisioningsysteme jedoch verzichtet, da die hier benötigte Funktionalität äquivalent über eine Kombination aus Identity Repository und Konnektoren erzielt werden kann, und diese beiden Einzelkomponenten hinsichtlich ihres Zusammenspiels mit den FIM-Komponenten im Vordergrund stehen.

4.3.6. Organisationsinterne Privacy Management Systeme

Organisationsinterne Privacy Management Systeme (PMS) haben, wie aus ihrem Namen bereits hervorgeht, die im I&AM-Umfeld wesentliche Aufgabe, Policies zur Datenverarbeitung unter Datenschutzaspekten zu verwalten sowie ihre Umsetzung zu erzwingen und zu kontrollieren.

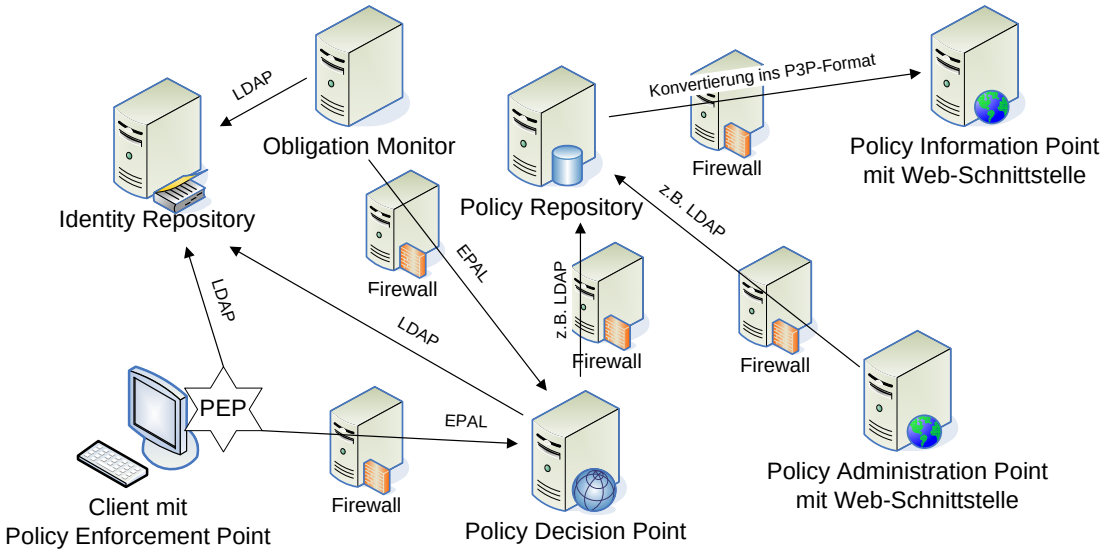


Abbildung 4.10.: Grundlegende Architektur eines organisationsinternen Privacy Management Systems

Wie in den Abschnitten 3.5 und 3.6 gezeigt wurde, existieren mehrere, zum Teil standardisierte Ansätze für verschiedene Aspekte von PMS, deren gesamtheitliche Zusammenführung jedoch noch nicht realisiert wurde und auch nicht im Fokus dieser Arbeit liegt. Um PMS in diesem Architekturkonzept berücksichtigen zu können, wird deshalb in diesem Abschnitt ein hypothetisches PMS mit seinen Schnittstellen zum I&AM-System geschildert, dessen Einzelkomponenten in Kapitel 3 erläutert wurden. Dabei wird vereinfachend davon ausgegangen, dass Schnittstellen zwischen diesen Komponenten zukünftig existieren werden; auf entsprechende Vorarbeiten wird entsprechend verwiesen.

4.3.6.1. Funktionalität

In seinem Kern besteht jedes PMS wie in Abbildung 4.10 dargestellt aus einem Policy Decision Point (PDP), der auf Basis von als Policies formulierten Regelwerken vor jedem Zugriff auf ein Element eines Datensatzes (z. B. Attribut einer Identität) entscheidet, ob der Zugreifende ausreichend berechtigt für diese Art des Zugriffs (z. B. Lesen, Modifizieren, Löschen) ist. Im Unterschied zu herkömmlichen und parallel einsetzbaren anderen Zugriffskontrollsystemen beschränken sich PMS auf **Datenschutzpolicies**, wobei jedoch insbesondere die **Versionierung der Policies** und ihre Veröffentlichung z. B. als Online-Datenschutzerklärung berücksichtigt werden müssen.

Die vom PDP ausgewerteten Policies müssen deshalb geeignet verwaltet und eingesehen werden können; die entsprechenden Komponenten eines PMS werden als Policy Administration Point (PAP) und Policy Information Point (PIP) bezeichnet. Die Speicherung der Policies erfolgt in einem Policy Repository (PR).

Jedes System, das von den Policies potentielle betroffene Daten verarbeitet, muss den PDP kontaktieren und die von ihm getroffene Entscheidung umsetzen, indem es den Zugriff darauf gestattet oder verwehrt; die entsprechend als Policy Enforcement Point (PEP) bezeichnete Komponente muss somit an der Schnittstelle zu den Daten oder gegebenenfalls in den Systemen, mit denen die Benutzer arbeiten, umgesetzt werden. Das PMS muss darüber hinaus einen weiteren PEP zur Verfügung stellen, der regelmäßig die Einhaltung von **Auflagen zur Langzeitdatenspeicherung**, beispielsweise das Löschen alter Daten nach einem bestimmten Zeitraum, in dem sie nicht mehr benötigt wurden, sicherstellt; er wird üblicherweise als **Obligation Monitor** (OM) bezeichnet.

4.3.6.2. Datenmodell

Im Rahmen dieses Architekturkonzepts wird davon ausgegangen, dass ein EPAL-basiertes PMS eingesetzt wird, dessen PIP die Policies zudem im von P3P vorgegebenen Format veröffentlichen kann (vgl. Abschnitte 3.5.2 und 3.5.1); dies entspricht einerseits dem aktuellen Stand der Technik und ist andererseits hinreichend flexibel für eine Übertragung auf andere Ansätze.

Für das Datenmodell und die Sicherstellung komponentenübergreifender Konsistenz ergeben sich somit folgende Anforderungen:

- In Identity Repositories gespeicherte Datensätze müssen um folgende Metadaten erweitert werden:
  - Die Versionen der Privacy Policies, die zum Zeitpunkt ihrer Erfassung gegolten haben, müssen explizit festgehalten werden. Diese Verknüpfung der Daten mit den sie betreffenden Policies entspricht auch einer Voraussetzung für die Umsetzung des Sticky-Policy-Paradigmas (siehe Abschnitt 3.6.2).
  - Sofern verschiedene Dienste oder Varianten eines Dienstes angeboten werden, sind darüber hinaus die mit dem jeweiligen Benutzer vereinbarten Datenverarbeitungszwecke festzuhalten.
  - Die Ausprägungen parametrisierbarer Obligationen oder anderweitig mit dem Benutzer individuell vereinbarter Auflagen sind ebenso explizit zu speichern.
- Für die Spezifikation konkreter EPAL-Policies sind Wertemengen für die in Abschnitt 3.5.2 aufgeführten Datenkategorien zu definieren, insbesondere für die *data users* und die Verarbeitungszwecke; eine Anlehnung an das P3P-Datenmodell erleichtert dabei die Abbildung von EPAL- auf P3P-Policies.
- Die Struktur des Policy Repository muss neben einer guten Wartbarkeit auch den effizienten Zugriff auf die für PDP-Anfragen relevanten Policies ermöglichen; beim Einsatz eines LDAP-Servers als Policy Repository bietet sich deshalb eine Aufgliederung des Directory Information Trees nach Verarbeitungszwecken und *data users* an.

Die Abbildung von EPAL- auf P3P-Policies wurde von IBM Research in [EPALP3] untersucht; die dabei verbleibenden notwendigen manuellen Eingriffe und die fehlende Möglichkeit zur Rückkonvertierung werden im Folgenden nicht näher betrachtet.

4.3.6.3. Kommunikationsschnittstellen und Kommunikationspartner

Das PMS kommuniziert mit den anderen I&AM-Komponenten und seinen Benutzern wie folgt:

- Der PDP benötigt zur Entscheidungsfindung neben Informationen über den zugreifenden Benutzer und den Policies Zugriff auf die Benutzerdaten, da die Entscheidung von Benutzerattributen und insbesondere den hinterlegten PMS-spezifischen Metadaten abhängt. Hierfür wird im Folgenden von einem direkten Zugriff auf das Identity Repository ausgegangen, obwohl auch der mittelbare Zugriff beispielsweise über einen virtuellen Verzeichnisdienst möglich wäre.
- Benutzer können die Policies typischerweise über eine webbasierte Schnittstelle einsehen, die P3P-Policies vom PIP bezieht; bei Diensten, die nicht webbasiert sind, beispielsweise beim interaktiven Login auf einem Hochleistungsrechner (vgl. Szenario 4), können die Policies ebenfalls über den PIP abgerufen werden, müssen allerdings entsprechend anders zur Anzeige aufbereitet werden.
- Die Administration des Systems und der Policies wird in Abschnitt 4.3.6.7 beschrieben.
- Die Nutzung der PDP-Funktionalität wird über die PEPs angestoßen und basiert auf dem von EPAL vorgegebenen Request-Response-Protokoll. Die PEPs selbst können einerseits in Identity Repositories wie LDAP-Server integriert werden und beispielsweise bei jeder LDAP-Anfrage aktiv werden, oder müssen in die datenverarbeitenden Applikationen eingebunden werden, was dem aufwendigeren, aber derzeit in der Praxis weiter verbreiteten Ansatz entspricht.

Abgesehen von der Verbindung zum Identity Repository ist das PMS somit vom I&AM-System weitgehend isoliert; in der Praxis zeigt sich dies in der weiten Verbreitung von I&AM-Systeminstallationen ohne PMS-Einsatz.

4.3.6.4. Interne Sicherheitsmechanismen

Die internen Sicherheitsaspekte von PMS wurden bislang nur unzureichend untersucht und werden hier auch nicht vertieft; in Anlehnung an allgemeine, policybasierte Zugriffskontrollsysteme können jedoch folgende Maßnahmen vorgesehen werden:

- Die Integrität der verarbeiteten Policies muss beispielsweise durch elektronische Signaturen sichergestellt werden. Ein diesbezüglich wesentlicher Aspekt ist, dass auch die Verfügbarkeit und Vollständigkeit aller Policies gewährleistet werden muss, da ein Angreifer andernfalls anstreben würde, Policies, die seine Rechte einschränken, zu entfernen oder anderweitig dem PDP vorzuenthalten.
- Bei der Implementierung von PEPs muss darauf geachtet werden, dass diese von einem Angreifer nicht umgangen werden können; insbesondere muss der PEP den PDP mit einem *starken* Verfahren authentifizieren, um zu verhindern, dass ein Angreifer den richtigen PDP gegen eine eigene Instanz austauscht.

Darüber hinaus muss sichergestellt werden, dass der Policy Administration Point nur von berechtigten Benutzern verwendet werden kann.

4.3.6.5. Einbettung in die Sicherheitsinfrastruktur

Der PDP ist das zentrale Element des PMS, das einerseits Clients zugänglich gemacht werden muss, andererseits einen hohen Schutzbedarf aufweist; somit können die in Abschnitt 4.3.1.6 diskutierten Maßnahmen angewendet werden.

Der PAP für Administratoren und der PIP für Benutzer sind in der Regel Webschnittstellen, die beispielsweise mit den in Abschnitt 4.3.7 diskutierten Self Services zusammengelegt werden können; somit ist die Umsetzung der dort besprochenen Schutzmaßnahmen für webbasierte Dienste anzustreben.

Für mit Identity Repositories kombinierte PEPs gelten die dort angegebenen Auflagen. In Applikationen integrierte PEPs werden hier nicht näher betrachtet; bei einer clientseitigen Ausführung müssen Gegenmaßnahmen zum Reverse Engineering getroffen werden, um eine Umgehung des PEPs zu verhindern.

Der Zugriff auf das Policy Repository kann ferner über Paketfilterfirewalls auf den PDP und den PAP eingeschränkt werden.

4.3.6.6. Hochverfügbarkeit

Alle Komponenten des PMS können über die in Abschnitt 4.3.1.7 beschriebenen Verfahren hochverfügbar gemacht werden; bei Policy Repositories ist hinsichtlich Replikaten analog zu Identity Repositories die Master-Eigenschaft zur Sicherstellung der Datenkonsistenz zu berücksichtigen.

Insbesondere der Hochverfügbarkeit des PDP kommt eine entscheidende Bedeutung zu, da ohne ihn kein Zugriff auf vom PMS kontrollierte Daten möglich ist und sein Ausfall somit zur praktischen Nichtverfügbarkeit des Identity Repositories führt.

4.3.6.7. Managementschnittstellen

Die Konfiguration des PMS umfasst neben den Grundeinstellung wie zu verwendenden Identity Repositories und zur Nutzung des PDP zugelassenen PEPs insbesondere die Verwaltung der Policies über den PAP. Eine wesentliche Eigenschaft ist die bereits im ARP-Kontext erwähnte verteilte Administration, da in der Regel organisationsweite Datenschutzvorgaben dienste- bzw. abteilungsspezifisch (z. B. Rechnungswesen, Marketingabteilung) verfeinert werden müssen; hieraus ergeben sich Auswirkungen u. a. auf die Gestaltung der Managementwerkzeuge und das Policydatenmodell. Diese Aspekte werden in Abschnitt 5.3 für ARPs vertieft und gelten hier analog, wobei Benutzer auf PMS-Policies nur optional in Form von parametrisierbaren Obligationen Einfluss haben.

Zur Überwachung des Systemstatus stellen die PMS-Komponenten Standardmechanismen wie SNMP zur Verfügung. Der Protokollierung, deren Detaillierungsgrad zur Fehleranalyse erhöht werden kann, kommt bei PMS eine wichtige Aufgabe zu: Da der PDP zur Entscheidungsfindung im Gegensatz zu einem Identity Repository nicht nur über die zugreifende Person und die abgerufenen Daten, sondern auch über den Verwendungszweck informiert wird, spielen PMS beispielsweise bei Compliance-Anforderungen eine wichtige Rolle. Protokolldateien eines PMS werden deshalb in der Regel länger aufbewahrt als diejenigen anderer Komponenten.

Zudem können Analysen durchgeführt werden, welche Arten von Zugriffen auffallend häufig abgelehnt werden; sie können neben der Erkennung von Angriffen auch Aufschluss über unzureichend spezifizierte Policies geben.

Die Benutzerverwaltung eines PMS unterscheidet zwischen Administratoren, Policyverwaltern und *data users*; sie ist in der Regel an das vorhandene Identity Repository angebunden.

4.3.6.8. Begründung der Verwendung in der Gesamtarchitektur

Der wesentliche technische Aspekt für die Integration eines PMS in die Gesamtarchitektur ist die in Abschnitt 4.4.4 erläuterte Notwendigkeit eines Obligation Monitors für das FIM Privacy Management. Aus organisatorischer Sicht ergibt sich hierdurch eine verbesserte Geschäftsprozessunterstützung durch ein durchgängiges organisationsinternes und -übergreifendes Privacy Management, das auch aufgrund zunehmender juristischer Randbedingungen immer wichtiger wird. Während PMS somit aus technischer Perspektive in rein organisationsinternen Identity Management Systemen eine optionale Komponente darstellen, ist ihr Einsatz im FIM-Umfeld dringend zu empfehlen.

4.3.7. Self Services und delegierte Administration

Die Administrationsaufgaben sind bei großen Benutzerdatenbeständen und einer Vielzahl angebotener Dienste nur effizient bewältigbar, wenn sie auf eine größere Anzahl der für die jeweiligen Aufgaben Zuständigen verteilt werden können. Das direkte Involvieren der Benutzer kann zudem die Datenqualität steigern, sofern diese in ihrem Eigeninteresse liegt und entsprechend motiviert wird.

Self Services (der Begriff ist gegenüber der deutschen Übersetzung „Selbstbedienungsfunktionen“ weiter verbreitet) werden als webbasierte Schnittstelle zu Benutzern und Administratoren mit eingeschränkten Rechten angeboten. Die Betrieb setzt somit neben der eigentlichen Applikationssoftware mindestens einen Webserver voraus; praktisch wird häufig ein dreischichtiges Architekturmodell eingesetzt, bei dem der Webserver die Präsentationsaufgaben übernimmt und der Programmcode für die Anwendungslogik von einem so genannten Application Server ausgeführt wird. Die Persistenzschicht entspricht entweder einem Identity Repository bzw. einem virtuellen Verzeichnisdienst oder einer Datenbasis, die über Konnektoren bidirektional mit einem Identity Repository synchronisiert wird.

4.3.7.1. Funktionalität

Self Services bieten jedem Benutzer einen geeignet eingeschränkten Lese- und Schreibzugriff auf die über ihn gespeicherten Daten. Damit wird einerseits dem Recht auf informationelle Selbstbestimmung nachgekommen und andererseits müssen beispielsweise für Passwortänderungen, Konfiguration von E-Mail-Adressen sowie Korrekturen der Kontakt- und Abrechnungsdaten keine Service Desk Mitarbeiter oder Administratoren involviert werden. Die Anwendungslogik muss Bedienungsfehler und offensichtliche Falscheingaben beispielsweise durch Plausibilitätsprüfung der Benutzereingaben verhindern. Für den Fall, dass Benutzer zusätzliche Berechtigungen beantragen können, wird in der Regel ein entsprechender Genehmigungsprozess angestoßen (siehe Abschnitt 4.3.9.3).

Dezentrale Administratoren (vgl. *Master User* in Szenario 3) erhalten vergleichbare Berechtigungen für eine Menge ihnen zugeteilter Benutzer und können ausgewählte Aspekte von Diensten konfigurieren, indem sie beispielsweise eigene Gruppen und Rollen definieren können. Je nach Abdeckungs- und Automatisierungsgrad des I&AM-Systems und Dienstspektrum kann zudem das manuelle Eintragen und Löschen von Benutzern über Self Services angeboten werden (vgl. Gästeverwaltung in Szenario 1).

Die Funktionalität von Self Services kann zwar nicht pauschal vollständig beschrieben werden, da sie szenarienabhängig ist; sie orientiert sich aber inhaltlich stark an den Möglichkeiten, die das Datenmodell des zugrunde liegenden Identity Repository bietet.

4.3.7.2. Datenmodell

Das von Self Services verwendete Datenmodell ist in der Regel sehr stark an das des darunter liegenden Identity Repository angelehnt und in der Applikation fest vorgegeben. Intern können davon abweichende Datenmodelle eingesetzt werden, die für verwendete Programmiersprache geeigneter sind oder Bulkoperationen auf mehreren Datensätzen effizienter gestalten.

4.3.7.3. Kommunikationsschnittstellen und Kommunikationspartner

Self Services kommunizieren mit ihren Benutzern und der verwendeten Datenbasis. Da es sich um Webapplikationen handelt, bei denen sensible Daten üblicherweise via Internet übertragen werden, erfolgt der clientseitige Zugriff verschlüsselt mittels des Protokolls HTTPS. Die Kommunikation mit der Datenbasis wird über eine von dieser angebotenen Schnittstelle realisiert, beispielsweise verschlüsseltes LDAP bei verzeichnisdienstbasierten Identity Repositories.

4.3.7.4. Interne Sicherheitsmechanismen

Die Nutzung der Self Services setzt wie die Verwendung vieler anderer webbasierter Dienste die Authentifizierung von Benutzern voraus; hierfür kommen neben der klassische Anmeldung mittels Benutzername und Passwort insbesondere Single-Sign-On-Verfahren in Frage (siehe Abschnitt 4.3.8).

Um Missbrauch, beispielsweise durch gestohlene Passwörter, zumindest einzuschränken, werden die über Self Services einsehbaren Benutzerdaten partiell unkenntlich gemacht, z. B. indem von Konto- oder Kreditkartennummern nur die ersten Stellen angezeigt werden, die für eine Wiedererkennung ausreichen, ohne die restlichen Informationen für einen Angreifer jedoch nutzlos sind.

Zugriffe auf die Datenbasis werden – sofern von dieser ermöglicht – im Kontext des Self-Service-Benutzers durchgeführt, dessen Rechte auf die für ihn relevanten Bereiche beschränkt sind; sofern nicht direkt auf das Identity Repository schreibend zugegriffen wird, können Sicherheitsprobleme, die von der Self-Service-Applikationslogik nicht erkannt werden, eventuell von der im Konnektor zum Identity Repository enthaltenen Programmlogik erkannt werden, bevor sie sich auf das gesamte I&AM-System auswirken (vgl. Abschnitt 4.3.2.3).

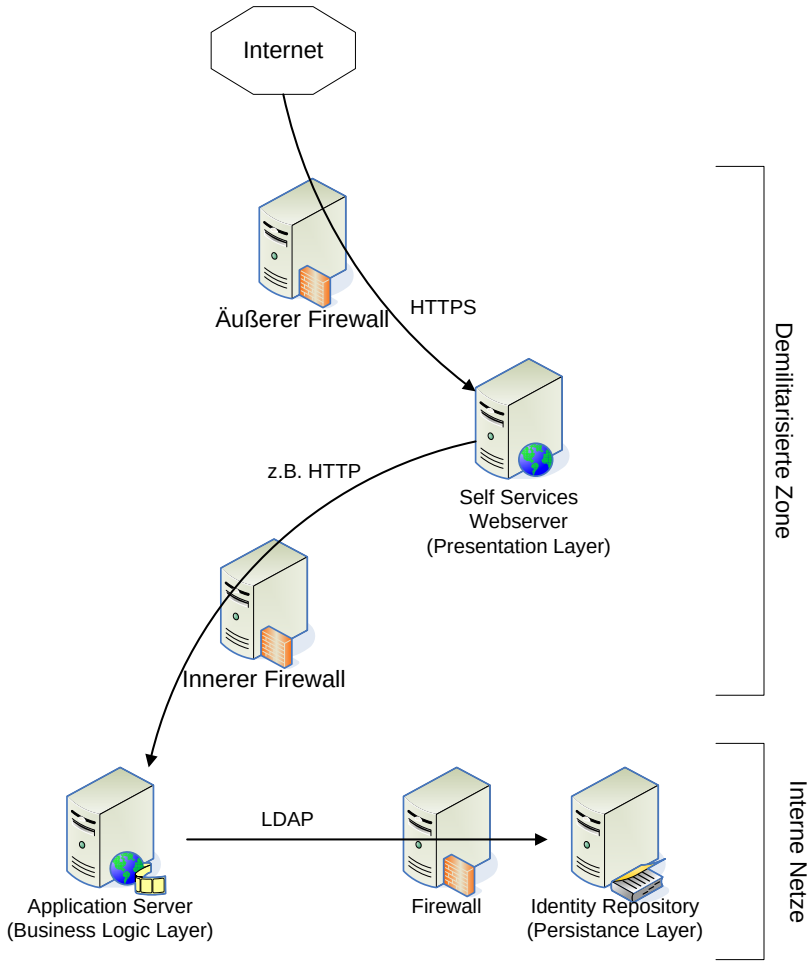


Abbildung 4.11.: Betrieb von Self Services als 3-Tier-Webapplikation in einer demilitarisierten Zone

4.3.7.5. Einbettung in die Sicherheitsinfrastruktur

Für die üblicherweise auf einem dedizierten Server betriebenen Self Services können die in Abschnitt 4.3.1.6 beschriebenen grundlegenden Maßnahmen angewendet werden.

Im Hinblick auf den Einsatz von Firewalls ist zu berücksichtigen, dass die Self Services und andere webbasierte Dienste in der Regel für alle Benutzer erreichbar sein sollen; sie werden deshalb wie in Abbildung 4.11 dargestellt üblicherweise in einer so genannten demilitarisierten Zone positioniert, in der auch andere über das Internet erreichbare Systeme wie Web- und E-Mail-Server betrieben werden. Sofern keine externen Nutzer vorhanden sein sollten, ist stattdessen ein geeignetes internes Servernetz zu verwenden.

Der optional verwendete Applikationsserver kann hingegen in beiden Fällen so abgeschottet werden, dass außer einem Managementzugang nur Verbindungen vom Webserver aus möglich sind; dies gilt analog für die verwendete Datenbasis, die nur entweder vom Webserver oder

vom Applikationsserver aus erreicht werden muss.

4.3.7.6. Hochverfügbarkeit

Die Hochverfügbarkeit der Self Services kann beispielsweise mit dem in Abschnitt 4.3.1.7 beschriebenen HA-Clusteringverfahren realisiert werden. Der Einsatz von Replikaten ist nur in Kombination mit Service Load Balancern sinnvoll, da Benutzer von webbasierten Anwendungen häufig keine Kenntnis über die Adressen von als Ersatzmaschinen dienenden Replikaten haben.

4.3.7.7. Managementschnittstellen

Web- und Applikationsserver stellen je nach Hersteller alle für Konfiguration, Fehlermanagement und Monitoring benötigten Schnittstellen bereit; sie lassen sich somit nahtlos in bestehende IT-Managementinfrastrukturen integrieren.

Der Umfang und die Gestaltung der Self Services muss in der Regel dem im Identity Repository verwendeten Datenmodell angepasst werden; in der Praxis müssen Self Services aufgrund des Mangels an standardisierter, aber ausreichend flexibler Software häufig szenariendediziert von Grund auf neu implementiert werden.

4.3.7.8. Begründung der Verwendung in der Gesamtarchitektur

Durch Self Services können vormals mit Aufwand für mehrere Personen verbundene Verwaltungsaufgaben effektiviert werden; sie sind ein fester Bestandteil moderner I&AM-Systeme. Im Rahmen von FIM werden einige weitere Funktionen ermöglicht, die idealerweise in die bereits vorhandenen Self Service Oberflächen integriert werden; bei der Beschreibung der FIM-Komponenten in Abschnitt 4.4 wird deshalb davon ausgegangen, dass bereits grundlegende Self Services verfügbar sind.

4.3.8. Werkzeuge für Unified Login und Single Sign-On

Ein Unified Login, d. h. die Nutzung aller Dienste z. B. mit derselben Kombination aus Benutzername und Passwort, wird durch die Identitätskorrelation in Kombination mit der dienstübergreifenden Synchronisation der Authentifizierungsinformationen durch die Konnektoren erreicht.

Single Sign-On (SSO) Systeme ermöglichen hingegen die Funktionalität, dass Benutzer ihr Passwort nur noch beispielsweise einmal pro Tag bei einem zentralen Dienst eingeben müssen und alle anderen Services anschließend ohne erneute Authentifizierung nutzen können. Dadurch wird neben dem Benutzungskomfort auch die Sicherheit erhöht, da über potentiell kompromittierte Dienste keine Benutzerpasswörter mehr abgegriffen werden können; zudem können Sicherheitsmechanismen zum Schutz der Authentifizierunginformationen fokussiert auf den SSO-Dienst angewendet werden.

4.3.8.1. Funktionalität

Der SSO-Dienst hat die prinzipielle Aufgabe, den Benutzer auf Basis der in einem Identity Repository hinterlegten Informationen zu authentifizieren und ihm darüber eine für die Nutzung der anderen lokalen Dienste geeignete Bestätigung auszustellen (vgl. [HGMM05]). Die Verwendung des SSO-Dienstes erfolgt entweder über eine webbasierte Benutzerschnittstelle oder ist geeignet ins Clientbetriebssystem integriert. Die weitere Funktionalität unterscheidet sich hinsichtlich des Kommunikationsverhaltens mit den diesen Diensten:

- Im einfachsten Fall reicht es aus, wenn der Benutzer die Bestätigung beim jeweils gewünschten Dienst vorlegt; er kann den Dienst im Anschluss so nutzen, als hätte er sich direkt bei ihm authentifiziert.
- Praktisch wird SSO häufig mit einer Autorisierungsfunktionalität verknüpft; bei der Vorlage der Bestätigung über die Authentifizierung stellt der Dienst die Anfrage an das SSO-System, ob der Benutzer für den gewünschten Dienst autorisiert ist.

Analog zum Single Sign-On soll darüber hinaus ein Single Logout (SLO) ermöglicht werden (vgl. Abschnitt 2.1.2.7 über FIM-SLO); in diesem Fall benötigt das SSO-System eine Schnittstelle zu den Diensten, um das gewünschte Ende der Dienstnutzung kommunizieren zu können.

4.3.8.2. Datenmodell

Zur Authentifizierung von Benutzern orientiert sich das SSO-System an den vom Identity Repository zur Verfügung gestellten Möglichkeiten. Am weitesten verbreitet ist die Durchführung eines LDAP-Binds mit Benutzername und Passwort (vgl. Abschnitt 4.3.1.5); der Einsatz von Clientzertifikaten und biometrischen Verfahren ist möglich, sofern die entsprechenden Daten und Merkmale im Identity Repository hinterlegt sind.

Die dem Benutzer ausgestellte Bestätigung über eine erfolgreiche Authentifizierung verwendet ein Datenformat, das von den ans SSO-System angeschlossenen Diensten unterstützt werden muss. Neben X.509v3-Zertifikaten bzw. Kerberostickets und cookiebasierten Verfahren für Webapplikationen finden inzwischen auch im organisationsinternen Einsatz SAML-Authentifizierungsbestätigungen weitere Verbreitung (vgl. Abschnitt 3.2.1).

Analog zu SAML enthalten die Bestätigungen in der Regel Metainformationen wie die Gültigkeitsdauer und sind durch elektronische Signatur vor unerwünschten Modifikationen geschützt.

4.3.8.3. Kommunikationsschnittstellen und Kommunikationspartner

Mit den in der Funktionsbeschreibung bereits erwähnten Systemen kommuniziert das SSO-System wie folgt (vgl. Abbildung 4.12):

- Das Identity Repository stellt eine Schnittstelle zur Überprüfung der vom Benutzer gelieferten Authentifizierungsinformationen bereit (vgl. Abschnitt 4.3.1.3); bei LDAP-Servern wird entweder das Benutzerpasswort durch einen LDAP-Bind verifiziert oder es

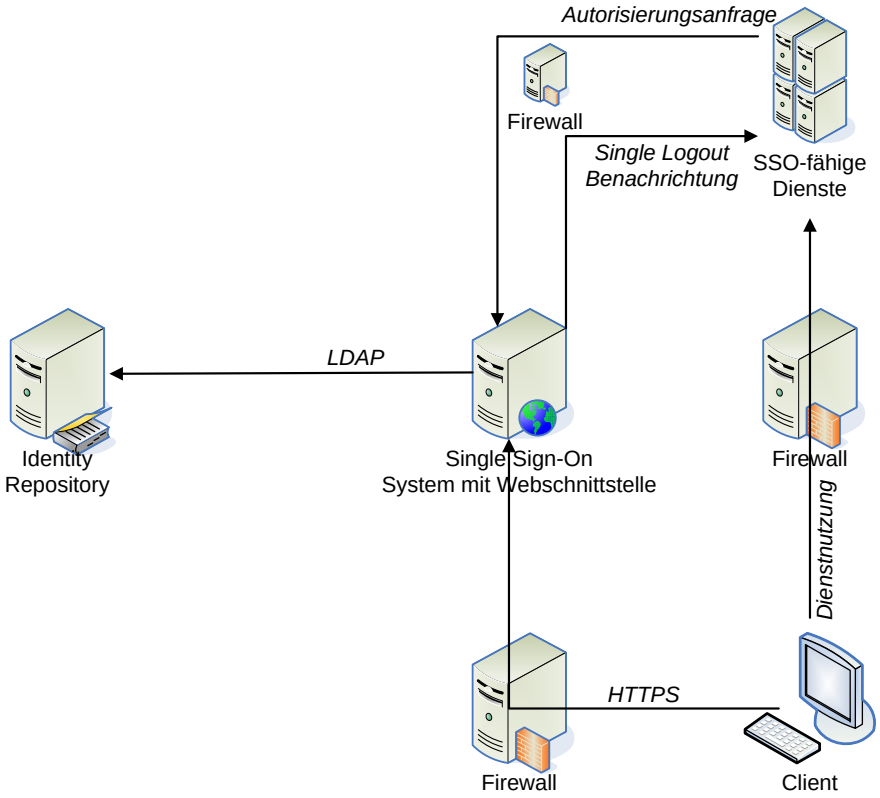


Abbildung 4.12.: Kommunikationsschnittstellen des organisationsinternen SSO-Systems

werden durch eine LDAP-Anfrage beispielsweise die gespeicherten biometrischen Merkmale ausgelesen, um vom SSO-System mit den aktuellen Benutzerdaten verglichen werden zu können.

- Die Kommunikation mit dem Benutzerclient erfolgt, sofern es sich um ein webbasiertes SSO-System handelt, über HTTPS. Für andere SSO-Systeme sind beliebige andere, typischerweise TCP/IP-basierte Protokolle einsetzbar, wobei auf die verschlüsselte Übertragung der Authentifizierungsinformationen geachtet wird. Standardisierte Schnittstellen sind beispielsweise die Generic Security Services API (GSS-API) und der Simple Authentication and Security Layer (SASL).

  Analog zu den FIM Use Cases *IDP first* bzw. *SP first* (siehe Abschnitt 2.1.2.7) kann es insbesondere bei webbasierten SSO-Systemen vorkommen, dass ein Benutzer einen Dienst nutzen möchte, noch bevor er vom SSO-System authentifiziert wurde. In diesem Fall wird der Benutzer vom Dienst an das SSO-System weitergeleitet und diesem ein Parameter übergeben, der spezifiziert, zu welchem Dienst nach Abschluss des Authentifizierungsvorgangs zurückgekehrt werden soll.

- Die Kommunikationsschnittstelle zwischen SSO-System und Diensten ist vom SSO-System abhängig und muss von den Diensten unterstützt werden; dabei wird häufig

die GSS-API-basierte Kommunikation gewählt, da sie relativ einfach in Dienste integriert werden kann und zur Unterstützung kerberosbasierter SSO-Systeme schon früh Verbreitung gefunden hat.

Der Verbindungsaufbau vom SSO-System zu den Diensten zum Zweck des Single Logout wird derzeit noch bei Weitem nicht von allen Systemen unterstützt. Er kann alternativ durch eine regelmäßige Nachfrage der Dienste beim SSO-System, ob die Anmeldeinformationen noch gültig sind, ersetzt werden; diese Variante ist jedoch mit einem entsprechenden Kommunikationsoverhead verbunden.

4.3.8.4. Interne Sicherheitsmechanismen

SSO-Systeme bieten in der Regel einen Schutz vor Brute-Force-Angriffen, indem sie erneute Authentifizierungsversuche nach bereits mehreren fehlgeschlagenen Anmeldungen verzögern, damit Passwörter durch das systematische Ausprobieren aller möglichen Zeichenkombinationen nicht effizient erraten werden können.

Auf das Sperren von Kennungen nach zu vielen Fehlversuchen wird häufig verzichtet, da hiermit ein gezielter Denial-of-Service-Angriff auf individuelle Benutzer durch absichtliche Falscheingaben möglich wäre.

4.3.8.5. Einbettung in die Sicherheitsinfrastruktur

Für das SSO-System können dieselben Sicherheitsmaßnahmen wie für die Self Services verwendet werden, da es sich ebenfalls um einen typischerweise webbasierten Dienst mit direktem Benutzerzugriff handelt (siehe Abschnitt 4.3.7.5).

Der Zugriff auf die Schnittstelle zur Kommunikation mit den Diensten kann über Paketfilterfirewalls auf die bekannten Dienste eingeschränkt werden; zur Überprüfung der elektronischen Signatur von Bestätigungen über erfolgreiche Authentifizierungen wird insbesondere wieder auf die eingesetzte PKI zurückgegriffen, sofern kein einfacheres symmetrisches Verschlüsselungsverfahren zum Einsatz kommt, das jedoch die Konfiguration eines auch von den Diensten genutzten Schlüssels (*shared secret*) erfordern würde, der wiederum aus Sicherheitsgründen periodisch geändert werden sollte.

4.3.8.6. Hochverfügbarkeit

Auch für die Realisierung der Hochverfügbarkeit des SSO-Systems gelten dieselben Aussagen wie für die Self Services (siehe Abschnitt 4.3.7.6).

Die Anforderungen an die Hochverfügbarkeit des SSO-Systems sind noch wesentlich höher als für Privacy Management System, da ihr Ausfall bedeutet, dass die daran angeschlossenen Dienste nur von Personen genutzt werden können, die bereits vor dem Ausfall authentifiziert wurden und in Abhängigkeit vom Autorisierungskonzept bereits mit der Nutzung des Dienstes begonnen haben. Im Unterschied zu Identity Repositories sind von einem Ausfall des SSO-Systems auch diejenigen Dienste betroffen, die von einem Provisioningsystem mit Benutzerdatensätzen gespeist werden.

4.3.8.7. Managementschnittstellen

Analog zu Privacy Management Systemen kommt SSO-Systemen eine besondere Rolle bei der Erkennung von Einbruchsversuchen zu; durch die Zentralisierung der Authentifizierung entfällt die diesbezügliche Korrelation von Protokolldateien der angebundenen Dienste. Für die Konfiguration und Überwachung werden wie von den anderen Komponenten Werkzeuge und Standardschnittstellen bereitgestellt.

4.3.8.8. Begründung der Verwendung in der Gesamtarchitektur

Das organisationsinterne SSO-System ist im Rahmen dieses Konzepts eine technisch zwingende Voraussetzung für das organisationsübergreifende SSO, da die in Abschnitt 4.4.1.1 beschriebene, IDP-seitig eingesetzte Komponente zur Abwicklung von FIM-Authentifizierungsanfragen darauf angewiesen ist.

4.3.9. Unterstützende Komponenten

In diesem Abschnitt werden weitere Komponenten und Funktionseinheiten vorgestellt, die in I&AM-Systemen typischerweise Verwendung finden, aber entweder nicht zum Standardfunktionsumfang gehören oder auch unabhängig von einem I&AM-System eingesetzt werden können. Neben ihrer Unterstützung von I&AM-Systemen sind sie insbesondere auch im FIM-Kontext zu berücksichtigen.

4.3.9.1. Werkzeuge für Identity Management Administratoren

Trotz der erreichbaren Automatisierung verbleibt die Notwendigkeit für manuelle Eingriffe durch Administratoren zumindest zu Kontrollzwecken. Über Werkzeuge für das Management der I&AM-Komponenten hinaus werden deshalb folgende Hilfsmittel eingesetzt:

- Werkzeuge zum direkten Zugriff auf Identity Repositories, beispielsweise graphische Datenbankfrontends oder so genannte LDAP-Editoren: Im Unterschied zu den Self Services bieten sie einen uneingeschränkten Zugriff auf alle gespeicherten Datensätze inklusive der Metadaten.

  Entsprechende Software wird typischerweise in Form von Webapplikationen, die in die Managementwerkzeuge für Identity Repositories integriert sind, vom Hersteller bereitgestellt; es existiert jedoch auch eine Vielzahl entsprechender Desktopapplikationen für die üblichen Arbeitsplatzbetriebssysteme, die aufgrund der derzeit noch beschränkten Gestaltungsmöglichkeiten für Webapplikationen ein effizienteres Arbeiten ermöglichen.

  Da diese Werkzeuge meist nur syntaktische Überprüfungen durchführen, muss bei ihrer Verwendung für Schreibzugriffe stark darauf geachtet werden, dass keine semantischen Fehler oder Inkonsistenzen auftreten; sie werden deshalb nur in Ausnahmesituationen für Schreibzugriffe auf Produktivsysteme eingesetzt.

- Zur Überprüfung der Konsistenz werden darüber hinaus Werkzeuge eingesetzt, die den Datenbestand des Identity Repository mit denen der ans I&AM-System angeschlossenen

Zielsysteme vergleichen; hierdurch werden Datensätze identifiziert, die in einem Zielsystem nicht korrekt angelegt oder gelöscht worden sind, bzw. deren Parametrisierung wie beispielsweise das zugewiesene Speicherplatzlimit nicht übereinstimmt. Neben Fehlern – beispielsweise im Provisioningsystem – können so auch Änderungen erkannt werden, die von lokalen Dienstadministratoren unter Umgehung des I&AM-Systems durchgeführt wurden.

- Zur Unterstützung des Accountings und Billings, aber auch zur Bereitstellung statistischer Informationen, die beispielsweise vom Capacity Management benötigt werden, wird der Benutzerdatenbestand auf entsprechende Metriken wie die Anzahl der Benutzer pro Kunde und Dienst abgebildet. Hierzu werden typischerweise von I&AM-Administratoren implementierte Skripte eingesetzt, die automatisch periodisch ausgeführt werden.
- Für das Backup und die Wiederherstellung von Nutzdaten werden neben systemweiten Sicherungskopien auch Werkzeuge eingesetzt, um einzelne Datensätze selektiv wiederherstellen zu können; diese Funktionalität wird benötigt, um beispielsweise versehentlich gelöschte Datensätze wiederherzustellen, da mit einem Zurücksetzen des Gesamtdatenbestandes auf den Stand des letzten Backups aufgrund der übrigen zwischenzeitlichen Änderungen ein zu großer Datenverlust verbunden wäre.

Darüber hinaus werden zentrale Managementkomponenten – beispielsweise für die Systemstatusüberwachung und Protokolldateiauswertung – so angepasst, dass sie den Administratoren eine auf das I&AM-System und z. B. davon benötigte Netzwerkkomponenten beschränkte Gesamtsicht präsentieren; hierfür wird eine Dokumentation der Abhängigkeiten, die insbesondere im Hinblick auf die beteiligten Netzwerkkomponenten durch Autodiscoverymechanismen unterstützt werden kann, benötigt.

4.3.9.2. Werkzeuge zur Identitätskorrelation

Eine Identitätskorrelation wird überall dort benötigt, wo ein Benutzer in mehr als einer Datenquelle des I&AM-Systems geführt werden könnte. In Szenario 1 (IntegraTUM) liegt die Überlappungsmenge von Studenten- und Mitarbeiterdatensätzen beispielsweise bei rund zehn Prozent.

Konnektoren unterstützen im Standardumfang lediglich die Korrelation auf Basis eines gemeinsamen Schlüsselattributs; da Quellsysteme häufig eigene Schlüsselattribute wie Kunden- oder Personalnummern vergeben, die nicht beeinflusst werden können, muss zusätzliche Programmlogik implementiert werden.

Eine häufig gewählte Korrelationsheuristik ist der Vergleich von Vorname, Nachname und Geburtsdatum je zweier Datensätze aus unterschiedlichen Quellsystemen; da bei einer ausreichend großen Zahl von namensgleichen Benutzern die Gefahr besteht, zwei verschiedene Personen versehentlich für dieselbe eine Person zu halten (vgl. das klassische Geburtstagsparadoxon), können weitere Attribute wie Bestandteile von Anschriften zur Korrelation herangezogen werden.

Während diese Vorgehensweise theoretisch sehr gute Resultate erzielt, wird die praktische Wirksamkeit durch Datenqualitätsdefizite beeinträchtigt; neben den praktisch kaum zu vermeidenden Tippfehlern bei manueller Datenerfassung im Quellsystem führt insbesondere die

nur partielle Verwendung amtlicher Dokumente zu Korrelationsfehlern. Wird eine Person beispielsweise mit ihrem vollständigen Vornamen „Hans-Joachim“ in der Personalverwaltung geführt, registriert sich in einem anderen Quellsystem jedoch mit der Kurzform „Hajo“, so scheitert ein maschineller Zeichenkettenvergleich zwangsweise, selbst wenn Ähnlichkeitsanalysen beispielsweise auf Basis der Levenshtein-Distanz durchgeführt werden.

Die geeignet erscheinenden Such- und Korrelationsfunktionen müssen mindestens in Quellsystemkonnektoren umgesetzt werden. Darüber hinaus bietet sich die Integration in die Quellsysteme selbst an, um bei einer Neueintragung die ggf. schon vorhandenen Daten übernehmen zu können und somit die erfolgreiche Korrelation mit einer Arbeitserleichterung zu verbinden. Eine Korrelation auf Zielsystemseite ist nur notwendig, wenn diese aus mehr als einem I&AM-System gespeist wird oder bei ihrer Integration ins I&AM-System bereits einen eigenen Datenbestand aufweist; im letzteren Fall ist lediglich ein Initialabgleich notwendig, bei dem sich ein manuelles Eingreifen bei nicht automatisch korrelierten Datensätzen anbietet.

4.3.9.3. Werkzeuge für den Service Desk und das Workflowmanagement

Dem Service Desk Personal und damit dem First Level Support müssen geeignete Werkzeuge zur Verfügung gestellt werden, um typische Supportanfragen effizient und ohne Weiterleitung an den Second Level Support bearbeiten zu können.

Dies umfasst insbesondere eine angepasste Version der Self Services, über die beispielsweise Benutzerpasswörter neu gesetzt und Dienstberechtigungen eingesehen werden können. Darüber hinaus muss der Service Desk den Status aller Komponenten des I&AM-Systems und der daran angeschlossenen Dienste einsehen können, um grundlegende Fehlerursachen schnell erkennen zu können.

Durch die Kopplung des eingesetzten Trouble Ticket Systems (TTS) mit dem Identity Repository kann die Erstellung neuer Trouble Tickets effektiviert werden, da beispielsweise Kontaktinformationen nicht immer wieder neu erfasst werden müssen.

Viele TTS bieten ferner Eskalations- und Workflowmanagementmechanismen, die für Genehmigungsprozesse eingesetzt werden können, wenn Benutzer beispielsweise weitere Dienstberechtigungen über den Service Desk oder die Self Services beantragen. Diesbezüglich ist in Anlehnung an ITIL seitens des Service Desks folglich zwischen Problemberichten (Incident Reports) und Änderungsanträgen (Requests for Change, RfC) zu unterscheiden. RfCs werden bei Bedarf an die für den Benutzer und Dienst zuständige Genehmigungsinstanz weitergeleitet und nach erfolgter Genehmigung entweder automatisch umgesetzt oder an den zuständigen Administrator weitergeleitet.

4.4. FIM-Komponenten

Während I&AM-Systeme bei allen an einer Föderation beteiligten Organisationen eingesetzt werden können und sich die Auswahl von I&AM-Komponenten primär an den anzubindenden Quell- und Zielsystemen und den Sicherheits- und Managementprozessen orientiert, variieren die zu implementierenden FIM-Komponenten mit der Rolle der sie einsetzenden Organisation in den Föderationen.

Neben den bei I&AM-Komponenten betrachteten Aspekten **Funktionalität**, **Datenmodell**, **Kommunikationsverhalten**, **Sicherheit** und **Management** spielt bei den nachfolgend erläuterten FIM-Komponenten deshalb auch die Unterstützung der FIM-Rollen eine zentrale Rolle. Die untenstehenden Ausführungen für Identity Provider, die als erstes diskutiert werden, gelten analog für Attribute Authorities und Authorization Provider, da diese eine Teilmenge der Funktionalität von IDPs bieten. Daran anschließend werden SP-seitige und schließlich im Rahmen aller Rollen benötigte Komponenten betrachtet.

In diesem Abschnitt werden neben Komponenten, die von den in Kapitel 3 diskutierten FIM-Ansätzen bereitgestellt werden, auch einige neue, im Rahmen dieser Arbeit konzipierte Komponenten vorgestellt; die detaillierte Spezifikation einiger dieser neuen Komponenten ist Gegenstand von Kapitel 5. Durch diesen starken Eingriff in das Zusammenspiel der FIM-Komponenten kommt auch den Begründungen der **Designentscheidungen** eine wichtige Aufgabe zu.

4.4.1. Identity Provider Software

Die hier beschriebene Komponente ist der IDP-seitige Endpunkt für die FIM-spezifische Kommunikation mit Benutzern und anderen Föderationsteilnehmern. In SAML, den Liberty Alliance Spezifikationen und von Shibboleth wird sie schlicht als Identity Provider bezeichnet; bei WS-Federation entspricht sie der IDP-seitigen Instanziierung eines Secure Token Services. Zur besseren Unterscheidung von der organisatorischen FIM-Rolle IDP wird sie hier als IDP-Software bezeichnet.

4.4.1.1. Funktionalität

Die IDP-Software ist eine Serverkomponente, die folgende Operationen im klassischen Request-Response-Verfahren anbietet:

- **Identifizierung und Authentifizierung von Benutzern**: Anfragen dieses Typs werden von SPs initiiert, bei der *ersten* Anfrage aber ausschließlich mittelbar über Benutzerclients wie Webbrowser gestellt, die in der Regel von einem IDP Discovery Service (siehe Abschnitt 4.4.10) an die IDP-Software weitergeleitet wurden.

  Als Parameter muss der URL eines Dienstes übergeben werden, dem die positive oder negative Authentifizierungsbestätigung übermittelt werden soll. Optional kann das vom Anfragesteller gewünschte Authentifizierungsverfahrens übergeben werden (Anforderung [SEC-Benutzerauthentifizierung]).

  Die IDP-Software überprüft initial, ob der Benutzer IDP-seitig bereits geeignet authentifiziert wurde und der Zeitpunkt der letzten Authentifizierung noch nicht zu lange zurückliegt; übliche **Gültigkeitsintervalle** liegen bei wenigen Minuten bis zu mehreren Stunden. Sofern die Authentifizierung noch nicht erfolgt ist, wird der Benutzer zu diesem Zweck an einen IDP-lokalen Dienst weitergeleitet, typischerweise das SSO-System (siehe Abschnitt 4.3.8). Dabei muss der Benutzer ggf. die Möglichkeit haben, eine seiner Identitäten auszuwählen (Anforderung [FA-Identitätswahl]).

Anhand der Attribute Release Policies wird überprüft, ob dem als Parameter übergebenen Dienst eine Authentifizierungsbestätigung ausgestellt werden darf (siehe Abschnitt 4.4.4, vgl. auch Anforderung [SEC-Benutzerkreis]), die ggf. entsprechend erzeugt und übermittelt wird. Zur Erfüllung der Anforderung [DSA-Unlinkability] kann der in der Authentifizierungsbestätigung enthaltene Benutzeridentifikator durch eine **Nonce**[3] ersetzt werden, die von der IDP-Software auch in nachfolgenden Anfragen desselben SPs im Gültigkeitszeitraum der Authentifizierung verwendet werden muss (vgl. [QUALIN]).

Da die Gültigkeitsdauer der ausgestellten Authentifizierungsbestätigung von der internen Gültigkeitsdauer abweichen kann, können SPs *wiederholte* Anfragen dieses Typs stellen, um die anhaltende Gültigkeit zu überprüfen oder ein anderes Authentifizierungsverfahren zu verlangen, beispielsweise wenn stärker geschützte Funktionen eines Dienstes genutzt werden sollen (Re-Authentifizierung).

Um einen späteren Single Logout zu ermöglichen, muss die IDP-Software eine Liste aller SPs, die Authentifizierungsbestätigungen erhalten haben, vorhalten (siehe unten).

- Ausstellen von **Autorisierungsbestätigungen** sowie allgemeinen **Attributsauskünften**: Anfragen dieser Art setzen voraus, dass der Benutzer bereits authentifiziert wurde und der Benutzeridentifikator neben Informationen über die gewünschten Auskünfte als Parameter übergeben wird. Optional kann der Identifikator des SP übergeben werden, der Empfänger der Antwort auf die Anfrage sein soll, sofern dieser vom Anfragesteller abweicht; dies ermöglicht ein **Push-Verfahren**, bei dem beispielsweise ein IDP-interner Dienst wie ein Webportal, auf dem verschiedene Dienste verlinkt sind, die Anfrage stellt, deren Antwort direkt dem vom Benutzer gewünschten SP zur Verfügung gestellt wird (Anforderung [FA-Pull&Push]).

  Anfragen nach Autorisierungsinformationen werden an ein lokales Privilege Management System (siehe Abschnitt 4.4.2) übergeben. Das Einholen der allgemeinen Attributsauskünfte erfolgt über eine Schnittstelle zu den lokalen Datenbeständen (siehe Abschnitt 4.4.3). In beiden Fällen werden die geltenden Attribute Release Policies berücksichtigt: Bei Autorisierungsinformationen wird die entsprechende Überprüfung von der IDP-Software angestoßen; die Schnittstelle zu den lokalen Datenbeständen muss diese Aufgabe aufgrund der potentiellen Interaktion mit dem Benutzer selbst übernehmen (siehe Abschnitte 4.4.4 und 4.4.3).

  Die einzelnen Ergebnisse werden zu einem Gesamtresultat kombiniert und als Antwort auf die Anfrage zurückgegeben. Für den Fall, dass die Anfrage nicht das einmalige Auslesen eines Benutzerattributs zum Ziel hatte, sondern beispielsweise über den Liberty ID-WSF Subscriptions & Notifications Service auch Mitteilungen über die Änderungen an den Daten gefordert wurden, wird das Tripel (SP, Benutzer, Attribut) in eine Datenbasis geschrieben, die im Rahmen eines von der in Abschnitt 4.4.6 erläuterten Komponente angestoßenen Workflows zum Versenden von Aktualisierungsnachrichten genutzt wird.

  Um die Anforderung [FA-UserOffline] zu erfüllen, können Anfragen dieser Art auch beantwortet werden, während der Benutzer nicht online bzw. authentifiziert ist; in diesem

[3] *Nonce* ist die in der Kryptographie gebräuchliche Abkürzung für „a **N**umber used only **once**“, also eine nur einmal verwendete, typischerweise randomisiert erzeugte Zahl, die hier als Benutzeridentifikator verwendet wird.

Fall existieren Einschränkungen hinsichtlich der möglichen Interaktion mit dem Benutzer (siehe Abschnitt 4.4.5).

Zur Unterstützung der Anforderung [DSA-Selbstbestimmung] muss protokolliert werden, welche personenbezogenen Daten zu welchen Zeitpunkten an welche SPs übermittelt wurden; hierfür wird ebenfalls eine geeignete Datenbasis gepflegt.

- **Senden von Aktualisierungsnachrichten**: Die in Abschnitt 4.4.6 beschriebene Komponente agiert als eventgesteuerter Konnektor zwischen dem Identity Repository und der IDP-Software. Bei jeder gemeldeten Änderung wird anhand der oben erläuterten Datenbasis überprüft, welchen Service Providern die jeweilige Datenänderung mitgeteilt werden soll. Eine entsprechende Aktualisierungsnachricht wird nach dem Überprüfen der aktuellen Attribute Release Policies auf Basis der von der Schnittstelle zu den Föderationsmetadaten gelieferten Informationen über den SP verschickt. Diese Funktionalität ist in den aktuellen FIM-Implementierungen noch nicht vorhanden.

- **Anstoßen des Single Logouts**: Eine Anfrage dieses Typs kann entweder von Benutzerclients direkt oder von SPs gestellt werden; im zweiten Fall wird über die Interaktionskomponente (siehe Abschnitt 4.4.5) optional beim Benutzer nachgefragt, ob er sich wirklich bei allen Diensten abmelden möchte.

  Die IDP-Software informiert alle SPs, die Authentifizierungsbestätigungen erhalten haben, über den Logoutvorgang; sofern sich ein Benutzer bei einzelnen Diensten schon manuell abgemeldet hat, wird diese Information von den entsprechenden SPs ignoriert.

- **Schreibzugriff auf das Benutzerprofil**: Komplementär zum Abruf allgemeiner Attributsauskünfte können SPs Schreibzugriffe auf die beim IDP hinterlegten Benutzerprofile initiieren (Anforderung [FA-Schreibzugriff]). Benutzer und IDP-seitige Administratoren verwenden hingegen z. B. die Self Services, um vergleichbare Operationen durchzuführen (siehe Abschnitt 4.3.7).

  Ebenfalls analog zu allgemeinen Attributsauskünften wird der schreibende Zugriff über die Schnittstelle zu den lokalen Datenbeständen abgewickelt (siehe Abschnitt 4.4.3). Hierzu kann die interaktive Zustimmung des Benutzers erforderlich sein (siehe Abschnitt 4.4.5, vgl. Anforderung [DSA-Schreibzugriff]), wodurch es zu Einschränkungen kommen kann, wenn der Benutzer nicht online ist.

- Einholen der **Zustimmung zu den dienstspezifischen Benutzerrichtlinien**: Sofern der Dienst keine geeignete Möglichkeit hat, den Benutzer selbst interaktiv nach seiner Zustimmung zu den Benutzerrichtlinien zu fragen, können diese an den IDP übermittelt werden (siehe Abschnitt 4.4.5).

Je nach gewähltem FIM-Ansatz können nur Teilmengen der hier beschriebenen Funktionalität bereitgestellt werden; beispielsweise ist der Schreibzugriff mit den meisten FIM-Lösungen noch nicht möglich, wobei davon ausgegangen wird, dass die von der Liberty Alliance und DIX diesbezüglich vorgesehenen Funktionalitäten in die IDP-Software integriert werden können. Entsprechend können sich zukünftig noch andere Erweiterungen ergeben.

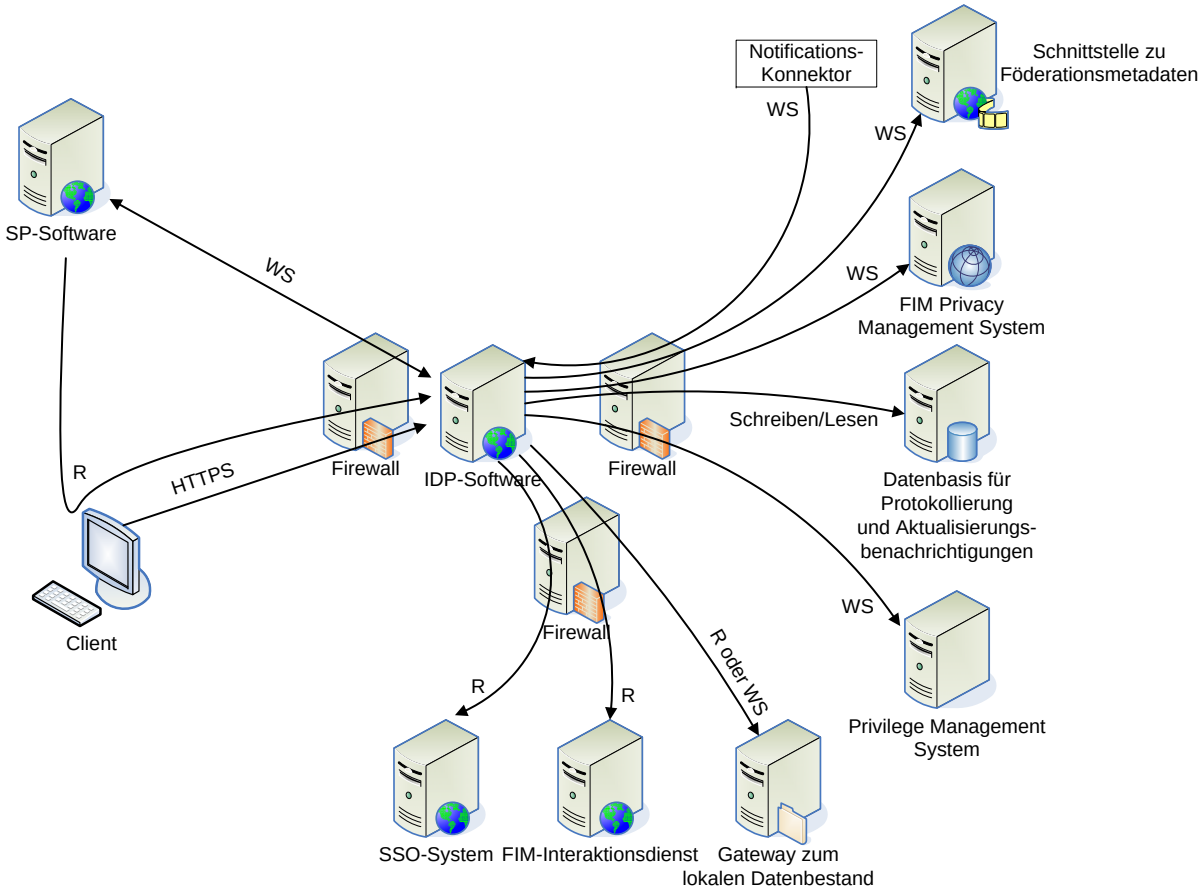


Abbildung 4.13.: Die IDP-Software und ihre direkten Kommunikationspartner

4.4.1.2. Datenmodell

Das von der IDP-Software verwendete Datenmodell hängt vom föderationsweit gewählten FIM-Ansatz und Datenmodell ab. Beispielsweise können Anfragen als SAML Requests eingehen, die mit SAML Assertions beantwortet werden, wobei die möglichen Benutzerattribute durch das LDAP-Schema `inetOrgPerson` vorgegeben werden (vgl. Abschnitte 3.2.1 und 3.8.1).

Die IDP-Software hat diesbezüglich die primäre Aufgabe, die Nutzdaten aus den eingehenden Anfragen zu extrahieren, an die angegebenen anderen Komponenten unverändert weiterzugeben und die von diesen gelieferten Ergebnisse ebenfalls ohne Modifikation der Nutzdaten in das vom FIM-Protokoll benötigte Übertragungsformat zu bringen (siehe auch Abschnitt 4.4.12).

Hieraus ergibt sich die für diese Architektur wichtige Eigenschaft, dass die IDP-Software nicht hinsichtlich des IDP-intern zu verwendenden Datenmodells konfiguriert werden muss, weshalb FIM-Ansätze und -Implementierungen verwendet werden können, von denen die Anforderung [FA-Schema] nicht erfüllt wird.

Ein Sonderfall tritt ein, wenn die Anfrage nach einem Benutzerattribut nicht beantwortet

werden kann, da es im lokalen Datenbestand unbekannt ist; in diesem Fall existieren zu reinen Fehlermeldungen die folgenden beiden Alternativen:

1. Optional kann die Fehlermeldung um einen **Verweis auf eine Attribute Authority** (AA) ergänzt werden, der entsprechend vorkonfiguriert werden muss (vgl. auch Anforderung [FA-Zusatzdaten]). Zur Erfüllung der Anforderung [ORG-Verweisgüte] müsste darüber hinaus die Angabe der Adresse der AA, die typischerweise in Form eines URI vorliegt, um entsprechende Angaben zur Datenqualität erweitert werden; da hierfür noch keine Standards existieren, muss ein föderationsweit einheitliches Format definiert werden.

2. Der Benutzer kann über die in Abschnitt 4.4.5.1 beschriebene Komponente interaktiv zur Eingabe der fehlenden Daten aufgefordert werden.

Obwohl alle FIM-Ansätze eine Klartextübertragung der Daten unterstützen, kann aus Sicherheits- und Datenschutzgründen nur eine verschlüsselte Datenübertragung empfohlen werden; da – wie im nächsten Abschnitt erläutert wird – eine mittelbare Kommunikation über die Benutzerclients erfolgen kann, muss eine so genannte **Ende-zu-Ende-Verschlüsselung** zwischen IDP und SP eingesetzt werden, d. h. dass die vom IDP verschlüsselten Daten nur vom SP entschlüsselt werden können, jedoch nicht von den dazwischenliegenden Übertragungsstationen. Während die Verwendung symmetrischer Verschlüsselungsverfahren auf Basis eines zwischen IDP und SP vereinbarten *shared secrets* prinzipiell möglich wäre, ist der Verwaltungsaufwand in größeren Föderationen hierfür zu groß (vergleiche Föderationsmodell „Pairwise Trust“ in Abschnitt 3.2.2.3 bzgl. SLAs). Deshalb wird bevorzugt asymmetrische Verschlüsselung auf Basis einer föderationsweit anerkannten PKI eingesetzt, wobei die in Abschnitt 4.4.11 erläuterte Komponente den Zugriff auf die relevanten Metadaten, insbesondere den IDP-seitig benötigten Public Key des SP, ermöglicht.

Das Format von Aktualisierungsnachrichten unterscheidet sich typischerweise leicht von den allgemeinen Attributsauskünften; es kann beispielsweise auf die Vorgaben des Liberty ID-WSF Subscriptions & Notifications Services zurückgegriffen werden (siehe [LASUBS]).

4.4.1.3. Kommunikationsschnittstellen und Kommunikationspartner

Die IDP-Software kommuniziert wie folgt mit der Außenwelt und den anderen FIM-Komponenten (vgl. Abbildung 4.13):

- Eingehende Anfragen werden entweder direkt von SPs oder mittelbar über die Benutzerclients gestellt. Hierfür stehen web-service- bzw. webbasierte Schnittstellen zur Verfügung, d. h. es werden die Protokolle SOAP bzw. HTTPS eingesetzt.

- Mit der FIM-Komponente, die als Schnittstelle zu den Föderationsmetadaten fungiert, sowie zum Autorisierungssystem kann über Protokolle kommuniziert werden, die einen entfernten Prozeduraufruf ermöglichen (siehe nachfolgende Abschnitte 4.4.11,4.4.2 und 4.4.4). Es liegt nahe, diese Kommunikation ebenfalls auf Basis von Web Services zu realisieren. Dies trifft auch auf die Kommunikation mit dem Privacy Management System bei Authentifizierungs- und Autorisierungsanfragen zu, da hierbei im Unterschied

zu Attributsauskünften keine Benutzerinteraktion bezüglich Attribute Release Policies erforderlich ist.

- Die für die Authentifizierung genutzte Komponente (siehe Abschnitte 4.3.8) muss als webbasierter Dienst realisiert sein, zu dem der Benutzer umgeleitet wird. Hierzu wird auf die Redirect-Funktionalität des HTTPS-Protokolls zurückgegriffen, wobei die benötigten Parameter z. B. im URL des aufgerufenen Dienstes übergeben werden (siehe Abschnitt 2.1.2.7).
- Die Kommunikation mit dem Gateway zu den lokalen Datenbeständen kann über Web Services oder HTTP-Redirects erfolgen (siehe Abschnitt 4.4.3); die Variante über HTTP-Redirects ermöglicht eine Weiterleitung des Benutzers an die Interaktionskomponente, um beispielsweise Datenfreigaben bei fehlenden Attribute Release Policies dynamisch bei Bedarf zu genehmigen, ist jedoch nur bei der über den Benutzerclient mittelbaren Kommunikation und somit insbesondere nicht im Rahmen der Anforderung [FA-BenutzerOffline] möglich.
- Beim Single Logout und bei Aktualisierungsbenachrichtigungen nimmt die IDP-Software auf Basis der in den Föderationsmetadaten enthaltenen Angaben Kontakt mit den betroffenen SPs auf (vgl. Abschnitt 4.4.7). Hierfür kommen die vom jeweiligen FIM-Ansatz vorgesehenen Benachrichtigungen zum Einsatz, die in der Regel webservice-basiert mittels SOAP übertragen werden.

Wie in Abschnitt 4.4.1.1 beschrieben wurde, können neben externen SPs auch IDP-interne Dienste Anfragen an die IDP-Software stellen; dies dient primär der Umsetzung der Anforderung [FA-Pull&Push], indem in den Anfragen ein vom Anfragesteller abweichender SP angegeben wird, dem die Antwort übermittelt werden soll. Sekundär kann diese Vorgehensweise auch gewählt werden, wenn eine Organisation sowohl IDP als auch SP ist und die eigenen Dienste auch intern über FIM-Protokolle genutzt werden sollen.

4.4.1.4. Interne Sicherheitsmechanismen

Die intern umgesetzten Sicherheitsmaßnahmen hängen stark von der Ausprägung der Föderation ab. In geschlossenen Föderationen werden Anfragen in der Regel nur von anhand der Föderationsmetadaten bekannten SPs akzeptiert; sofern FIM-Techniken außerhalb eines Föderationskontextes eingesetzt werden sollen, beispielsweise wenn Internetprovider als IDPs für ihre Privatkunden fungieren und mit beliebigen Dienstleistern genutzt werden können sollen, muss hingegen lediglich sichergestellt werden, dass die zur Verschlüsselung notwendigen Daten geeignet abgerufen werden können – hierfür existieren beispielsweise Ansätze, Serverzertifikate über DNS abrufen zu können, die im Rahmen dieser Arbeit jedoch nicht vertieft untersucht werden.

Darüber hinaus werden Autorisierungsanfragen, allgemeine Attributsauskünfte und Schreibzugriffe meist nur genau dann ermöglicht, wenn an den entsprechenden SP bereits jemals eine Authentifizierungsbestätigung ausgestellt worden ist; da diese wie in Abschnitt 4.4.1.1 beim ersten Mal nur durch Benutzerclients gestellt werden kann, wird sichergestellt, dass der Benutzer den SP kennt und dieser Daten nicht nur auf Basis der Kenntnis des Benutzeridentifikators abrufen kann.

Die Herausgabe personenbezogener Daten wird zudem durch das in Abschnitt 4.4.4 beschriebene Privacy Management System gesteuert, so dass die IDP-Software keine diesbezüglichen Kontrollen durchführen muss.

In einer FIM-Defizitanalyse zeigen Hommel und Reiser ferner, dass Aspekte der föderationsweiten IT-Security bislang nur unzureichend berücksichtigt werden [HoRe05b]. Für Angriffsszenarien, in denen beispielsweise von kompromittierten Diensten so viele Daten wie möglich ausgelesen werden, existieren noch keine geeigneten Schutzmechanismen (siehe auch Abschnitt 4.7.1). In dieser Arbeit wird gezeigt, dass die geeignete Verwendung von Attribute Release Policies einen grundlegenden Schutz gewährleisten kann (vgl. Abschnitte 4.4.4 und 5.3); sie setzt jedoch entsprechende föderationsweite Konzepte voraus, die im Rahmen parallel entstehender Arbeiten im MNM-Team untersucht werden: Reiser erarbeitet ein Architekturkonzept für föderiertes Sicherheitsmanagement, Boursas stellt Methoden für dynamisches Trust & Reputation Management zur Verfügung und O. v. d. gentschen Felde arbeitet an einem Intrusion-Detection-System-basierten Frühwarnsystem für virtuelle Organisationen.

4.4.1.5. Einbettung in die Sicherheitsinfrastruktur

Da die IDP-Software typischerweise auf einer dedizierten Servermaschine betrieben wird, können die in Abschnitt 4.3.1.6 beschriebenen grundlegenden Sicherheitsmaßnahmen eingesetzt werden.

Eine aus Sicherheitsperspektive anzustrebende möglichst weitreichende Abschottung der IDP-Software, beispielsweise durch Paketfilterfirewalls, ist jedoch nur schwierig zu realisieren. Der direkte Zugriff durch SPs kann auf Basis der Föderationsmetadaten durch eine entsprechende Konvertierung in Firewallkonfigurationsregeln relativ einfach auf bekannte SPs eingeschränkt werden; aufgrund der Möglichkeit zur über die Benutzerclients mittelbaren Kommunikation muss jedoch auch allen vom IDP verwalteten Benutzern Zugriff gewährt werden. In Business-to-Business-Föderationen kann somit eine Einschränkung auf die internen Mitarbeiternetze erfolgen; da IDPs im Allgemeinen jedoch auch über das Internet, insbesondere auch ohne den Einsatz virtueller privater Netze (VPNs) genutzt werden können sollen, ist eine Platzierung des Servers z. B. in einer demilitarisierten Zone neben den anderen öffentlich zugänglichen webbasierten Diensten notwendig.

Zusätzliche Sicherheit können zukünftig **Web-Services-Firewalls** bringen, bei denen es sich um Firewalls der Kategorie Application Level Gateway für das SOAP-Protokoll handelt (vgl. [SOAPFW]). Sie führen eine Inhaltsanalyse der eingehenden Anfragen durch und können somit der Ausnutzung von Implementierungsfehlern in der IDP-Software vorbeugen; allerdings befinden sie sich noch im Forschungsstadium und auch für marktreif werdende Produkte müssen an den jeweils verwendeten FIM-Ansatz angepasste Regelsätze definiert werden. Aufgrund des Umfangs und der Komplexität der FIM-Spezifikationen und der daraus resultierenden FIM-Nachrichten ist die kundenseitige Implementierung entsprechender Regeln aber sehr aufwendig, so dass mit großer Wahrscheinlichkeit auf ihre Bereitstellung durch die Hersteller gewartet werden muss.

4.4.1.6. Hochverfügbarkeit

Prinzipiell können die in Abschnitt 4.3.1.7 erläuterten Hochverfügbarkeitsmechanismen eingesetzt werden. Dabei werden HA-Clusteringverfahren und der Einsatz SLB-basierter Lastverteilung bevorzugt verwendet, da diese die erwünschte Eigenschaft haben, nur einen einzigen nach außen sichtbaren Kommunikationsendpunkt darzustellen, der in die Föderationsmetadaten aufgenommen werden muss.

Es wurde bereits in Kapitel 2 dargelegt, dass der Hochverfügbarkeit der IDP-Software als einziger IDP-seitiger Schnittstelle zur föderationsweiten Kommunikation eine zentrale Bedeutung zukommt (Anforderung [FA-IDP-Verfügbarkeit]); von ihr hängen neben der FIM-basierten interaktiven Nutzung von Diensten durch die vom IDP verwalteten Benutzer auch die bei SPs potentiell asynchron ablaufenden Prozesse ab. Neben der zu garantierenden Datenqualität spielt deshalb die Verfügbarkeit der IDP-Software eine wichtige Rolle bei der Definition von Güteparametern in Föderations-SLAs.

4.4.1.7. Managementschnittstellen

Neben den auch bei den anderen Komponenten üblichen Schnittstellen zur Konfiguration, Protokollierung, Fehleranalyse und Leistungsüberwachung spielt das Accounting bei der IDP-Software eine wichtige Rolle, da die Anzahl sowie Art und Umfang von FIM-basierten Zugriffen gegebenenfalls mit den SPs abgerechnet werden sollen; hierfür ist die Granularität der zu erfassenden Daten festzulegen, die einem Abrechnungssystem zur Verfügung gestellt werden.

4.4.1.8. Begründung des Designs der Komponente

Die hier beschriebene IDP-Software weist die Gemeinsamkeit mit allen bisherigen FIM-Ansätzen auf, dass sie der nach außen einzige technische Kommunikationsendpunkt für die gesamte FIM-Funktionalität ist. Sowohl im Hinblick auf den Verwaltungsaufwand für die Föderationsmetadaten (siehe Abschnitt 4.4.11) als auch bezüglich der IT-Sicherheitsmaßnahmen für von außen erreichbare Serversysteme hat dies offensichtliche Vorteile (vgl. Abschnitt 4.7).

Der wesentliche Unterschied liegt darin, dass die IDP-Software nicht mehr monolithisch aufgebaut ist, sondern zur Bereitstellung der geforderten Funktionalität modular auf dedizierte Systeme zurückgreifen kann, die zum Teil bereits existieren. Hierdurch wird nicht nur die Komplexität reduziert, sondern auch eine wesentlich flexiblere Anpassung an das typischerweise bereits vorhandene I&AM-System ermöglicht; die vollständige Integration von I&AM- und FIM-Komponenten wird dadurch – wie in Abschnitt 4.6 gezeigt wird – deutlich erleichtert.

4.4.2. Autorisierung auf Basis von Privilege Management Systemen

Über die Datenkategorie *Autorisierungsbestätigung* bietet FIM eine sehr effektive Möglichkeit zur Realisierung verteilter Zugriffsverteilungsstrukturen. Seitens der Identity bzw. Authorization Provider werden dabei so genannte Privilege Management Systeme herangezogen, die einen Policy Decision Point implementieren, dessen Entscheidungen SP-seitig ausgewertet und von einem Policy Enforcement Point umgesetzt werden können.

Privilege Management Systeme, zu deren bekannten Vertretern beispielsweise PERMIS [PERMIS] gehört, wurden wissenschaftlich bereits fundiert untersucht und werden hier deshalb nur FIM-spezifisch betrachtet (siehe auch [XPOLA], [GRIDSA] und [WP05] für Grid-Spezifika). Entsprechende Implementierungen existieren u. a. auch für Shibboleth, das Autorisierungsinformationen ansonsten in Form von Attributsauskünften übermittelt (siehe [XCO05] und [SHIBTR]).

4.4.2.1. Funktionalität

Der wesentliche Unterschied zu statisch in Identity Repositories hinterlegten Benutzerberechtigungen liegt bei Privilege Management Systemen in der dynamischen Ermittlung und Auswertung relevanter Policies (vgl. [WEK05] und [BBG05]). Die Funktionalität eines Privilege Management Systems wird durch den folgenden Ablauf beschrieben:

1. Von der IDP-Software wird eine Anfrage gestellt, bei der neben dem Benutzeridentifikator auch der Name des Dienstes bzw. der Dienstfunktionalität sowie der Name des Anfragestellers übergeben werden.
2. Analog zur Vorgehensweise in organisationsinternen Privacy Management Systemen werden alle für diesen Benutzer bzw. Dienst relevanten Policies ermittelt (vgl. Abschnitt 4.3.6).
3. Zur Auswertung der Policies werden in der Regel Informationen über den Benutzer benötigt, die über die Schnittstelle zum lokalen Datenbestand abgerufen werden (siehe Abschnitt 4.4.3).
4. Durch die Auswertung der Policies wird im einfachsten Fall eine Entscheidung getroffen, ob der Benutzer aus Sicht des lokalen Privilege Management Systems den entsprechenden Dienst nutzen darf oder nicht; fortgeschrittene Ansätze liefern darüber hinaus auch explizite Rückmeldungen, falls keine passenden Policies gefunden wurden oder ein interner Verarbeitungsfehler aufgetreten ist.

Die Administration von und Einsichtnahme in Policies kann wie bei organisationsinternen Privacy Management Systemen über PAPs und PIPs erfolgen (vgl. Abschnitt 4.3.6.1). Im Hinblick auf die Attribute Release Policies, die von der IDP-Software geprüft werden, ist dabei zu beachten, dass Benutzer in der Regel keinen Einfluss auf die sie betreffenden Autorisierungsinformationen und deren Herausgabe an Service Provider haben.

4.4.2.2. Datenmodell

Das vom Privilege Management System intern verwendete Format, beispielsweise zur Spezifikation der Policies, wird im Kontext dieser Arbeit nicht näher betrachtet. Zur Integration in die FIM-Transaktionen sind die folgenden Aspekte zu berücksichtigen:

- Der als Parameter übergebene Benutzeridentifikator muss ein Auffinden des entsprechenden Datensatzes durch die Schnittstelle zum lokalen Datenbestand (siehe Ab-

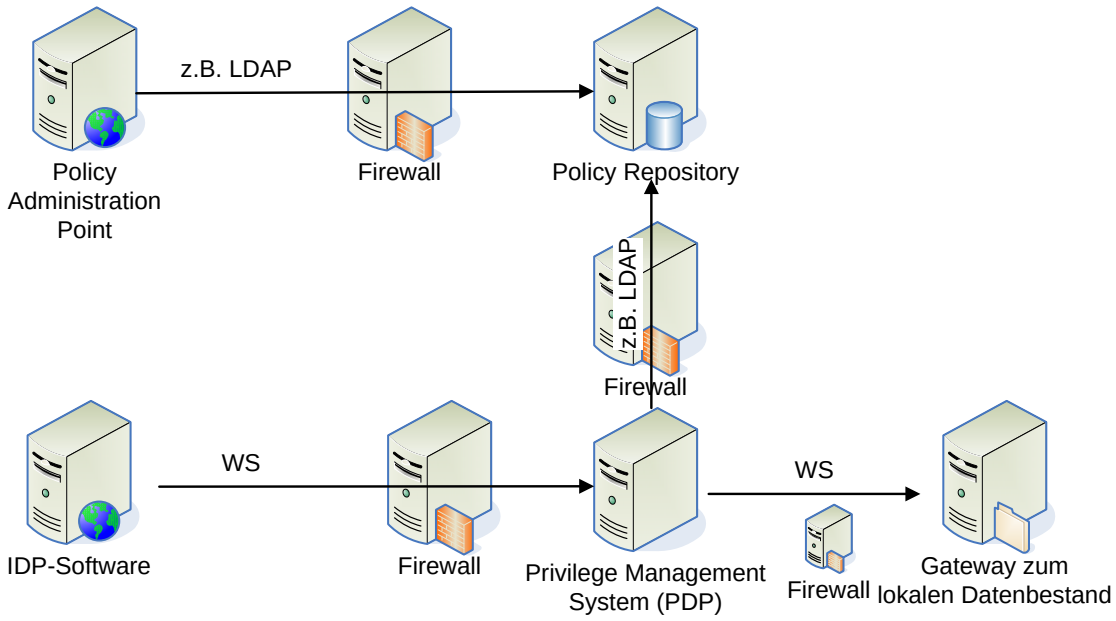


Abbildung 4.14.: Einsatz von Privilege Management Systemen für die Autorisierung

schnitt 4.4.3) ermöglichen; auch wenn die IDP-Software gegenüber dem SP beispielsweise eine Nonce als Pseudonym verwendet (Anforderung [DSA-Unlinkability]), muss hier das IDP-intern verwendete Schlüsselattribut übergeben werden (vgl. Abschnitt 4.4.1.1).

- Der Namensraum für die Dienste bzw. deren geschützte Teilbereiche muss föderationsweit einheitlich definiert werden. SAML und das in Abschnitt 5.3 vorgestellte Konzept für Attribute Release Policies sehen hierfür die Verwendung von URIs vor; insbesondere sollte die Konsistenz mit den SP-Einträgen in den Föderationsmetadaten angestrebt werden.

In der Praxis muss darüber hinaus beachtet werden, dass in SAML-Autorisierungsbestätigungen derzeit nur die so genannten SAML DecisionTypes *Permit*, *Deny* und *Indeterminate* verwendet werden können; das vom Privilege Management System gelieferte Resultat muss von der IDP-Software geeignet darauf abgebildet werden.

4.4.2.3. Kommunikationsschnittstellen und Kommunikationspartner

Die Kommunikation mit der IDP-Software und dem Gateway zu den lokalen Datenbeständen erfolgt wie in Abbildung 4.14 dargestellt über Web Services.

Die Schnittstellen zu Policy Repository, PAP, PIP und ggf. weiteren, eventuell auch organisationsexternen Komponenten des Privilege Management Systems werden von diesem vorgegeben und hier aufgrund der Vielzahl möglicher Ausprägungen ohne direkte Auswirkung auf die FIM-Architektur nicht näher untersucht.

4.4.2.4. Interne Sicherheitsmechanismen

Durch Authentifizierungsmechanismen wie Server- bzw. Clientzertifikate wird z. B. sichergestellt, dass Anfragen an das Privilege Management System nur von dazu berechtigten anderen Systemen, in diesem Fall von der IDP-Software, erfolgen.

Für darüber hinaus vom Privilege Management System vorgesehene Schutzmechanismen gelten dieselben Aussagen wie für organisationsinterne Privacy Management Systeme (siehe Abschnitt 4.3.6.4).

4.4.2.5. Einbettung in die Sicherheitsinfrastruktur

Bezüglich der Integration in die vorhandene Sicherheitsinfrastruktur gelten analog zu den internen Sicherheitsmechanismen die in Abschnitt 4.3.6.5 über Privacy Management Systeme gemachten Aussagen.

Da das Privilege Management System nur intern benötigt wird und auf einen Policy Information Point für Benutzer meist verzichtet wird, kann es z. B. über Paketfilterfirewalls effizient stark abgeschottet werden.

4.4.2.6. Hochverfügbarkeit

Ohne Berücksichtigung spezifischer Ausprägungen von Privilege Management Systemen können prinzipiell dieselben Hochverfügbarkeitsmaßnahmen wie bei der IDP-Software angewendet werden (siehe Abschnitt 4.4.1.6).

Die Notwendigkeit eines hochverfügbaren Privilege Management Systems muss aus der Intensität der Nutzung von Autorisierungsbestätigungen und der Reaktion von Diensten auf die Nichtverfügbarkeit abgeleitet werden. Ein temporärer Ausfall könnte beispielsweise als relativ unkritisch eingestuft werden, wenn ein Dienst bei der Nichtverfügbarkeit einer Autorisierungsbestätigung auf gecachte Informationen zurückgreift, so dass Benutzer den Dienst zumindest verwenden können, wenn sie bei der letzten erfolgreichen Anfrage autorisiert wurden.

4.4.2.7. Managementschnittstellen

Die vom Privilege Management System zur Verfügung gestellten Managementschnittstellen hängen vom konkreten Ansatz und seiner Implementierung ab. Sie sind in der Regel vergleichbar mit den Managementschnittstellen von Privacy Management Systemen (siehe Abschnitt 4.3.6.7).

4.4.2.8. Begründung des Designs der Komponente

Der Fokus aktueller FIM-Systeme liegt klar auf dem organisationsübergreifenden Single Sign-On und dem Austausch von Benutzerprofilen, wohingegen von den Möglichkeiten zur Übertragung von Autorisierungsbestätigungen nur wenig Gebrauch gemacht wird – vielmehr werden häufig Benutzerattribute übertragen, aus denen SP-seitig Berechtigungen abgeleitet werden;

das Konzept der delegierten Autorisierung wird von Privilege Management Systemen deshalb derzeit noch wesentlich konsequenter umgesetzt.

In Szenarien, die bereits vor dem Aufkommen von FIM auf delegierte Autorisierung angewiesen waren, sind Privilege Management Systeme bereits häufig vorzufinden und werden somit vollständig und ohne großen Aufwand integriert, da lediglich ein neuer, FIM-basierter Transportmechanismus für Autorisierungsentscheidungen eingeführt wird.

4.4.3. Gateway zu IDP-lokalen Datenbeständen

Diese in den bisherigen FIM-Ansätzen nicht konkret berücksichtigte Komponente fungiert als Schnittstelle zu den IDP-seitig vorhandenen Datenbeständen, d. h. zu Identity Repositories bzw. Meta-Directories und virtuellen Verzeichnisdiensten.

4.4.3.1. Funktionalität

Die Funktionalität dieser Komponente kann mit einem virtuellen Verzeichnisdienst verglichen werden, der neben den für eingehende Anfragen abweichenden Kommunikationsschnittstellen (siehe Abschnitt 4.4.3.2) folgende FIM-Spezifika aufweist (vgl. Abbildung 4.15):

- Die bidirektionale Konvertierung zwischen den lokal bzw. vom Anfragesteller verwendeten Datenformaten erfolgt nicht über statisch vorgegebene Regeln, sondern auf Basis des in Abschnitt 4.4.12 beschriebenen Konverters, der im Unterschied zu herkömmlichen virtuellen Verzeichnisdiensten mit mehreren verschiedenen Anfrageformaten umgehen kann.
- Aus den auf Attributsanfragen ermittelten Ergebnissen werden diejenigen Elemente entfernt, die auf Grundlage der Attribute Release Policies nicht übertragen werden dürfen; hierfür wird die in Abschnitt 4.4.4 beschriebene Komponente herangezogen.
- Schreibzugriffe unterliegen ebenfalls der in Abschnitt 4.4.4 beschriebenen policybasierten Kontrolle und können optional eine interaktive Zustimmung durch den Benutzer erfordern, die von der in Abschnitt 4.4.5 erläuterten Komponente eingeholt wird.

Lese- und Schreibzugriffe werden dabei im Hinblick auf die mögliche Interaktion mit dem Benutzer wie folgt behandelt:

- Bei Lesezugriffen kann die Interaktion mit dem Benutzer von dieser Komponente angestoßen werden, wenn die ARP-Auswertung ergibt, dass für mindestens ein Attribut eine passende Release Policy fehlt, d. h. keine passende positive oder negative Regel spezifiziert wurde. In der Präsentation des betroffenen Attributs wird das IDP-interne Format verwendet, wie es der Benutzer auch aus den Self Services kennt, d. h. die Interaktion erfolgt noch bevor der Rückgabewert ins Format des Anfragenden konvertiert wird.
- Bei Schreibzugriffen erfolgen zuerst die Konvertierung der Daten ins lokale Format und die Auswertung der Policies, bevor der Benutzer optional interaktiv um seine Zustimmung gebeten wird. Zur Überprüfung der Korrektheit des Eintrags sollten dem Benutzer sowohl die ursprüngliche als auch die konvertierte Darstellung präsentiert werden, sofern diese voneinander abweichen.

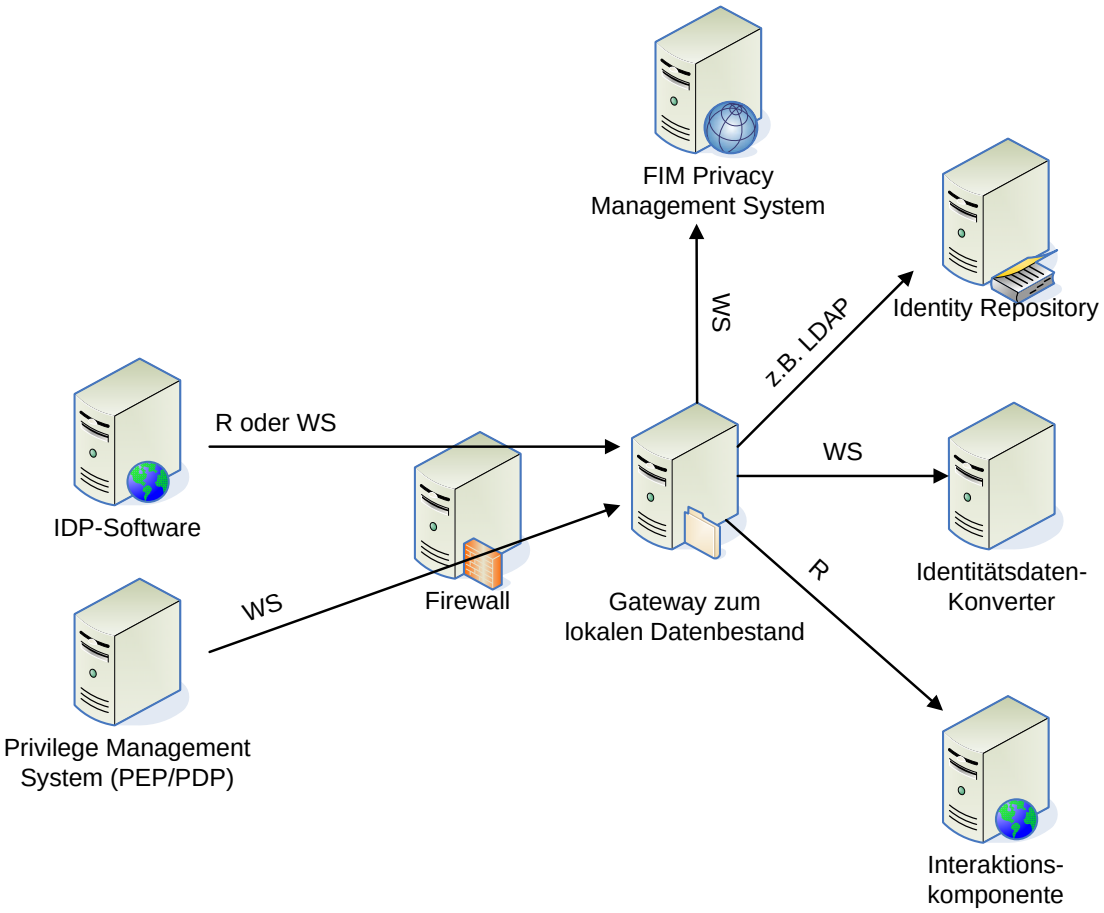


Abbildung 4.15.: Einbettung des Gateways zu den IDP-lokalen Datenbeständen

Darüber hinaus ist zu beachten, dass die vom SP übermittelten und an diese Komponente durchgereichten Anfragen Metainformationen wie den Zweck des Zugriffs enthalten, die in Attribute Release Policies ausgewertet und dem Benutzer bei Interaktionen angezeigt werden können.

Zusammenfassend kombiniert die hier beschriebene Gatewaykomponente die Funktionalität eines virtuellen Verzeichnisdienstes mit den Komponenten für die Datenkonvertierung, die Auswertung der Datenfreigabepolicies und die Interaktion mit dem Benutzer.

4.4.3.2. Workflow, Datenmodell und Kommunikationsverhalten

Da die Hauptaufgabe der Gatewaykomponente im sequentiellen Weiterleiten der Daten an die anderen Komponenten besteht, werden ihr Datenmodell und die Kommunikationsschnittstellen zusammen beschrieben.

Anfragen an die Gatewaykomponente werden über das Web-Service-Protokoll SOAP oder über HTTPS gestellt; HTTPS-Anfragen erfolgen bei über den Benutzerclient mittelbarer

Kommunikation und ermöglichen die webbasierten Interaktionsschritte. Als Parameter werden die Namen bzw. Identifikatoren des anfragenden Dienstes und des betroffenen Benutzers sowie eine Liste der betroffenen Attribute mit dem jeweiligen Anfragezweck übergeben; bei Schreibzugriffen werden darüber hinaus die neuen Werte der entsprechenden Attribute mitgeteilt. Es ist zu berücksichtigen, dass es sich beim anfragenden Dienst nicht nur um den eines externen SPs, sondern auch um eine andere lokale FIM-Komponente wie das Privilege Management System handeln kann, für das in der Regel alle Lesezugriffe erlaubende Attribute Release Policies definiert werden.

Die Liste der Attribute und ggf. ihre neuen Sollwerte werden dem in Abschnitt 4.4.12 beschriebenen Konverter zusammen mit dem Dienstidentifikator übergeben und von diesem im lokalen Datenformat zurückgeliefert. Auch bei lesenden Anfragen können sich hierdurch die Anzahl und Namen der angeforderten Attribute ändern, da später beispielsweise mehrere lokal vorhandene Attribute zu einem einzigen Attribut im fremden Schema kombiniert werden müssen.

Über einen Zugriff auf die lokalen Datenquellen (vgl. Abschnitt 4.3.1.3) wird anschließend z. B. mittels LDAP der komplette Benutzerdatensatz ausgelesen. Dieser wird der in Abschnitt 4.4.4 beschriebenen FIM-Privacy-Komponente zusammen mit der Information über die Art des Zugriffs (z. B. einmalig lesend), dem Dienstidentifikator und der Liste der angeforderten Attribute sowie deren Zweckangaben und ggf. deren vom SP gewünschten Sollwerte übergeben.

Der vollständige Benutzerdatensatz wird benötigt, da zur Auswertung der Attribute Release Policies mehr als nur die vom SP angefragten Attribute benötigt werden können; bei Schreibzugriffen ermöglicht die Übergabe des schon vorhandenen Datensatzes eine kontextsensitive Überprüfung bei Modifikationen auf Basis der alten und neuen Attributwerte.

Die FIM-Privacy-Komponente liefert drei Ergebnislisten zurück (vgl. Abschnitt 4.4.4):

- Attribute, für die der Zugriff auf Basis der Policies erlaubt wurde.
- Attribute, bei denen der Benutzer interaktiv um Genehmigung gefragt werden müsste, da keine passenden Policies vorhanden waren oder die zutreffende Regel explizit zur Interaktion auffordert.
- Attribute, für die der Zugriff auf Basis der Policies verboten wurde.

Sofern notwendig und auf Basis der Benutzerpräsenz möglich, werden die ausstehenden Genehmigungen über die in Abschnitt 4.4.5 beschriebene Komponente interaktiv eingeholt. Wie in Abschnitt 4.4.5.1 beschrieben wird, kann dies insbesondere beim Einsatz von Attributszertifikaten mit überlappenden Attributsmengen notwendig werden (vgl. Anforderung [FA-IDP-Antwortvorschlag]).

Bei Lesezugriffen werden die freigegebenen Daten über den in Abschnitt 4.4.12 beschriebenen Konverter ins Format des Anfragestellers konvertiert und zurückgegeben; bei Schreibzugriffen werden die akzeptierten Attribute in den lokalen Datenbestand eingetragen und dem Anfragesteller eine entsprechende Bestätigung zurückgegeben.

4.4.3.3. Sicherheitsmechanismen und -infrastruktur

Die Gatewaykomponente stellt beispielsweise über Serverzertifikate die Authentizität ihrer Kommunikationspartner sicher; darüber hinaus gelten dieselben Aussagen wie für virtuelle Verzeichnisdienste (siehe Abschnitt 4.3.4). Insbesondere ist denkbar, diese Komponente in die IDP-Software zu integrieren, so dass deren Sicherheitsinfrastruktur genutzt werden kann; diese Vorgehensweise wurde beispielsweise in Shibboleth gewählt – die Funktionalität der aktuellen Implementierung in Shibboleth bleibt jedoch weit hinter den hier genannten Möglichkeiten zurück.

4.4.3.4. Hochverfügbarkeit

Bezüglich der technischen Maßnahmen und der Notwendigkeit gelten für die Verfügbarkeit der Gatewaykomponente dieselben Aussagen wie für die IDP-Software (siehe Abschnitt 4.4.1.6).

4.4.3.5. Managementschnittstellen

Die Gatewaykomponente stellt die üblichen Schnittstellen zur Konfiguration und Überwachung bereit; sie spielt darüber hinaus eine zentrale Rolle beim FIM-Fehlermanagement, da in ihr die meisten IDP-intern für FIM-Transaktionen relevanten Datenflüsse zusammenlaufen.

4.4.3.6. Begründung des Designs der Komponente

Durch die Kapselung des Zugriffs auf den lokalen Datenbestand in einer eigenen Komponente wird eine Entkopplung erreicht, die einen klar definierten Übergang von FIM- zu I&AM-Komponenten ermöglicht und somit das Change Management erleichtert, indem die Zuständigkeiten genau definiert werden (vgl. Abschnitt 4.8); dieser Aspekt wurde bereits als Defizit der bisherigen FIM-Ansätze herausgearbeitet.

Dadurch, dass darüber hinaus die Datenschutzrandbedingungen eingehalten werden müssen und Identitätsdaten im Allgemeinen je nach Organisation in unterschiedlichen Formaten vorliegen, ist das Abrufen lokaler Datenbestände nur scheinbar trivial; diese Gatewaykomponente übernimmt deshalb auch die Orchestrierung der anderen am Datenaustausch beteiligten Komponenten und trägt somit wesentlich zur Strukturierung der IDP-internen FIM-spezifischen Datenflüsse bei.

4.4.4. Komponente für organisationsübergreifendes Privacy Management

Die in diesem Abschnitt beschriebene Komponente hat die Aufgabe, sämtliche Lese- und Schreibzugriffe auf IDP- oder AA-seitig gespeicherte Identitätsdaten aus Datenschutzperspektive zu kontrollieren und ggf. zu verhindern; hierzu kommen die bereits erläuterten Attribute Release Policies zum Einsatz.

Sie unterscheidet sich von den in Abschnitt 4.3.6 beschriebenen organisationsinternen Privacy Management Systemen dadurch, dass sich die verwalteten Policies einerseits auf externe Organisationen und Dienste beziehen, also nicht organisationsinterne *data users*, und andererseits auch die Benutzer einen maßgeblichen Einfluss auf die Policies haben, mit denen die

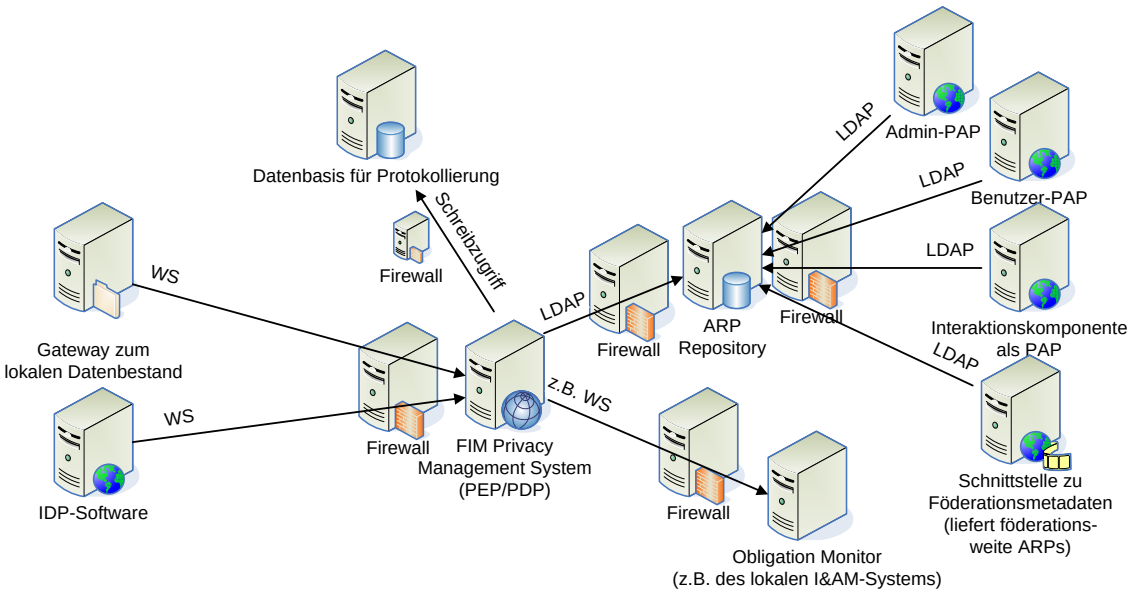


Abbildung 4.16.: Kommunikationsbeziehungen der Komponente für organisationsübergreifendes Privacy Management

Herausgabe der über sie gespeicherten Daten an Dritte gesteuert werden kann. Diese Komponente wird insbesondere auch dann benötigt, wenn kein organisationsinternes PMS eingesetzt wird, da die Anforderung [DSA-ARPs] *essentiell* ist (vgl. Kapitel 2).

Wie in Kapitel 3 gezeigt wurde, wird die Notwendigkeit einer solchen Komponente von SAML, den Liberty Alliance Spezifikationen und WS-Federation erwähnt; bislang wurde sie jedoch lediglich in Shibboleth konkret umgesetzt, ist dort Bestandteil der IDP-Software und mit den in Abschnitt 3.5.3 diskutierten Nachteilen behaftet.

Die interne Funktionsweise dieser von Grund auf neu konzipierten Komponente ist Gegenstand des in Abschnitt 5.3 beschriebenen Werkzeugkonzepts; hier wird deshalb lediglich ihr in Abbildung 4.16 dargestelltes Zusammenspiel mit den anderen Komponenten erläutert.

4.4.4.1. Funktionalität

Die Komponente erhält Eingaben, die Aufschluss über den betroffenen Benutzer, den anfragenden SP bzw. Dienst und die von diesem gewünschten Lese- und Schreiboperationen sowie deren Zwecke geben; darüber hinaus wird der Komponente bei der Anfrage nach allgemeinen Attributsauskünften oder Schreibzugriffen der gesamte Benutzerdatensatz übergeben, so dass keine zusätzlichen Zugriffe auf die lokalen Datenbestände erforderlich sind.

Im ersten Schritt werden alle für die Anfrage relevanten Attribute Release Policies aus dem zur Komponente gehörenden Policy Repository abgerufen; hierzu gehören neben IDP-seitig pauschal vorgegebenen Policies insbesondere diejenigen, die auf die vorliegende Kombination aus Service Provider und Dienst zutreffen, sowie die vom betroffenen Benutzer vorgegebenen.

Lediglich bei von der IDP-Software gestellten Anfragen nach der Freigabe von Autorisierungsinformationen spielen Benutzer-ARPs in der Regel keine Rolle (siehe Abschnitt 4.4.4.7).

Die Ermittlung und der Abruf der Policies sowie die Erstellung des daraus resultierenden Policysets werden in Abschnitt 5.3 näher beschrieben; zu beachten ist dabei insbesondere, dass der Benutzerdatensatz sowie die Werte der ggf. zu schreibenden Attribute in das Policyset eingearbeitet werden. Dem Policy Decision Point stehen somit alle zur Entscheidungsfindung benötigten Daten zur Verfügung.

Die Komponente realisiert ebenfalls einen Policy Enforcement Point, der neben der Aufbereitung der Rückgabewerte insbesondere für das **Erfüllen von Obligationen**, die in den relevanten Policies enthalten sind, zuständig ist. Hierzu gehört beispielsweise das Festhalten von Zugriffen in einem vom Benutzer einsehbaren Protokoll; hierfür kann die auch von der IDP-Software genutzte Datenbasis verwendet werden (siehe auch Abschnitt 4.4.5) und das Verschicken von Benachrichtigungs-E-Mails, beispielsweise immer wenn bestimmte Datenfelder wie die Kreditkartennummer von SPs abgerufen werden.

Für jedes zu überprüfende Attribut wird entschieden, ob der Zugriff stattfinden darf, ob der Benutzer interaktiv um Erlaubnis gefragt werden soll, oder ob der Zugriff nicht durchgeführt werden darf; entsprechende Attributslisten werden an die aufrufende Komponente zurückgegeben.

4.4.4.2. Datenmodell

Wie in Abschnitt 5.3 beschrieben wird, arbeitet die Komponente intern mit XACML Policies, wobei ein föderationsweiter Namensraum für SP- und Dienstidentifikatoren sowie Verwendungszwecke geschaffen werden muss; die übergebenen Parameter werden in Form von XACML `ResourceContent` in das erstellte XACML `PolicySet` eingepflegt. Als Policy Repository kommt wie im Werkzeugkonzept beschrieben ein LDAP-Server zum Einsatz, der ein effizientes Auffinden und Auslesen der für eine Anfrage relevanten Policies ermöglicht.

4.4.4.3. Kommunikationsschnittstellen und Kommunikationspartner

Die Funktionalität dieser Komponente wird vom Gateway zu den lokalen Datenbeständen und der IDP-Software wie in Abschnitt 4.4.3 beschrieben über Web Services, also über das Protokoll SOAP genutzt. Der Zugriff auf das Policy Repository erfolgt wie in Abschnitt 5.3 spezifiziert über LDAP.

Eine Besonderheit stellen Langzeit-Obligationen dar, d. h. die Obligation wird nicht unmittelbar im Anschluss an das Auswerten einer Policy erfüllt, sondern zu einem von dieser spezifizierten späteren Zeitpunkt; ein Beispiel hierfür ist, dass von SPs geschriebene Daten, die länger als ein Jahr nicht benutzt werden, automatisch wieder gelöscht werden sollen. Hierzu wird wie bei organisationsinternen PMS ein Obligation Monitor benötigt (vgl. Abschnitt 4.3.6.1); es ist anzustreben, diesen nicht für FIM separat instanziieren zu müssen, sondern einen bereits vorhandenen Obligation Monitor mitbenutzen zu können. Eine primitive Möglichkeit bestünde in der Eintragung der entsprechenden Auflagen in den im Identity Repository zur Person hinterlegten Metadaten; um direkte Schreibzugriffe zu vermeiden und Formatunabhängigkeit zu erlangen, sollte das PMS jedoch Schnittstellen für das Einspielen von Obligationen bereitstellen.

4.4.4.4. Interne Sicherheitsmechanismen

Die von dieser Komponente zu berücksichtigenden Sicherheitsmaßnahmen sind ähnlich den bei internen PMS eingesetzten (vgl. Abschnitt 4.3.6.4). Neben der Integrität der verarbeiteten Policies ist dabei insbesondere sicherzustellen, dass nur Anfragen von vertrauenswürdigen anderen Komponenten bearbeitet werden, um ein systematisches Ausspähen der ARPs zu verhindern.

4.4.4.5. Einbettung in die Sicherheitsinfrastruktur

Die Integration dieser Komponente in die Sicherheitsinfrastruktur hängt im Wesentlichen davon ab, ob sie als alleinstehender Dienst betrieben oder z. B. wie im Fall von Shibboleth in den Gateway zum lokalen Datenbestand bzw. die IDP-Software integriert wird.

Beim Betrieb des PDPs auf einem dedizierten Server kann dieser z. B. durch den Einsatz von Firewalls stark abgeschottet werden; ebenso gelten auch für die übrigen Komponenten wie das Repository und die PAPs die in Abschnitt 4.3.1.6 beschriebenen Grundsätze.

4.4.4.6. Hochverfügbarkeit

Insbesondere der Gateway zu den lokalen Datenbeständen ist von der Verfügbarkeit dieser Komponente stark abhängig; insofern gelten dieselben Aussagen wie für die IDP-Software (siehe Abschnitt 4.4.1.6).

4.4.4.7. Managementschnittstellen

Für das Management der Komponente selbst spielt neben den üblichen Schnittstellen zur Konfiguration, Protokollierung, Fehleranalyse und Leistungsüberwachung vor allem die Verwaltung der Attribute Release Policies eine zentrale Rolle.

Hierbei ist zwischen der Pflege durch Administratoren, Benutzer und andere FIM-Komponenten zu unterscheiden:

- Für **Administratoren** können mehrere Policy Administration Points (PAPs) vorgesehen werden, da das in Abschnitt 5.3 beschriebene Policykonzept eine beliebige Verteilung erlaubt, um beispielsweise eine **hierarchische Umsetzung** organisationsweiter Vorgaben, die standort-, abteilungs- und dienstspezifisch verfeinert werden, realisieren zu können; alternativ kann ein zentraler PAP angeboten werden. Langfristig sollte eine Integration mit dem PAP des organisationsinternen PMS angestrebt werden, um Datenschutzvorgaben, die aus Geschäftsprozessen abgeleitet werden, möglichst automatisch konsistent für die organisationsinterne und -übergreifende Anwendung zu implementieren.
- Die Verwaltung von **Benutzer-ARPs** stellt im Idealfall eine Erweiterung der Self Services für Benutzer dar (vgl. Abschnitt 4.3.7); dadurch wird auch benutzerseitig ein integriertes Management der Daten und der diese betreffenden Release Policies ermöglicht. Wie bereits in Abschnitt 3.3.1.2 erläutert wurde, stellt das Fehlen intuitiv bedienbarer

PAP-Software für Benutzer-ARPs derzeit ein großes Problem in der Praxis dar; die wenigen derzeit verfügbaren Implementierungen müssen separat betrieben werden, können aber z. B. über Single Sign-On ansatzweise transparent in die Self Services eingebunden werden.

- Die in Abschnitt 4.4.5 beschriebene Komponente zur Interaktion mit dem Benutzer kann dazu verwendet werden, während einer Anfrage, für die noch keine passende ARP definiert wurde, neue ARPs zu erzeugen; sie fungiert somit ebenfalls als PAP, weist jedoch einen sehr beschränkten Funktionsumfang auf.

  Die Komponente, die föderationsweite Metadaten zur Verfügung stellt, spielt darüber hinaus wie in Abschnitt 4.4.11 beschrieben eventuell vorhandene **föderationsweite ARPs** in das Policy Repository ein.

Der Funktionsumfang der Benutzer-ARP-Verwaltung muss an den gewünschten Einfluss der Benutzer angepasst werden, da das in Abschnitt 5.3 beschriebene Konzept nicht vorgibt, ob z. B. Benutzer-ARPs die von IDP-Administratoren vorgegebenen ARPs überschreiben können oder umgekehrt; somit sind beide Varianten bzw. das Melden von Konflikten möglich.

Langfristig sind die beiden folgenden weiteren Aspekte zu berücksichtigen:

- Dieses Konzept sieht vor, dass zukünftig föderationsweite ARPs, die bislang in Service Level Agreements festgehalten und von IDP-Administratoren manuell umgesetzt wurden, einen Bestandteil der Föderationsmetadaten darstellen werden (siehe Abschnitt 4.4.11). Damit besteht insbesondere die Möglichkeit, von einer zentralen Stelle aus kurzfristig die Datenherausgabe an einzelne SPs zu unterbinden, beispielsweise wenn Sicherheitsprobleme bekannt geworden sind (vgl. Abschnitt 4.4.1.4). Dieser Ansatz müsste jedoch vor dem Hintergrund der Gefahr seiner missbräuchlichen, einer Zensur ähnlichen Verwendung näher untersucht werden und wird hier nur prinzipiell in Erwägung gezogen.

- Benutzer verwenden für ihre beruflichen und privaten Aktivitäten im Allgemeinen unterschiedliche Identitäten und IDPs; im Sinne eines integrierten Managements, das insbesondere eine gesamtheitliche informationelle Selbstbestimmung unterstützt, könnte das IDP-übergreifende Management von Benutzer-ARPs beispielsweise in Kombination mit UCIM-Ansätzen angestrebt werden. Diese Fragestellung wird jedoch erst relevant, wenn FIM weiter verbreitet ist und die UCIM-Ansätze ausgereifter sind, da momentan noch kein praktischer Bedarf und keine geeigneten Schnittstellen existieren.

Wie bei organisationsinternen Privacy Management Systemen gilt darüber hinaus, dass die häufige negative Entscheidung durch den PDP auf fehlerhafte Policies oder Einbruchsversuche hinweisen kann; diesbezüglich ist bei aktuellen SP-Implementierungen wie Shibboleth jedoch zu berücksichtigen, dass sie Attribute nicht selektiv abfragen, sondern pauschal das gesamte Benutzerprofil anfordern und davon ausgehen, dass die ARPs entsprechend restriktiv konfiguriert sind.

4.4.4.8. Begründung des Designs der Komponente

Die Notwendigkeit und die Aufgaben dieser Komponente folgen unmittelbar aus der *essentiellen* Anforderung [DSA-ARPs], deren Erfüllung aufgrund der Integration in alle relevanten FIM-Datenflüsse klar ermöglicht wird.

Die Entscheidung für einen policybasierten Ansatz folgt den in Abschnitt 3.5 erläuterten aktuellen Entwicklungen. Die für policybasiertes Management charakteristischen Architekturelemente wie Policy Repository und Policy Decision/Enforcement Points können konzeptionell unverändert übernommen werden; von einem organisationintern bereits vorhandenen Privacy Management System wird zur Vermeidung redundanter Funktionalität direkter Gebrauch gemacht.

4.4.5. IDP-seitige Komponente zur Benutzerinteraktion

Die Interaktion mit den Benutzern spielt bei FIM insbesondere im Hinblick auf datenschutzrechtliche Randbedingungen eine essentielle Rolle (vgl. Anforderung [FA-Interaktion]).

Die hier beschriebene Komponente kapselt die Interaktionsfunktionalität, so dass diese nicht von den anderen FIM-Komponenten implementiert werden muss; während auf die graphische Gestaltung von Benutzeroberflächen in dieser Arbeit nicht näher eingegangen wird, darf nicht übersehen werden, dass der Aspekt Usability nicht nur aufgrund der für viele Benutzer neuen FIM-Funktionalität, sondern auch aufgrund der immer populärer werdenden Nutzung von Diensten mit mobilen Endgeräten nicht trivial umzusetzen ist.

4.4.5.1. Funktionalität

Die FIM-Benutzerinteraktion ist ein webbasierter Dienst, der dem Benutzer die von der aufrufenden Komponente übergebenen Daten zusammen mit passenden Entscheidungsmöglichkeiten anzeigt und die resultierenden Benutzereingaben zurückliefert. Sie kommt in den folgenden Fällen zum Einsatz (vgl. Abbildung 4.17):

- **Bestätigung eines Single-Logout-Vorgangs** (vgl. Abschnitt 4.4.1.1): Dieser Schritt ist optional und kommt im Allgemeinen nicht zum Einsatz, wenn der SLO-Vorgang vom Benutzer selbst direkt beim IDP angestoßen wurde; er dient als Sicherheitsmaßnahme, falls der SLO von einem SP gegen den Willen des Benutzers angestoßen wird. Es handelt sich um eine einfache Ja/Nein-Entscheidung.
- **Zustimmung zu Lese- und Schreibzugriffen** (vgl. Abschnitt 4.4.3): Zu lesende oder zu schreibende Attribute, für die keine Attribute Release Policies definiert wurden, oder für die diese explizit zurückmelden, dass eine interaktive Zustimmung erforderlich ist, werden dem Benutzer mit den jeweiligen Werten angezeigt. Er muss dann jedes Attribut markieren, für das der gewünschte Zugriff für den vom SP angegebenen Zweck erfolgen darf. Dabei sollte die Möglichkeit bestehen, die getroffene Entscheidung in Form einer neuen Attribute Release Policy festzuhalten, um zukünftige identische Nachfragen zu vermeiden.

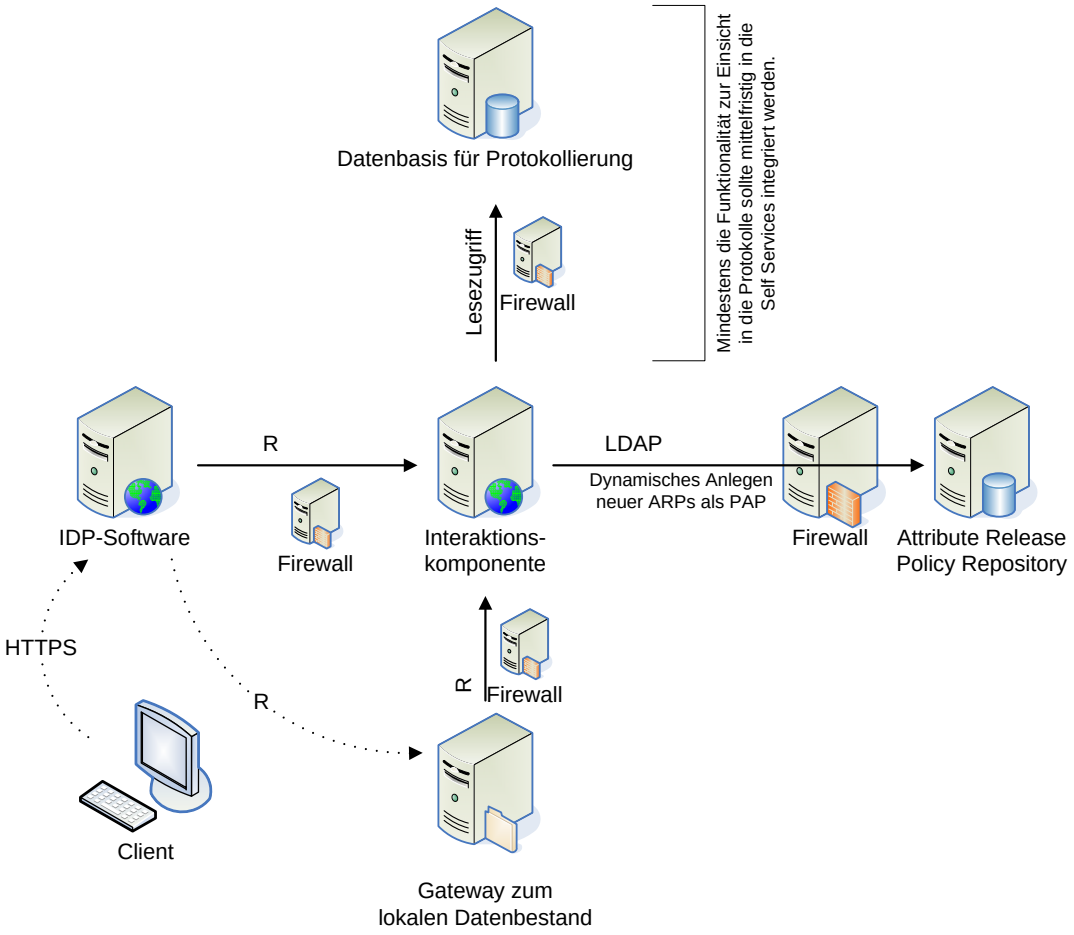


Abbildung 4.17.: Eingliederung der Komponente zur IDP-seitigen Benutzerinteraktion

Ein Sonderfall liegt vor, wenn Attributszertifikate eingesetzt werden, die überlappende Mengen von Benutzerattributen enthalten; der Benutzer muss dann analog zu UCIM-Systemen bei der **Zusammenstellung einer Antwort** möglichst minimalen Umfangs unterstützt werden (vgl. Anforderungen [FA-IDP-Antwortvorschlag] und [DSA-Attributszertifikate] sowie die Beschreibung der Abläufe in Szenario 2).

- **Eingabe fehlender Daten** (vgl. Abschnitt 4.4.1.1): Sofern eine Anfrage eines SPs nicht beantwortet werden kann, da für das entsprechende Attribut lokal kein Wert gespeichert und kein Verweis auf eine passende Attribute Authority konfiguriert wurde, kann der Benutzer optional zur Eingabe der entsprechenden Werte aufgefordert werden. Im Hinblick auf die Anforderung [FA-Zusatzdaten] bleibt diesbezüglich zukünftig zu untersuchen, inwiefern die so eingegebenen Daten auch IDP-seitig dauerhaft gespeichert werden können, da das Schema des lokalen Identity Repository ggf. dynamisch erweitert werden müsste; wie auch bei den nachfolgenden Punkten erwähnt wird, bietet sich deshalb mittelfristig die Integration dieser Komponente in die Self Services an.

- **Einsehen von Protokollen** (vgl. Abschnitte 4.4.1.1 und 4.4.4): Zur Unterstützung der informationellen Selbstbestimmung werden von der IDP-Software Anfragen von SPs mitprotokolliert; über Obligationen in ARPs können darüber hinaus benutzerspezifische Protokolleinträge generiert werden. Da nicht vorausgesetzt werden kann, dass diese Daten im Rahmen der Self Services oder der graphischen Oberfläche für das Benutzer-ARP-Management abgerufen werden können, wird eine entsprechende Funktionalität von der Interaktionskomponente bereitgestellt; wie beim Benutzer-ARP-Management ist jedoch die mittelfristige **Integration in die Self Services** anzustreben.
- **Zustimmung zu Benutzerrichtlinien** (vgl. Abschnitt 4.4.1.1): Die von einem SP übermittelten Benutzerrichtlinien werden dem Benutzer zur Zustimmung vorgelegt; die Dienstnutzung ist nicht möglich, wenn er sie ablehnt (vgl. Anforderung [DSA-Zustimmung]).

Eine grundsätzliche und offensichtliche Voraussetzung für die Interaktion ist die Verfügbarkeit des Benutzers; sie wird im Rahmen dieser Arbeit als erfüllt angesehen, wenn der Benutzer ein Gerät verwendet, mit dem er die hier beschriebene Komponente benutzen kann. Diskussionen über den Liberty Interaction Service haben die Möglichkeit aufgezeigt, Anfragen an den Benutzer beispielsweise auch per SMS-Textnachricht an dessen Mobiltelefon zu schicken und Antworten auf demselben Weg entgegen zu nehmen. Da dieses Konzept nicht in die Liberty-Spezifikationen eingeflossen ist und mit Zeitverzögerungen verbunden sein kann, die bei der heute üblichen Parametrisierung von Web-Service-Protokollen zur Überschreitung von Zeitlimits führen, wird es an dieser Stelle nicht berücksichtigt.

4.4.5.2. Datenmodell und Kommunikationsschnittstellen

Die Kommunikation mit dieser Komponente erfolgt verschlüsselt über HTTPS, da häufig sensible Daten angezeigt werden sollen; die Kodierung der dem Benutzer anzuzeigenden Daten und Formulare erfolgt nach den Vorgaben des Liberty ID-WSF Interaction Services [LAISS], dessen Syntax Analogien zu HTML-Formularen aufweist, wie das folgende Beispiel zeigt:

```
<InteractionRequest xmlns="urn:liberty:is:2006-08">
  <Inquiry title="Single Logout Nachfrage">
    <Help moreLink="http://idp.example.com/hilfe/logout">
      Von http://sp.example.com/ wurde ein Abmeldeversuch mitgeteilt.
    </Help>
    <Select name="slo_choice">
      <Label>Wollen Sie sich wirklich von allen gerade benutzten Diensten abmelden?</Label>
      <Value>Nein</Value> <!-- Dies ist die Voreinstellung -->
      <Item label="Nein" value="Nein"/>
      <Item label="Ja" value="Ja"/>
    </Select>
  </Inquiry>
</InteractionRequest>
```

Die Interaktionskomponente muss daraus eine für das Zielsystem geeignete Darstellungsform generieren, in der Regel HTML.

Da die Kommunikation mit der Komponente mittelbar über den Benutzerclient erfolgt, muss ihr als Parameter die Zieladresse für die Rückgabewerte übergeben werden; sowohl beim Aufruf als auch bei der Rückgabe werden entsprechend HTTPS-Redirects eingesetzt.

Für das dynamische Anlegen neuer Attribute Release Policies fungiert diese Komponente als Policy Administration Point; um einen direkten Schreibzugriff auf das Policy Repository zu

vermeiden, kann sie eine geeignete Schnittstelle eines anderen PAP verwenden. Wie in Abschnitt 4.4.4.7 beschrieben wurde, ist hierfür eine entsprechende Erweiterung der Self Services anzustreben.

4.4.5.3. Interne Sicherheitsmechanismen

Da die Kommunikation mittelbar über den Benutzerclient erfolgt, muss über Verschlüsselung und elektronische Signatur der Anfragen und Antworten sichergestellt werden, dass Daten nur mit einer vertrauenswürdigen anderen FIM-Komponente ausgetauscht werden und vom Benutzer nicht eingesehen oder modifiziert werden können.

4.4.5.4. Sicherheitsinfrastruktur, Hochverfügbarkeit und Managementschnittstellen

Aufgrund der Analogien hinsichtlich der Funktionalität und des Kommunikationsverhaltens gelten bezüglich der Integration in die Sicherheitsinfrastruktur, der Hochverfügbarkeit und der Managementschnittstellen dieselben Aussagen wie für die Self Services (siehe Abschnitte 4.3.7.5 bis 4.3.7.7).

Ein Ausfall dieser Komponente führt zur IDP-seitig reduzierten Funktionalität, die auch zur Verfügung steht, wenn der Benutzer offline ist – mit der Ausnahme, dass die Authentifizierung, die über das SSO-System abgewickelt wird, noch möglich ist. Es kommt somit insbesondere zu Einschränkungen bei den allgemeinen Attributsauskünften, für die keine passenden ARPs definiert wurden.

4.4.5.5. Begründung des Designs der Komponente

Die Kapselung der Abwicklung sämtlicher Benutzerinteraktionen über eine dedizierte Komponente erfolgt einerseits im Hinblick auf die Anforderung [FA-UserOffline], die eine möglichst einfache Fallunterscheidung zwischen der Präsenz bzw. Absenz des Benutzers bedingt.

Andererseits handelt es sich bei der notwendigen Benutzerinteraktion um kein FIM-Spezifikum, so dass der Schwerpunkt bei der Realisierung primär auf der Unterstützung verschiedenster clientseitiger Endgeräte sowie der Bedienung unter Usabilityaspekten liegt. Auch im Hinblick auf die sich in diesem Sektor im ständigen Fluss befindlichen technischen Möglichkeiten und Anforderungen an die nahezu periodische Überarbeitung der graphischen Gestaltung von Benutzeroberflächen bietet sich eine Entkopplung von den übrigen Komponenten an.

4.4.6. Notifications-Konnektor zur Propagation von Datenänderungen an Service Provider

Sofern der gewählte FIM-Ansatz die Möglichkeit bietet, dass SPs die Daten nicht nur auf Anfrage auslesen, sondern auch über Änderungen informiert werden können (vgl. Liberty ID-WSF Subscriptions & Notifications Service [LASUBS]), muss eine entsprechende weitere Komponente IDP- bzw. AA-seitig eingesetzt werden.

Sie entspricht einem Spezialfall der in Abschnitt 4.3.2 beschriebenen Konnektoren, bei dem das Identity Repository als Quellsystem fungiert und relevante Änderungen an die IDP-Software übermittelt werden; diese leitet die modifizierten Daten wie in Abschnitt 4.4.1.1 skizziert unter Berücksichtigung der aktuellen Attribute Release Policies und Föderationsmetadaten an die betroffenen Service Provider weiter. Die interne Funktionsweise dieses Konnektors und die von ihm angestoßenen Datenflüsse werden in Abschnitt 5.5 detailliert spezifiziert.

4.4.7. Service Provider Software

Die SP-Software stellt das Pendant zur IDP-Software dar; analog dazu erfolgte in den FIM-Standards bislang keine explizite Namensgebung für diese Komponente.

Zum Verständnis des hier vorgelegten Konzepts muss berücksichtigt werden, dass sämtliche bisherigen FIM-Ansätze eine direkte Verknüpfung zwischen der SP-Software und einem vom SP angebotenen Dienst vorgesehen haben, woraus sich die bereits erörterten Probleme ergeben, dass die Dienste FIM-fähig sein müssen und SP-seitig vorhandene I&AM-Systeme umgangen werden.

In dieser Arbeit wird die SP-Software einerseits als SP-seitiger FIM-Kommunikationsendpunkt betrachtet, aus dem sich die Außendarstellung ergibt, und fungiert andererseits sowohl als Datenquelle für das SP-seitige I&AM-System als auch als Schnittstelle zur vollständigen FIM-Funktionalität für FIM-fähige Dienste. Dies entspricht einer Erweiterung der bisherigen Konzepte um die Berücksichtigung SP-seitiger I&AM-Systeme, verzichtet aber bewusst auf eine vollständige Entkopplung von den Diensten, da eine durchgängige Nutzung von Funktionen wie Single Sign-On und Single Logout ansonsten beim aktuellen Stand der Technik nicht möglich wäre. Die langfristige Vision, dass die SP-Software nahtlos in das Identity Repository und das interne SSO-System des SP integriert wird und Anfragen nach lokal nicht verfügbaren Daten mittels FIM transparent an IDPs und AAs stellt, gibt somit zwar Ziele und Randbedingungen vor, wäre derzeit aber eine unrealistische Forderung, da die hierfür eingesetzten Protokolle wie LDAP beispielsweise den Zweck eines Datenabrufs nicht transportieren können.

4.4.7.1. Funktionalität

Die SP-Software ist ein Serverdienst, der wie die IDP-Software Anfragen in einem Request-Response-Verfahren entgegennimmt, die sich in die folgenden Kategorien einteilen lassen:

- Anfragen von SP-lokalen Diensten:
  - **Identifizierung und Authentifizierung eines Benutzers**: Diese Anfrage trifft im SP-First Use Case ein (siehe Abschnitt 2.1.2.7) – ein Dienst wurde aufgerufen, ohne dass sich der Benutzer vorher bei seinem IDP authentifiziert hat; der Dienst wendet sich an die SP-Software. Die Bearbeitung dieser Art von Anfragen wird von der in Abschnitt 4.4.10 beschriebenen IDP Discovery Komponente abgewickelt, die SP-lokal oder föderationsweit zur Verfügung stehen kann.

  - **Einholen von (Re-)Authentifizierungs- und Autorisierungsbestätigungen sowie allgemeinen Attributsauskünften**: In diesen Fällen erfolgt die Abwicklung über den bereits ermittelten IDP des Benutzers bzw. eine Attribute Authority oder einen Authorization Provider. Zu verwendende AAs und APs müssen entweder SP-seitig vorkonfiguriert sein oder werden als Verweise in Fehlermeldungen vom IDP zurückgeliefert, wenn dieser die gewünschten Informationen nicht zur Verfügung stellen kann (vgl. Abschnitt 4.4.1.1).
  - **Schreiben von Daten ins IDP-seitige Benutzerprofil**: Aus Sicht der SP-Software handelt es sich hierbei um die inverse Operation zu allgemeinen Attributsauskünften. Sofern der eingesetzte FIM-Ansatz keine Schreibzugriffe unterstützt, kann die SP-Software die Schreiboperationen auf eine lokale Datenbasis ausführen, die beim Einholen allgemeiner Attributsauskünfte berücksichtigt werden muss; dadurch kann eine Unabhängigkeit von tatsächlichen technischen Möglichkeiten geschaffen werden, die hier jedoch nicht weiter vertieft wird, da davon auszugehen ist, dass viele Dienste die Möglichkeit zum Schreibzugriff erst nutzen werden, wenn sie von den FIM-Protokollen bereits unterstützt wird.
  - **Übermitteln der Benutzerrichtlinien**: Die Nutzungsbedingungen eines Dienstes sollen dem IDP übergeben werden, damit dieser sie dem Benutzer zur interaktiven Zustimmung vorlegt; die IDP-Software bietet eine entsprechende Schnittstelle (siehe Abschnitt 4.4.1.1).
  - **Anstoßen des Single Logouts**: Interaktiv genutzte Dienste, die auf den Einsatz im FIM-Umfeld vorbereitet sind, bieten in der Regel neben einem lokalen Logout auch den Single Logout für alle parallel genutzten Dienste an; im letzteren Fall wird eine entsprechende SLO-Nachricht an den für den Benutzer zuständigen IDP geschickt (vgl. Abschnitt 4.4.1.1).

- Von IDPs initiierte Operationen:

  - Im Rahmen des IDP-First Use Cases (siehe Abschnitt 2.1.2.7) werden Daten vom IDP an den SP in einem Pushverfahren ausgeliefert (siehe Nutzung des SP-/Dienstidentifikators in Abschnitt 4.4.1.1); die Bereitstellung der Daten ist implizit mit dem Wunsch nach interaktiver Dienstnutzung verbunden.
  - Sofern der gewählte FIM-Ansatz die Anforderung [FA-Updates] erfüllt, können darüber hinaus unabhängig von einer aktuellen Dienstnutzung Informationen über veränderte Benutzerattribute eingehen; im Unterschied zum interaktiven Fall trifft dies nicht nur auf IDPs, sondern auch auf AAs zu.

Beim Aufruf der jeweiligen Operation sind dabei diejenigen Parameter zu übergeben, die bereits bei der IDP-Software beschrieben wurden. Im Unterschied zur IDP-Software muss die SP-Software jedoch neben der reinen Datenformatkonvertierung auch eine Interpretation der Nutzdaten vornehmen: Die Ergebnisse von Attributsauskünften sind nicht nur an den Dienst weiterzuleiten, sondern über die in Abschnitt 4.4.9 beschriebene Komponente auch ins lokale I&AM-System einzutragen.

Bevor entgegengenommene Daten an das lokale I&AM-System oder den entsprechenden Dienst weitergegeben werden, wird ihre Eignung von der in Abschnitt 4.4.8 beschriebenen Komponente auf Basis der so genannten Attribute Acceptance Policies überprüft; sie liefert Listen der akzeptierten, zurückgewiesenen und noch einzuholenden Attribute zurück.

4.4.7.2. Datenmodell und Kommunikationsschnittstellen

Im Hinblick auf das bei der Kommunikation mit den anderen Föderationsteilnehmern eingesetzte Datenmodell gelten zur IDP-Software analoge Aussagen; beispielsweise können SAML Assertions und ein föderationsweit vereinbartes Benutzerdatenmodell verwendet werden.

Zur bidirektionalen Konvertierung der lokalen Datenbestände in das zur Übertragung verwendete Datenformat wird wie auch IDP-seitig die in Abschnitt 4.4.12 beschriebene Komponente eingesetzt; ebenso werden für die elektronische Signatur und Verschlüsselung sowie deren inverse Operationen die föderationsweiten Metadaten benötigt (siehe Abschnitt 4.4.11).

Da die SP-Software in dieser Form in den derzeitigen FIM-Ansätzen nicht vorgesehen ist, existieren noch keine Vorgaben hinsichtlich der Kommunikation zwischen Diensten und SP-Software. Um eine möglichst weitreichende Kompatibilität zu erreichen, wird deshalb die folgende Vorgehensweise empfohlen:

- Es muss mindestens die vom gewählten FIM-Ansatz vorgesehene Schnittstelle unterstützt werden, so dass beispielsweise SAML-fähige Dienste über SAML Requests mit der SP-Software kommunizieren können. Voraussetzung für die nahtlose Integration ist dann lediglich, dass diese FIM-fähigen Dienste nicht direkt mit den anderen Föderationsteilnehmern kommunizieren, sondern alle Transaktionen über die SP-Software abwickeln.
- Darüber hinaus kann optional eine simplere Schnittstelle angeboten werden, auf deren Basis die Dienste einfacher FIM-fähig gestaltet werden können; beispielsweise können über Web Services bzw. webbasierte Anwendungen entfernte Funktionsaufrufe mit minimalen Signaturen realisiert werden, wodurch die Verarbeitung z. B. komplexer SAML Nachrichten im Zielsystem entfällt.

Dienste, die nicht FIM-fähig sind, kommunizieren nicht direkt mit der SP-Software; die Benutzerdaten fließen in diesem Fall über das I&AM-System des SPs. Hieraus ergibt sich der eingangs erläuterte langfristige Wunsch, dass die SP-Software als eine Art virtueller Verzeichnisdienst realisiert wird, der Daten bei Bedarf von externen Datenquellen abruft; da in den hierbei eingesetzten LDAP-Aufrufen jedoch die für die FIM-Kommunikation benötigten Parameter nicht mitgeliefert werden und keine Interaktion mit dem Benutzer möglich ist, könnte diese Variante derzeit nicht ohne massive Eingriffe realisiert werden, deren Umsetzung wiederum einen inakzeptabel hohen Aufwand bedeuten würde.

Zur Kommunikation werden entsprechend die folgenden Protokolle eingesetzt (vgl. Abbildung 4.18):

- Anfragen im Rahmen der IDP- bzw. SP-First Use Cases erfordern eine Benutzerinteraktion; mit den IDPs bzw. den Diensten muss deshalb über HTTPS auf Basis von Redirects über den Benutzerclient mittelbar kommuniziert werden. Hierzu gehören ebenfalls die Weiterleitung des Benutzers an den in Abschnitt 4.4.10 beschriebenen IDP Discovery Service sowie das Anstoßen des Single Logouts.
- Weitere Anfragen während der Dienstnutzung können direkt über Web Services oder ebenfalls mittelbar über den Benutzerclient auf Basis von HTTPS abgewickelt werden.

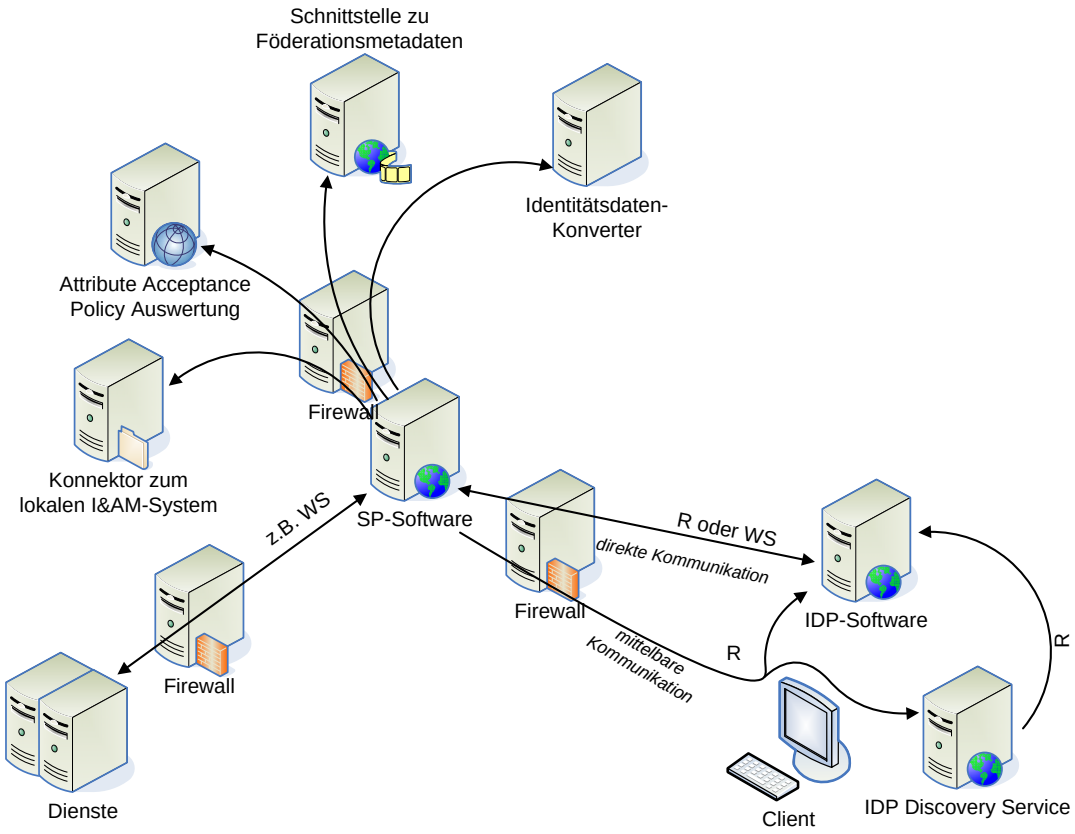


Abbildung 4.18.: Kommunikationsbeziehungen der Service Provider Software

- Mit dem Konnektor zum lokalen I&AM-System (siehe Abschnitt 4.4.9), dem Konnektor zu den föderationsweiten Metadaten (siehe Abschnitt 4.4.11), der Komponente zur Auswertung der Attribute Acceptance Policies (siehe Abschnitt 4.4.8) und dem Konverter für die Nutzdaten (siehe Abschnitt 4.4.12) wird über Web Services kommuniziert.

- Die Unterstützung von Benachrichtigungen über Datenänderungen durch IDPs und AAs (vgl. Anforderung [FA-Updates]) erfolgt über Web Services; als Referenz wird hierbei der Liberty ID-WSF Subscriptions & Notifications Service [LASUBS] angesehen, wobei – wie in Kapitel 3 erläutert – mit einer mittelfristigen Integration in SAML zu rechnen ist.

Im Bezug auf die Anpassung von Diensten ist zu berücksichtigen, dass diese auch organisationintern über FIM-Techniken genutzt werden können, sofern die Organisation sowohl SP als auch IDP ist; eine direktere Nutzung des lokalen I&AM-Systems ist jedoch im Allgemeinen einfacher zu implementieren und zwangsweise effizienter, wodurch im Gegenzug die Integration von FIM-Komponenten in das SP-seitige I&AM-System anstatt der Umstellung aller Dienste auf FIM mit motiviert wird.

4.4.7.3. Interne Sicherheitsmechanismen

Die in der IDP-Software angewandten Sicherheitsmechanismen lassen sich auf die SP-Software übertragen und werden hier deshalb nur skizziert:

- Die Authentizität der Kommunikationspartner muss z.B. durch Client- und Serverzertifikate überprüft werden. Insbesondere dürfen Aufträge zum Einholen von Auskünften nur von den eigenen Diensten akzeptiert werden.
- Im Rahmen der durch [FA-Updates] vorgegebenen Funktionalität dürfen Aktualisierungen nur von denjenigen Föderationsteilnehmern entgegen genommen werden, von denen die entsprechenden Attribute vorher mit dem expliziten Wunsch nach Updates abgefragt worden sind, um unerwünschten Modifikationen der lokalen Datenbestände vorzubeugen.

Die Datenqualität wird darüber hinaus über die in Abschnitt 4.4.8 erläuterten Attribute Acceptance Policies sichergestellt.

4.4.7.4. Einbettung in die Sicherheitsinfrastruktur

Für die SP-Software gelten dieselben Aussagen wie für die IDP-Software (siehe Abschnitt 4.4.1.5). Insbesondere ist auch hier eine starke Abschottung aufgrund der über die Benutzerclients mittelbaren Kommunikation praktisch nicht zu realisieren, sondern die Positionierung in einer demilitarisierten Zone anzustreben.

4.4.7.5. Hochverfügbarkeit

Auch hinsichtlich der Hochverfügbarkeit können bei der SP-Software dieselben Maßnahmen getroffen werden wie bei der IDP-Software (siehe Abschnitt 4.4.1.6).

Ein Ausfall der SP-Software würde dazu führen, das FIM-Funktionalitäten wie das organisationsübergreifende Single Sign-On nicht mehr genutzt werden können; die Konsequenzen für die einzelnen Dienste sind szenarienspezifisch und insbesondere davon abhängig, ob die Dienste alternativ die ins lokale I&AM-System eingespeisten Daten nutzen können oder eigene lokale Datenbestände haben, die z.B. als Cache genutzt werden können. Im Allgemeinen ist die Verfügbarkeit der SP-Software als essentiell einzustufen.

4.4.7.6. Managementschnittstellen

Bei der SP-Software sind zwei Managementaspekte besonders hervorzuheben:

1. Die Konfiguration umfasst neben den lokal zugelassenen Diensten insbesondere auch die Angabe, welche Daten aus den über die SP-Software abgewickelten Transaktionen extrahiert und über die in Abschnitt 4.4.9 beschriebene Komponente ins lokale I&AM-System eingetragen werden müssen.

2. Das **Accounting** muss je nach eingesetztem Abrechnungsmodell konfiguriert werden. Dabei besteht die Möglichkeit, sowohl die Nutzung der eigenen Dienste über FIM als auch die an IDPs, AAs und APs gestellten Anfragen zu erfassen, um diese Werte mit den von den Diensten bzw. als Datenquellen fungierenden Föderationsteilnehmern gelieferten Werten zu vergleichen.

Die SP-Software lässt sich darüber hinaus wie die übrigen Komponenten in das Systemmonitoring integrieren und ist erster Anlaufpunkt bei der Analyse vermutlich FIM-spezifischer Fehler auf SP-Seite.

4.4.7.7. Begründung des Designs der Komponente

Für die gewählte Gestaltung der SP-Software gelten im Wesentlichen dieselben Argumente wie bei der IDP-Software (siehe Abschnitt 4.4.1.8).

Durch die von allen FIM-Ansätzen vorgesehene Möglichkeit zur direkten Kommunikation zwischen Diensten und SP-Software muss diese die Koordination der anderen SP-seitigen FIM-Komponenten übernehmen, wohingegen dies IDP-seitig größtenteils Aufgabe des Gateways zum lokalen Datenbestand ist. Eine künstliche Entkopplung wäre zudem aufgrund der SP-seitig in Relation zu IDPs einfacheren Datenflüsse nicht sinnvoll; als Vorteil ergibt sich, dass die Realisierung des in Abschnitt 4.4.9 beschriebenen Konnektors zum SP-lokalen I&AM-System deutlich vereinfacht wird.

4.4.8. Komponente zur Auswertung von Attribute Acceptance Policies

Das Gegenstück zu Attribute Release Policies (ARPs) beim IDP stellen SP-seitig die so genannten Attribute Acceptance Policies (AAPs) dar; über sie kann konfiguriert werden, welche Datenkategorien bzw. Attribute von welchen IDPs bzw. AAs unter welchen Bedingungen (z.B. Vergleich gelieferter Attribute mit gültigen Wertemengen) angenommen werden sollen (vgl. Anforderungen [SEC-Trust], [ORG-Trust] und [ORG-SLAs]).

Analog zu ARPs können dabei föderationsweite, SP-weite und dienstspezifische AAPs miteinander kombiniert werden; im Unterschied zu ARPs haben Benutzer jedoch keinen Einfluss auf AAPs.

Zur Umsetzung kann entsprechend die in Abschnitt 4.4.4 beschriebenen Komponente auch auf SP-Seite eingesetzt werden, wobei sich lediglich die Ausprägungen der verwendeten Policies unterscheiden und die Kommunikation in diesem Fall mit der SP-Software stattfindet; auf das Zusammenspiel von ARPs und AAPs wird in Abschnitt 5.4 näher eingegangen.

4.4.9. Konnektor zum lokalen I&AM-System

Wie bereits in Abschnitt 4.4.7 beschrieben wurde, ist die FIM-basierte Ansteuerung von I&AM-Systemen beim SP in den bisherigen Ansätzen nicht vorgesehen gewesen, da der Endpunkt für die FIM-Kommunikation der jeweilige Dienst selbst sein musste.

Durch die Verlagerung dieses Kommunikationsendpunktes in die von den Diensten separierte SP-Software ergibt sich die Möglichkeit, über FIM bezogene Daten nicht nur an den vom

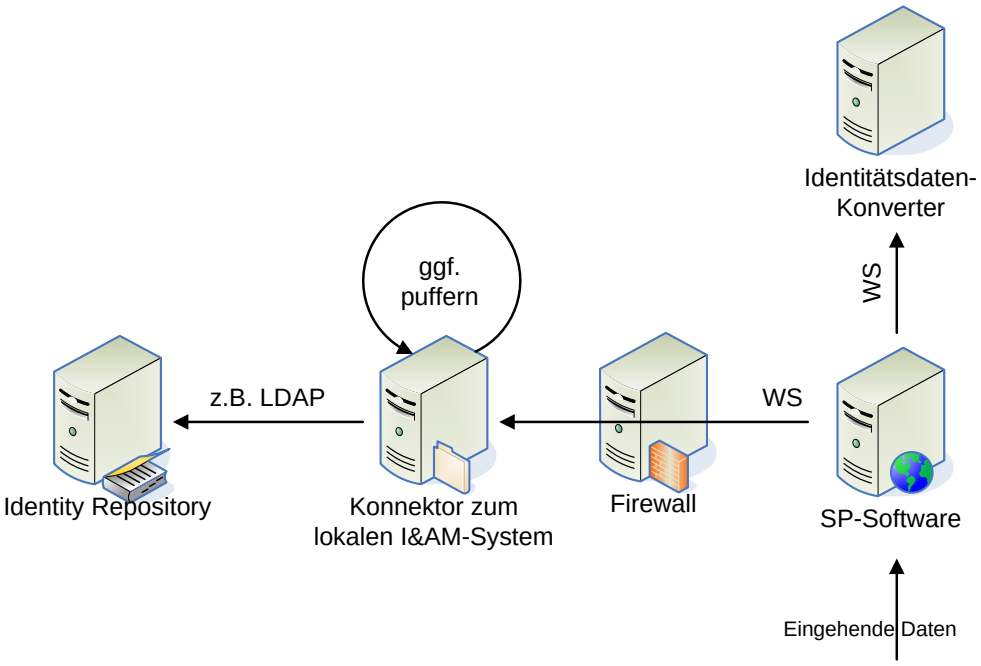


Abbildung 4.19.: Konnektor zum lokalen I&AM-System

Benutzer gewünschten Dienst, sondern auch an das I&AM-System des SP weiterzuleiten. Sofern es sich bei dem Dienst nicht um eine bereits verwendete Datenquelle des I&AM-Systems handelt, was praktisch nur selten der Fall ist, bildet diese Vorgehensweise eine hinreichende Grundlage für die Erfüllung der Anforderungen [FA-Abhängigkeiten] und [ORG-Datennutzung]: Abhängigkeiten zwischen Diensten werden von I&AM-System per Definition berücksichtigt, wenn ein Dienst korrekt daran angeschlossen ist, und die Verfügbarkeit der Daten im Identity Repository wird – im Gegensatz zur lokalen Speicherung bei nur einem Dienst – als ausreichend für ihre Verarbeitung durch andere Prozesse angesehen.

Die hier beschriebene und in Abbildung 4.19 dargestellte Komponente ist somit ein herkömmlicher Konnektor, wie er in Abschnitt 4.3.2 beschrieben wurde. Er arbeitet **unidirektional** und **eventgesteuert** in einem **Push-Verfahren** von der SP-Software hin zu einem lokalen Identity Repository, bei dem es sich um den zentralen Datenbestand des SP handeln kann, aber nicht muss – in Szenario 3 wurde bereits der Einsatz eines auf den Datenimport spezialisierten Verzeichnisdienstes erläutert, der als Puffer fungiert, wiederum mit dem zentralen Datenbestand abgeglichen wird und somit ein mehrstufiges Sicherheitskonzept erlaubt. Da die SP-Software den Identitätsdatenkonverter verwendet und die Daten somit bereits im lokal benötigten Format vorliegen, vereinfacht sich die Implementierung dieses Konnektors.

Als Besonderheit ist zu beachten, dass in der Regel ein vom I&AM-System vorgegebenes Minimum an Attributen bekannt sein muss, bevor ein Objekt dort angelegt werden darf (vgl. Beschreibung der *mandatory* Attribute in Abschnitt 2.1.2.4 und Anforderung [FA-Schema]). Hieraus ergeben sich zwei Teilanforderungen:

1. Es muss sichergestellt werden, dass jeder über FIM nutzbare Dienst mindestens diese

Benutzerattribute anfordert; diese Anforderung wird im Normalfall erfüllt.

2. Es muss davon ausgegangen werden, dass nicht immer alle benötigten Attribute bereits bei der ersten FIM-basierten Datenabfrage zur Verfügung gestellt werden, sondern über mehrere Anfragen verteilt eingehen. Der Konnektor muss diese Teilergebnisse zwischenpuffern, bis ein minimal vollständiges Objekt im Identity Repository angelegt werden kann.

Da die SP-Software die Nutzdaten analysiert und modifizieren kann, könnten alternativ gegebenenfalls notwendige zusätzliche Attributsanfragen für den Dienst transparent ergänzt werden, d. h. die SP-Software würde mehr Benutzerattribute anfordern als vom Dienst eigentlich verlangt. Diese Vorgehensweise müsste jedoch z. B. in den Datenschutzerklärungen zusätzlich berücksichtigt werden, da sich das IDP-seitig beobachtete Anfrageverhalten ansonsten von dem vom Dienst angegebenen unterscheiden würde.

4.4.10. IDP Discovery Service

In Abschnitt 2.1.2.7 wurde im Kontext des SP-First Use Cases erläutert, dass die Zuordnung eines noch nicht authentifizierten Benutzers zu dem für ihn zuständigen IDP ein unscheinbares, aber nicht triviales Problem darstellt.

Die hier beschriebene, in Anlehnung an SAML 2.0 als IDP Discovery Service bezeichnete Komponente kann SP-seitig oder als Trusted Third Party Service föderationsweit zentral betrieben werden; welche dieser beiden Varianten genutzt wird, hängt neben dem Betriebsaufwand auch von der Anzahl der Föderationen ab, an denen ein SP beteiligt ist: Bereits bei mehr als einer Föderation wäre unklar, welcher der für jeweils eine ganze Föderation eingesetzten IDP Discovery Services für einen Benutzer zuständig ist. Im Rahmen der Entwicklung von Shibboleth 2.0 spielen deshalb auch so genannte *Multi-Federation IDP Discovery Services*, die den herkömmlichen *Where Are You From* Service ablösen sollen, eine Rolle.

4.4.10.1. Funktionalität

Der IDP Discovery Service wird wie in Abbildung 4.20 dargestellt von der SP-Software eines SP mittelbar über den Benutzerclient aufgerufen und bietet als einzige Funktion das Ermitteln des zuständigen IDP an, zu dem der Benutzer wiederum zur Identifizierung und Authentifizierung weitergeleitet wird.

Die in Frage kommenden IDPs können über die in Abschnitt 4.4.11 beschriebene Komponente aus den Föderationsmetadaten ermittelt werden; Multi-Federation IDP Discovery Services unterstützen diesbezüglich die Auswertung der Metadaten von mehr als einer Föderation.

Im Regelfall erfolgt die Auswahl des zuständigen IDPs (IDP Selection) manuell durch den Benutzer, dem eine entsprechende Liste vorgelegt wird. Dies ermöglicht die primär in Privatkundenszenarien angestrebte freie IDP-Wahl durch Benutzer; insbesondere können für verschiedene Identitäten derselben Person auch verschiedene IDPs verwendet werden.

Wie in Abschnitt 2.1.2.7 bereits beschrieben wurde, existieren Alternativen wie beispielsweise die Auswertung der IP-Adresse des Benutzerclients, um daraus auf den zuständigen IDP zu schließen; um die freie Wahl des IDP nicht zu beeinträchtigen, wird der so ermittelte IDP

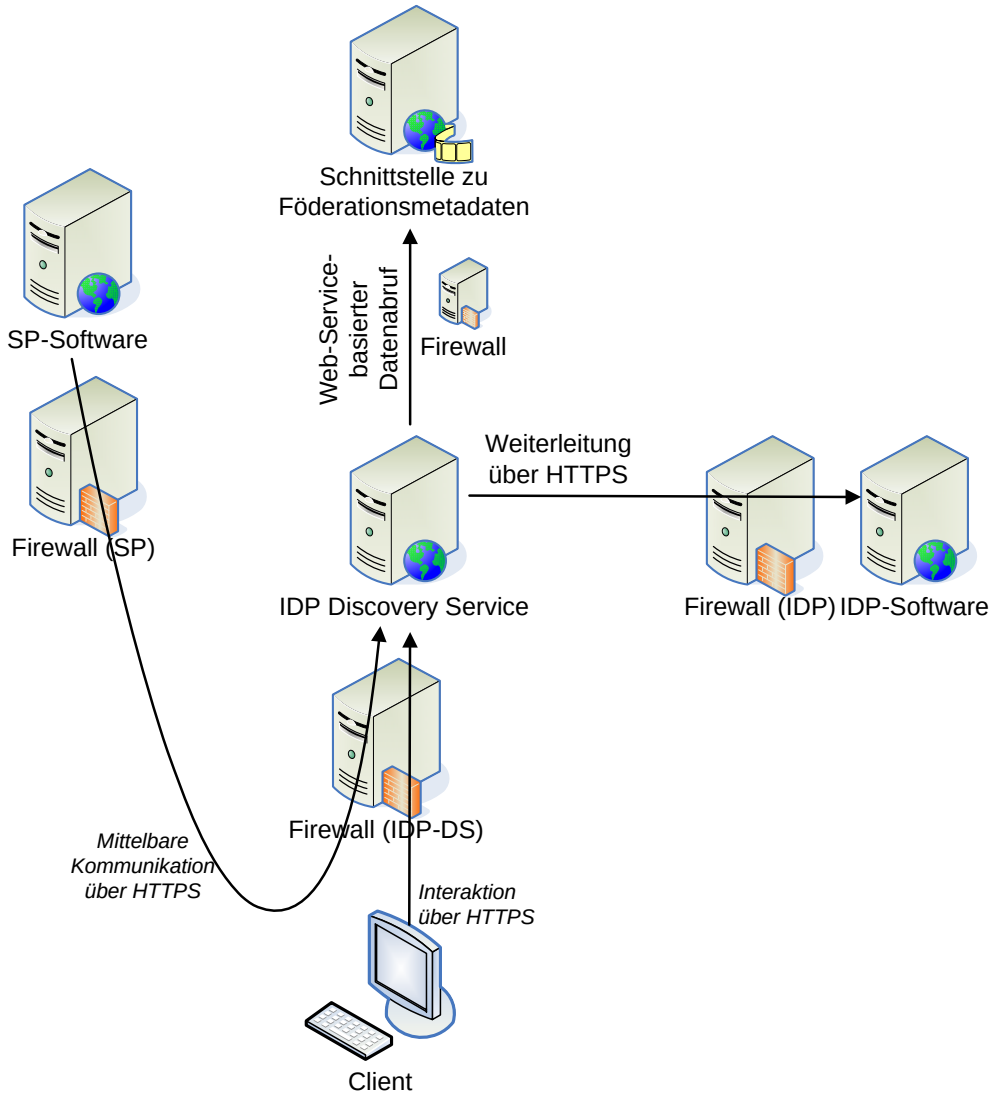


Abbildung 4.20.: Verwendung des IDP Discovery Services

jedoch in der Regel nur als Vorschlag angezeigt, der vom Benutzer bestätigt oder korrigiert werden kann.

Alternativ zur ständig wiederkehrenden Auswahl des IDP können Cookies verwendet werden, in denen die vom Benutzer getroffene Wahl hinterlegt wird. Der Benutzerclient schickt diese Information dann bei nachfolgenden Aufrufen automatisch an den IDP Discovery Service, so dass die Interaktion entfallen kann. In der Praxis wird diese Variante optional angeboten und primär von denjenigen Benutzern in Anspruch genommen, die nur einen einzigen IDP haben.

4.4.10.2. Datenmodell und Kommunikationsschnittstellen

Der IDP Discovery Service ist ein webbasierter Dienst, der mit dem aufrufenden SP und dem ermittelten IDP mittelbar über den Benutzerclient kommuniziert; hierbei kommt wie zur Interaktion mit dem Benutzer das Protokoll HTTPS zum Einsatz.

Der Service Provider übergibt als Parameter den URL des vom Benutzer angeforderten Dienstes und optional die Bezeichnung eines Authentifizierungsverfahrens, das der zuständige IDP aus Sicht des SP anwenden soll. Diese Daten werden dem ermittelten IDP unverändert übergeben.

Die Föderationsmetadaten werden von der in Abschnitt 4.4.11 beschriebenen Komponente über Web Services abgerufen.

4.4.10.3. Sicherheitsmechanismen und -infrastruktur

Ein grundlegender Schutz wird erreicht, indem Anfragen nur von SPs entgegen genommen bzw. nur an IDPs weitergeleitet werden, die in den Föderationsmetadaten verzeichnet sind.

Darüber hinaus kommt der Vertrauenswürdigkeit des IDP Discovery Services aus Sicht des Benutzers eine besondere Rolle zu: Er sollte sich darauf verlassen können, dass er wirklich zu demjenigen IDP weitergeleitet wird, den er aus der Liste ausgewählt hat. Im Hinblick auf die im Internet weit verbreiteten, so genannten Phishing-Angriffe ist zu befürchten, dass ein kompromittierter IDP Discovery Service den Benutzer zu der Webseite eines Angreifers umleitet, die identisch zu derjenigen des richtigen IDP aussieht, aber nur das Ziel hat, Benutzernamen und Passwörter abzugreifen. Seriöse IDP Discovery Services sollten ihre Benutzer auf diese Risiken hinweisen und zu einer genauen Überprüfung der Webseite, auf der sie ihre Authentifizierungsinformationen eingeben sollen, auffordern.

Da es sich um einen webbasierten Dienst handelt, auf den ggf. alle Benutzer einer Föderation zugreifen können müssen, gelten im Hinblick auf die Einbettung in die Sicherheitsinfrastruktur des Betreibers zu den Self Services analoge Aussagen (siehe Abschnitt 4.3.7.5).

4.4.10.4. Hochverfügbarkeit

Als webbasierter Dienst kann der IDP Discovery Service beispielsweise analog zu den Self Services hochverfügbar gestaltet werden (siehe Abschnitt 4.3.7.6).

Seine Verfügbarkeit ist beim föderationsweit zentralen Einsatz buchstäblich essentiell. In Kombination mit der noch geringen Verbreitung von Multi-Federation IDP Discovery Services ist dies derzeit für viele Service Provider ausschlaggebend dafür, den IDP Discovery Service bevorzugt lokal zu implementieren anstatt einen föderationsweit zur Verfügung stehenden Trusted Third Party Service in Anspruch zu nehmen.

4.4.10.5. Managementschnittstellen

Der IDP Discovery Service ist sehr wartungsfreundlich, da er dynamisch über die Föderationsmetadaten konfiguriert wird. Im Wesentlichen ist deshalb nur seine Verfügbarkeit und Auslastung zu überwachen. Im Hinblick auf die Protokollierung und das Fehlermanagement sind die folgenden Aspekte zu berücksichtigen:

- Aus Datenschutzperspektive ist bedenklich, dass dem IDP Discovery Service zwangsläufig Daten vorliegen, die Auskunft darüber geben, wie viele Benutzer welcher Identity Provider welche Dienste in Anspruch nehmen. Die Speicherung und Verarbeitung dieser Daten muss bei föderationsweiten IDP Discovery Services organisatorisch geregelt werden.
- Dauerhafte Fehler beim Weiterleiten von Benutzern an einen IDP lassen auf veraltete Föderationsmetadaten schließen, die deren Verwaltern mitgeteilt werden sollten. Dies betrifft insbesondere große Föderationen mit einer hohen Teilnehmerfluktuation.

Als Konsequenz empfiehlt sich beispielsweise, bei dieser Komponente nur Fehlersituationen festzuhalten und die Protokolldateien periodisch nach ihrer Auswertung zu löschen.

4.4.10.6. Begründung des Designs der Komponente

Die Komponente wurde unverändert von den anderen FIM-Ansätzen übernommen; dabei wurde die erst allmählich aufkommende Forderung nach der parallelen Unterstützung mehrerer Föderationen manifestiert.

Die Notwendigkeit dieser Komponente ist inhärent mit der beschränkten Funktionalität der ebenfalls unverändert übernommenen Clientsysteme verbunden: Sofern die Benutzerclients keine Information über den zuständigen IDP mitliefern, kann auf die Funktionalität des IDP Discovery Services nicht verzichtet werden.

4.4.11. Schnittstelle zu den Föderationsmetadaten

Während FIM-Transaktionen letztendlich eine Kommunikation zwischen zwei Organisationen darstellen und Benutzer mit dem Konzept von Föderationen höchstens im Rahmen des IDP Discovery Services in Berührung kommen, schaffen die Föderationsmetadaten die Grundlage für die folgenden Funktionalitäten:

1. **Ermittlung der Kommunikationsendpunkte** aller FIM-relevanten Dienste aller Föderationsteilnehmer: Typischerweise werden die zu verwendenden Protokolle, IP-Adressen bzw. DNS-Namen und TCP-Ports aller von außen erreichbaren FIM-Komponenten jedes Föderationsteilnehmers in Form von URIs erfasst.
2. **Ermittlung von Serverzertifikaten**: Die Zertifikate von Kommunikationspartnern werden zu deren Authentifizierung sowie für die Ende-zu-Ende-Verschlüsselung der an sie geschickten Nachrichten benötigt. Die zentrale Bereitstellung in den Föderationsmetadaten vereinfacht diese so genannte Schlüsselverwaltung, die aufgrund der beschränkten Gültigkeitsdauer von Zertifikaten und dem möglichen Widerrufen von Zertifikaten (engl. *certificate revocation*) eine bei großen Föderationen potentiell hohe Dynamik aufweist.
3. **Ermittlung von Ansprechpartnern**: Analog beispielsweise zu DNS-Zoneneinträgen werden organisatorische und technische Ansprechpartner für jeden Föderationsteilnehmer verzeichnet, um das Fehlermanagement zu unterstützen.

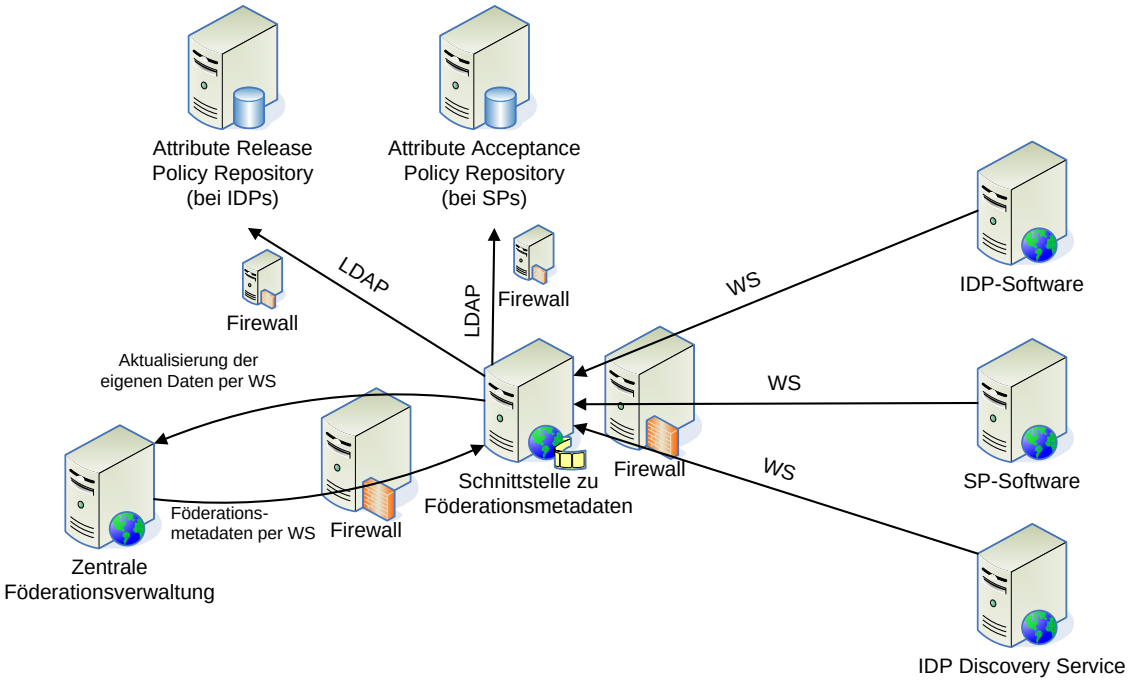


Abbildung 4.21.: Umfeld der Schnittstelle zu den Föderationsmetadaten

4. **Distribution föderationsweiter Policies**: Vereinbarungen zum Datenschutz und zur Datenqualität können über föderationsweite Attribute Release bzw. Acceptance Policies einheitlich umgesetzt werden.

Dabei ist zu beachten, dass in den bisherigen FIM-Ansätzen nur die ersten drei Punkte berücksichtigt werden und nur ein lesender Zugriff auf diese Daten vorgesehen ist.

4.4.11.1. Funktionalität

Die hier beschriebene und in Abbildung 4.21 dargestellte Komponente dient dem lesenden und schreibenden Zugriff auf die Föderationsmetadaten; ihre Funktion wird nachfolgend lediglich in einer abstrakten Black-Box-Sicht beschrieben, da die interne Funktionsweise und die exakten Signaturen keine Auswirkungen auf die Gesamtarchitektur haben:

- Die föderationsweiten Metadaten werden jedem Föderationsteilnehmer bei jeder Änderung zugeschickt, so dass immer der aktuelle Datenbestand lokal vorliegt, wodurch neben der Verfügbarkeit auch die Performanz lokaler Leseoperationen erhöht wird.

  Es ist zu beachten, dass die hier beschriebene **Auslieferung der Föderationsmetadaten in einem Push-Verfahren** nicht der gängigen Praxis entspricht. Vielmehr werden die Föderationsdaten derzeit üblicherweise einmal pro Tag in einem Pull-Verfahren von einer zentralen Stelle abgerufen und die dabei potentiell auftretenden temporären Inkonsistenzen in Kauf genommen. Dadurch reduziert sich der Implementierungsaufwand

auf der Seite der Föderationsverwaltung, da beispielsweise keine Fehlerbehandlung für temporär nicht verfügbare Föderationsteilnehmer notwendig ist.

- Beim lesenden Zugriff durch eine andere FIM-Komponente sind die gewünschten Daten zu spezifizieren; hierfür müssen geeignete Funktionen bereitgestellt werden, denen entsprechende Suchkriterien als Parameter übergeben werden können. Ein Beispiel ist der Abruf einer Liste aller IDPs mit ihren Namen und den URIs der zugehörigen IDP-Software-Komponenten, die vom IDP Discovery Service benötigt wird.

- **Schreibzugriffe** auf die zentral gehaltenen Föderationsmetadaten stellen Managementoperationen dar, mit denen jeder Föderationsteilnehmer die ihn betreffenden Metadaten modifizieren kann. Sie setzen eine Authentifizierung des Föderationsteilnehmers voraus, die erst dann maschinell durchgeführt werden kann, wenn das Zertifikat des lokal eingesetzten Kommunikationsendpunktes von der Föderationsverwaltung bereits eingetragen, d. h. die Organisation in die Föderation aufgenommen wurde.

- **Einspeisen föderationsweiter Policies** in die lokalen Systeme; die in den Metadaten enthaltenen Attribute Release und Acceptance Policies müssen wie unten beschrieben in die Policy Repositories der entsprechenden Komponenten übertragen werden.

Je nach Organisation der Föderationsverwaltung können Schreibzugriffe einem Genehmigungsverfahren und damit einer Zeitverzögerung unterliegen, die insbesondere bei der Änderung von Kommunikationsendpunkten und Zertifikaten berücksichtigt werden muss.

4.4.11.2. Datenmodell und Kommunikationsschnittstellen

Für SAML, die Liberty Alliance Spezifikationen und WS-Federation existieren standardisierte Metadatenformate, die geeignete Erweiterungsmechanismen z. B. für die in diesem Konzept geforderte Integration von föderationsweiten Policies bieten [S2META, LAMETA, WS-MDX].

In der Regel werden alle Föderationsmetadaten zu einer Datei zusammengefasst, die elektronisch signiert und über eine web-service-basierte Schnittstelle übertragen wird, die ebenfalls für die Kommunikation mit den anderen lokalen FIM-Komponenten eingesetzt wird; beim derzeit üblichen Pull-Verfahren wird in der Regel HTTPS zum Abruf der Daten von der zentralen Föderationsverwaltung verwendet. Bei der Datenübertragung findet eine Authentifizierung der Gegenstelle statt, die durch eine Überprüfung der Metadatensignatur beim Empfänger zur Sicherstellung der Integrität ergänzt wird.

Langfristig ist mit wachsendem Umfang der Föderationsmetadaten in Erwägung zu ziehen, im Regelbetrieb lediglich Differenzmengen zu übertragen.

Im Hinblick auf die in den Metadaten enthaltenen föderationsweiten Attribute Release und Acceptance Policies ist zu beachten, dass sich diese zwangsläufig auf das föderationsweite Datenmodell beziehen und vor dem Einspielen in das lokale ARP bzw. AAP Repository entsprechend konvertiert werden müssen. Hierfür kann die im Konverter für heterogene Informationsmodelle eingesetzte Technik angewandt werden (siehe Abschnitt 4.4.12); ein Beispiel für die Transformation ganzer Policies (im Gegensatz zur Konvertierung einzelner Benutzerattribute) wird in Abschnitt 5.3.4.2 gegeben.

4.4.11.3. Interne Sicherheitsmechanismen

Die Sicherheitsaspekte von Föderationsmetadaten wurden bislang noch nicht tiefgehend analysiert. Offensichtlich ist, dass ihre Verfälschung dazu führen kann, dass vermeintlich mit einem Föderationsteilnehmer kommuniziert wird, obwohl es sich um ein System eines Angreifers handelt. Dadurch können personenbezogene Daten kompromittiert oder die Nutzung von Diensten unter falschem Namen erschlichen werden. Derzeit wird das Signieren der Föderationsmetadaten als ausreichende Sicherheitsmaßnahme angesehen.

4.4.11.4. Einbettung in die Sicherheitsinfrastruktur

Die Kommunikation mit dieser Komponente kann beispielsweise über Paketfilterfirewalls auf die bekannten anderen FIM-Komponenten und die zentrale Föderationsverwaltung eingeschränkt werden.

Darüber hinaus können die in Abschnitt 4.3.1.6 beschriebenen Maßnahmen angewendet werden.

4.4.11.5. Hochverfügbarkeit

Zur Umsetzung der Hochverfügbarkeit können die in Abschnitt 4.3.1.7 erläuterten Maßnahmen eingesetzt werden. Die Hochverfügbarkeit dieser Komponente ist für die IDP-Software, die SP-Software sowie den IDP Discovery Service essentiell, so dass sie auch aus Performanzgründen häufig in diese integriert wird.

4.4.11.6. Managementschnittstellen

Neben der Überwachung der Komponente auf ihre Verfügbarkeit und reguläre Operation im Hinblick auf den kontinuierlichen Bezug aktueller Föderationsmetadaten liegt der Managementschwerpunkt auf der Pflege der die eigene Organisation betreffende Teilmenge der Metadaten. Diesbezüglich sind zukünftig geeignete Werkzeuge zu schaffen, die diesen Prozess beispielsweise durch den Einsatz von Discoverymechanismen und Service Registries partiell automatisieren können.

4.4.11.7. Begründung des Designs der Komponente

Die bereits in den anderen FIM-Ansätzen vorgesehene Schnittstelle zu den Föderationsmetadaten wurde um föderationsweite Policies erweitert und auf ein push-basiertes Verteilungsverfahren umgestellt.

Szenarien, in denen föderationsweite Policies gewinnbringend eingesetzt werden können, sind leicht zu konstruieren, wenngleich von dieser Funktionalität aufgrund des bislang allgemein zurückhaltenden Einsatzes von ARPs und AAPs erst mittelfristig Gebrauch gemacht werden wird.

Die Entscheidung für ein von einer zentralen Stelle ausgehendes Push-Verfahren wird primär durch die ansonsten zwischen Organisationen auftretenden Metadateninkonsistenzen

motiviert, die z. B. bei derzeit existierenden Shibboleth-basierten Föderationen zu schwierig diagnostizierbaren Fehlersituationen führen.

Da die Schnittstelle zu den Föderationsmetadaten prinzipiell auch von Trusted Third Party Diensten benötigt werden kann, wurde sie als eigenständige Komponente beschrieben; wie oben erläutert wurde, ist jedoch eine Integration z. B. in IDP- oder SP-Software möglich.

4.4.12. Konverter für Identitätsdaten bei heterogenen Informationsmodellen

Der Konverter für heterogene Identitätsdatenmodelle ist in den bisherigen FIM-Ansätzen nicht vorgesehen; seine genaue Funktionsweise wird in Abschnitt 5.2 beschrieben.

Die prinzipielle Aufgabe dieser Komponente ist die Umwandlung der über FIM eingehenden Nutzdaten ins lokal verwendete Datenformat bzw. die Konvertierung zu übertragender Daten in ein vom Empfänger verarbeitbares Format. Im einfachsten Fall entspricht dies der **bidirektionalen Konvertierung** des lokalen Datenschemas in ein föderationsweites Datenschema; die entsprechenden Konvertierungsregeln müssen vor Inbetriebnahme spezifiziert werden.

Der in dieser Arbeit konzipierte Konverter geht jedoch noch einen Schritt weiter und berücksichtigt Föderationen, für die kein föderationsweites Datenmodell spezifiziert werden kann; dieser Fall liegt insbesondere in Privatkundenszenarien vor, in denen die Anzahl beteiligter IDPs und SPs nicht beschränkt werden kann und außer der Nutzung von FIM-basiertem Datenaustausch keine Motivation für die organisatorisch enge Zusammenarbeit der Föderationsteilnehmer besteht. Beispielsweise ist unwahrscheinlich, dass sich eine große Zahl konkurrierender E-Commerce-Provider auf ein gemeinsames Datenmodell einigen wird, da alle bisherigen Ansätze dazu gescheitert sind (vgl. z. B. [CPXCHG]).

Bei n verschiedenen Datenmodellen müssten somit $O(n^2)$ Konvertierungsregelsätze implementiert werden; dies würde einen praktisch inakzeptabel hohen Aufwand darstellen. Aus diesem Grund sieht das Konzept für diese Komponente vor, dass die Bestandteile von Regelsätzen wiederverwendbar sind und über ein föderationsweites Repository, das als Federation Schema Correlation Service (FSCS) bezeichnet wird, zugänglich gemacht werden. Dadurch wird das Ausnutzen der Transitivität von Konvertierungsregeln sowie der Einsatz von auf Datenkonvertierungsregeln spezialisierten Trusted Third Parties ermöglicht.

4.4.12.1. Funktionalität und Datenmodell

Die über den FSCS abrufbaren Konvertierungsregeln werden analog zu den Föderationsmetadaten lokal gespeichert, so dass auch sämtliche Konvertierungsprozesse lokal ablaufen und die Nutzdaten nicht an einen Dritten übergeben werden müssen.

Beim Aufruf erhält die Komponente die zu konvertierenden Daten, zu denen neben Autorisierungsinformationen insbesondere die Namen und Werte von Benutzerattributen und die Angabe des Absenders bzw. Empfängers der Daten gehören.

Die Nutzdaten liegen intern in XML vor und werden mittels so genannter Stylesheets für die standardisierte XML-Transformationssprache XSLT bearbeitet; die Details hierzu werden in Abschnitt 5.2 beschrieben.

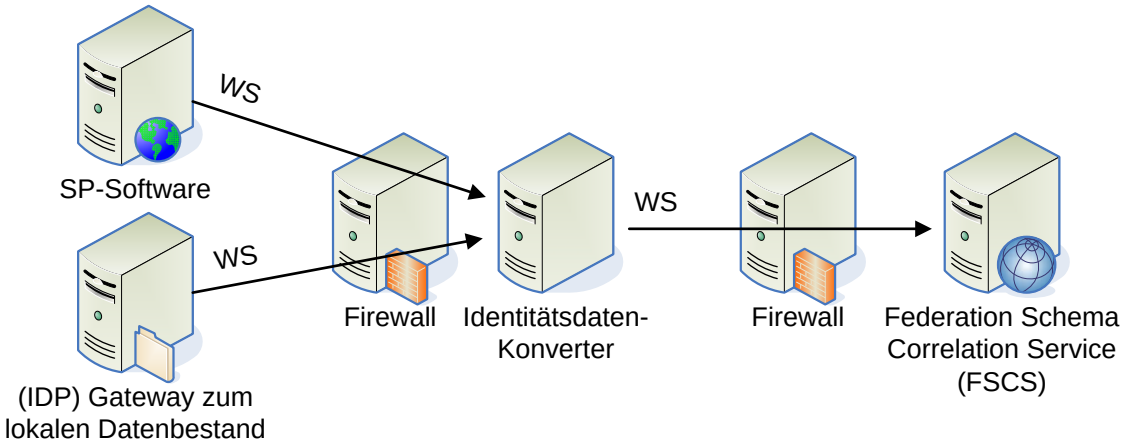


Abbildung 4.22.: Kommunikationsschnittstellen des Identitätsdatenkonverters

4.4.12.2. Kommunikationsschnittstellen und Kommunikationspartner

Die SP-Software und die IDP-seitige Schnittstelle zu den lokalen Datenbeständen verwenden web-service-basierte entfernte Prozeduraufrufe; mit dem zentralen Repository für Konvertierungsregeln wird wie in Abbildung 4.22 dargestellt ebenfalls über Web Services kommuniziert.

4.4.12.3. Interne Sicherheitsmechanismen

Über eine beispielsweise serverzertifikatsbasierte Authentifizierung wird die Authentizität der Kommunikationspartner sichergestellt; die Integrität der verwendeten Konvertierungsregeln kann anhand ihrer elektronischen Signaturen überprüft werden.

4.4.12.4. Einbettung in die Sicherheitsinfrastruktur

Die Kommunikation dieser Komponente kann beispielsweise über Paketfilterfirewalls auf die übrigen FIM-Komponenten und den FSCS eingeschränkt werden, wodurch eine sehr starke Abschottung insbesondere von den Benutzern erreicht wird.

Ebenso können die in Abschnitt 4.3.1.6 beschriebenen Maßnahmen eingesetzt werden.

4.4.12.5. Hochverfügbarkeit

Die Abhängigkeiten von diesem Konverter sind mit der Komponente zum Zugriff auf die Föderationsmetadaten vergleichbar; entsprechend gelten auch für die Realisierung der Hochverfügbarkeit die in Abschnitt 4.4.11 gemachten Aussagen.

4.4.12.6. Managementschnittstellen

Der zentrale Managementaspekt bei dieser Komponente ist die Administration der das eigene Datenmodell betreffenden Konvertierungsregeln; durch die Verwendung des Standards XSLT

kann auf eine breite Palette an Entwicklungs- und Testwerkzeugen zurückgegriffen werden.

Das Fehlermanagement ist insbesondere durch das Protokollieren fehlgeschlagener Konvertierungsoperationen zu unterstützen; sie geben Aufschluss darüber, für welche Kommunikationsbeziehungen und Datenmengen noch keine passenden Konvertierungsregeln spezifiziert wurden.

Neben der Verfügbarkeit der Komponente ist insbesondere ihre Auslastung zu überwachen; aufgrund der eventuell vielen komplexen XML-Transformationen bei jeder FIM-Transaktion besteht die Gefahr, dass diese Komponente zum Flaschenhals beim Datendurchsatz wird.

4.4.12.7. Begründung des Designs der Komponente

Der Funktionsumfang des Identitätsdatenkonverters wird durch die mit I&AM-Systemen gemachten praktischen Erfahrungen motiviert, dass heterogene Datenmodelle keine Ausnahme, sondern die Regel sind, und dass mit einem einzigen gemeinsamen Datenmodell nicht immer alle Anforderungen erfüllt werden können.

Die Einführung des FSCS ist aufgrund der von ihm gebotenen Funktionalität notwendig (siehe Abschnitt 5.2), so dass eine Distribution der Konvertierungsregeln über die Föderationsmetadaten nicht ausreichend wäre; zudem gelten die Konvertierungsregeln unabhängig vom aktuellen Föderationskontext, so dass eine Pflege derselben Regeln in den Metadaten mehrerer Föderationen unerwünscht redundant wäre.

4.4.13. Unterstützende Komponenten

Der Betrieb von Identitätsföderationen setzt weitere Komponenten voraus, die nur zum Teil FIM-spezifisch sind. Sie haben nur indirekte Auswirkungen auf das hier vorgestellte Architekturkonzept und werden deshalb nachfolgend nur knapp skizziert:

- **Public-Key Infrastruktur** (PKI): Das Management und die Überprüfung von Serverzertifikaten wird durch eine föderationsweit einheitliche PKI wesentlich erleichtert. Da eine PKI typischerweise auch außerhalb von FIM benötigt wird, werden ihr Aufbau und die organisatorischen Rollen wie Certificate Authority und Registration Authority nicht erläutert. Es ist jedoch zu beachten, dass Attribute Authorities und Identity Provider, die ihren Benutzern Attributszertifikate ausstellen möchten, neben den Serverzertifikaten für ihre FIM-Komponenten ein weiteres Zertifikat benötigten, das sie zur Ausstellung solcher Zertifikate berechtigt (siehe [RFCAC]).
- **Trust Level Management**: Die differenzierte Behandlung von Föderationsteilnehmern wird seitens der FIM-Komponenten über die Attribute Release und Acceptance Policies gesteuert. Deren diesbezügliche Konfiguration orientiert sich typischerweise primär an im Rahmen von SLAs relativ statisch vereinbarten und auf Geschäftsprozessebene zugesicherten Dienstgüteparametern; die Dynamik größer werdender Föderationen muss jedoch geeignet unterstützt werden. Entsprechend sind Werkzeuge aus dem Umfeld des Trust & Reputation Managements einzusetzen, die beispielsweise die Einstellungen für schwellwertbasierte Datenfreigaben dynamisch aktualisieren. Die Dissertation von Boursas untersucht u. a. diese FIM-spezifische Anwendung.

- **Föderationsverwaltung**: Die organisatorisch komplexe Verwaltung von Föderationen muss beispielsweise bezüglich des SLA-Managements geeignet unterstützt werden. Im Kontext dieser Arbeit ist lediglich der technische Prozess der Erstellung der Föderationsmetadaten relevant; das Zusammenfügen der einzelnen Bestandteile zu einer Datei und das elektronische Signieren werden derzeit noch häufig manuell erledigt. Da es sich um die Verarbeitung von Text- bzw. XML-Dateien handelt, können diese Vorgänge jedoch mit relativ einfachen Mitteln automatisiert werden, auf die hier nicht näher eingegangen wird.

Für die durchgängige Unterstützung organisationsübergreifender Prozesse reicht FIM als technische Lösung alleine zwangsläufig nicht aus; für das organisationsübergreifende Workflowmanagement kann jedoch beispielsweise auf die in den Föderationsmetadaten enthaltenen Kontaktinformationen zurückgegriffen werden.

4.5. Abhängigkeiten zwischen I&AM- und FIM-Komponenten

In den Abschnitten 4.3 und 4.4 wurden alle an der Gesamtarchitektur beteiligten Komponenten erläutert. Aus den jeweils genannten Schnittstellen ergeben sich die direkten Abhängigkeiten zwischen diesen Komponenten, deren isolierte Analyse jedoch nur eine sehr eingeschränkte Sicht auf das Gesamtsystem ermöglicht.

In diesem Abschnitt werden deshalb grundlegende Aspekte der komponentenübergreifenden Abhängigkeiten sowie Randbedingungen auf Basis der bereits in Abbildung 4.3 auf Seite 167 gezeigten Gesamtarchitektur dargestellt, anhand derer die in Abschnitt 4.6 beschriebene Integrationsmethodik motiviert wird; für das in Abschnitt 4.8 beschriebene Change Management müssen zudem die in Abschnitt 4.7 erläuterten Sicherheitsaspekte berücksichtigt werden.

4.5.1. Abhängigkeiten und Randbedingungen bei Identity Providern und Attribute Authorities

Die IDP-seitigen FIM-Komponenten sind im Unterschied zu den I&AM-Komponenten sehr stark aufeinander abgestimmt und nicht beliebig kombinierbar; es kann jedoch je nach gewünschtem Nutzungsumfang von FIM beispielsweise auf das Privilege Management System oder auf den Notifications-Konnektor und die entsprechende Datenbasis verzichtet werden. Alle übrigen FIM-Komponenten werden für einen realen praktischen Einsatz jedoch benötigt.

Der Gateway zum lokalen Datenbestand sieht den Abruf der Benutzerdaten aus einem Identity Repository im Pull-Verfahren vor; als Konsequenz sind somit rein provisioningsystembasierte I&AM-Systeme für den Einsatz von FIM nicht geeignet. Auch vom Einsatz ausschließlich auf Basis virtueller Verzeichnisdienste realisierter I&AM-Systeme muss abgeraten werden, da sich in diesem Fall die Quellsysteme in der Regel nur sehr bedingt für die Hinterlegung FIM-spezifischer Daten bzw. föderationsspezifischer Zusatzdaten, z. B. bei Schreibzugriffen durch die SPs, eignen. Somit stellen **Meta-Directories die beste Ausgangsbasis** für die Integration der FIM-Komponenten dar.

Im Rahmen dieses Konzeptes wird ohne Beschränkung der Allgemeinheit davon ausgegangen, dass ein IDP bzw. eine AA über genau ein Identity Repository verfügt; sofern eine

Verteilung der Identitätsdaten auf mehrere Identity Repositories aus organisatorischen oder juristischen Gründen notwendig ist, kann davon ausgegangen werden, dass der Gateway zum lokalen Datenbestand mit mehr als einer Datenquelle umgehen kann (vgl. Beschreibung der Funktionalität in Abschnitt 4.4.3).

Auf dieser Basis ergeben sich die folgenden weiteren Abhängigkeiten:

- Das IDP-seitig eingesetzte Datenmodell muss ggf. um föderationsspezifische Attribute erweitert werden; hiervon sind auch Werkzeuge wie die Self Services betroffen, die das benutzergesteuerte Modifizieren dieser Daten selektiv ermöglichen oder ggf. verhindern müssen.
- Die Authentifizierung des Benutzers durch den IDP ist eine notwendige Voraussetzung für alle weiteren FIM-Transaktionen; da die IDP-Software hierfür auf I&AM-Komponenten wie organisationsinterne Single Sign-On Systeme zurückgreift, müssen diese bereits im Einsatz sein oder mit der Einführung von FIM nachgerüstet werden.
- Analog gilt für die Unterstützung von Langzeit-Obligationen im organisationsübergreifenden Privacy Management, dass der Obligation Monitor eines lokalen Privacy Management Systems verwendet werden können sollte.
- Der das Identity Repository und die IDP-Software verbindende Notifications-Konnektor gehört aktuell noch nicht zum Standardlieferumfang z. B. von Meta-Directory-Produkten; somit müssen Frameworks eingesetzt werden, die eine geeignete Implementierung dieses Konnektors ermöglichen.

Daraus lässt sich ableiten, dass bereits existierende umfassende und flexible I&AM-Systeme die Integration von FIM-Komponenten gegenüber einer völligen Neuinstallation wesentlich erleichtern.

4.5.2. Abhängigkeiten bei Service Providern

Aufgrund der geringeren Notwendigkeit für FIM-spezifische Benutzerinteraktionen ist die Anzahl der SP-seitig benötigten Komponenten im Vergleich zum IDP niedriger, woraus sich auch ein niedrigerer Grad an Abhängigkeiten ergibt.

Zu beachtende Randbedingungen ergeben sich beim SP primär aus der Rolle der SP-Software als Datenquelle für das lokale I&AM-System. Insbesondere an die Datenqualität werden Anforderungen gestellt, die ebenfalls für andere lokale Datenquellen gelten können; sie müssen entsprechend auf die Attribute Acceptance Policies abgebildet werden.

Die Implementierung des Konnektors zum lokalen I&AM-System wird dadurch vereinfacht, dass die eingehenden Daten aufgrund der Vorverarbeitung durch den Identitätsdatenkonverter bereits im lokal benötigten Datenformat vorliegen. Die Eventorientierung dieses Konnektors legt jedoch eine sehr enge Verknüpfung mit der SP-Software nahe, so dass in der Regel nicht die Konnektorenframeworks des lokalen I&AM-Systems verwendet werden können.

Ein zentraler Aspekt der SP-seitigen FIM-Einführung bleibt jedoch die FIM-Fähigkeit der Dienste; nur wenn diese gegeben ist, können FIM-Funktionalitäten wie organisationsübergreifendes Single Sign-On im SP-first Use Case und dynamische, verteilte Autorisierungsin-

frastrukturen genutzt werden, da diese über das Einspeisen der Benutzerdaten in das lokale Identity Repository nicht erreicht werden können.

4.5.3. Zusammenspiel der policybasierten Systeme

Der parallele Einsatz mehrerer policybasierter Systeme wird durch ihren komplementären Charakter wie folgt motiviert:

- Die organisationsinternen Privacy Management Systeme steuern den Zugriff lokaler Mitarbeiter auf personenbezogene Daten von Benutzern. Sie liegen in der Regel im Hoheitsbereich des Datenschutzbeauftragten bzw. CPO (Chief Privacy Officer) der Organisation; Benutzer haben keinen Einfluss darauf, aber in der Regel ein ggf. eingeschränktes Einsichtsrecht.
- Das organisationsübergreifende Privacy Management System wird IDP- und AA-seitig eingesetzt, um die Herausgabe personenbezogener Daten an Dritte (Service Provider) zu regeln. Sie werden somit primär von den betroffenen Benutzern selbst konfiguriert, wobei Administratoren geeignete Voreinstellungen konfigurieren sollten, um insbesondere unerfahrenen oder desinteressierten Benutzern eine brauchbare Ausgangsbasis zur Verfügung zu stellen.
- Die SP-seitigen Attribute Acceptance Policies (AAPs) dienen nur sekundär der Einhaltung von Datenschutzauflagen, indem sie nicht benötigte Benutzerattribute verwerfen, bevor sie ins SP-seitige I&AM-System eingespielt werden; ihre Hauptaufgabe ist hingegen die Sicherstellung der erforderlichen Datenqualität.
- Privilege Management Systeme verwalten organisationsübergreifend relevante Autorisierungsinformationen, die sich von ARPs zudem dadurch unterscheiden, dass Benutzer in der Regel keinen Einfluss darauf haben.

Da Privacy und Privilege Management Systeme bereits unabhängig voneinander existieren können, wird die Zusammenführung zu einem großen policybasierten Managementsystem in dieser Arbeit nicht verfolgt. Wie in Abschnitt 5.3 gezeigt wird, lassen sich jedoch bei ARPs und AAPs Synergien durch den Einsatz einer gemeinsamen Policysprache mit einer entsprechend vergleichbaren Administrations- und Auswertungsarchitektur auf IDP- und SP-Seite ausnutzen.

4.5.4. Abhängigkeitsgraphen

Die Abbildungen 4.23 und 4.24 verdeutlichen die Abhängigkeiten zwischen den I&AM- und FIM-Komponenten anhand ihrer Funktionalität: Eine Komponente auf einer Schicht kann erst erfolgreich umgesetzt werden, wenn die dazu benötigten Komponenten auf den darunter liegenden Schichten bereits in Betrieb sind.

Sofern diese Abhängigkeiten berücksichtigt werden, kann die Realisierung aller Komponenten einer Schicht parallel angestrebt werden. Diese Vorgehensweise wird im folgenden Abschnitt vertiefend erläutert.

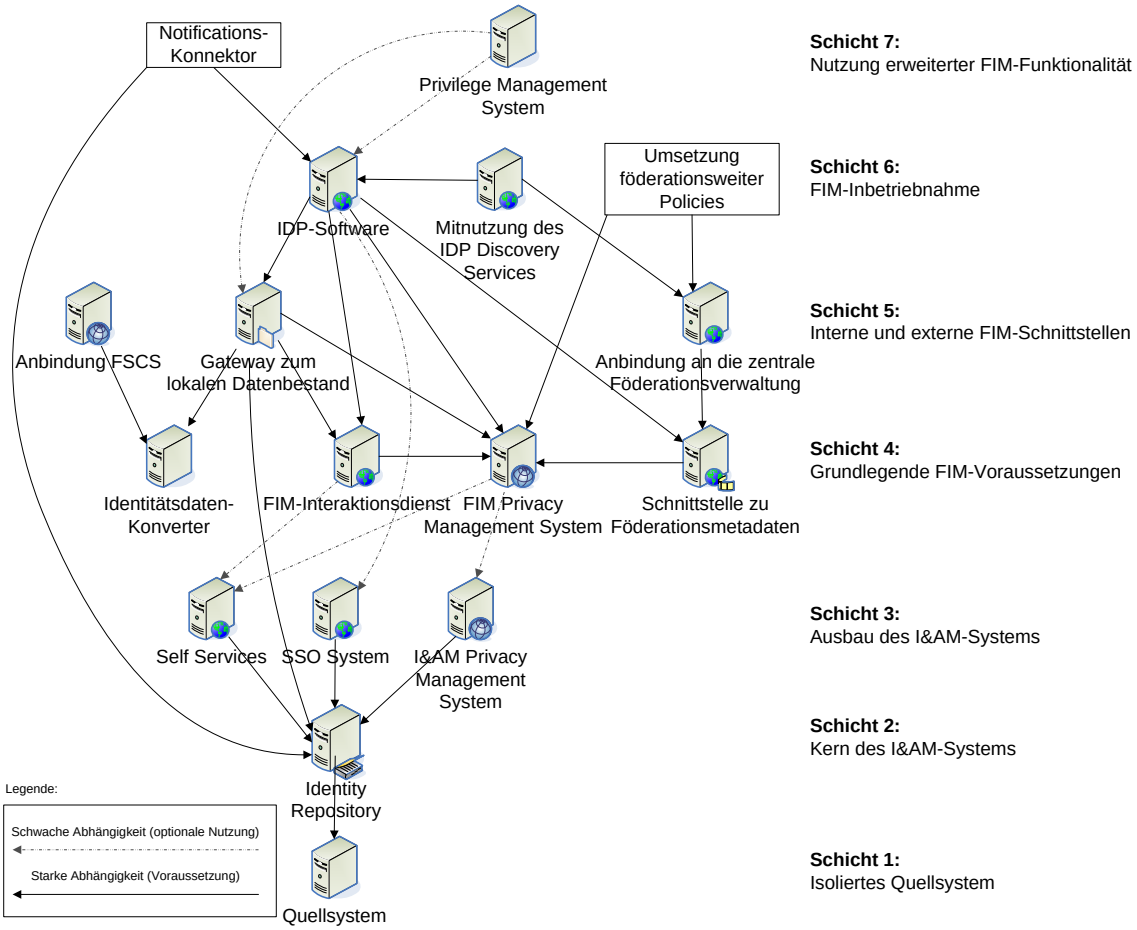


Abbildung 4.23.: IDP-seitige Abhängigkeiten bei der Inbetriebnahme der Komponenten

4.6. Integrationsmethodik

Nach der Betrachtung der Einzelkomponenten und ihrer gegenseitigen Abhängigkeiten werden nun Wege zur systematischen Integration der FIM-Komponenten in bestehende I&AM-Systeme aufgezeigt. Neben der rein technischen Systemintegration spielt dabei auch die Weiterentwicklung der organisatorischen Abläufe eine wesentliche Rolle.

Die einzelnen Schritte werden zuerst separat für Identity Provider und Service Provider erläutert; in Abschnitt 4.6.5 wird anschließend auf die Besonderheiten eingegangen, wenn eine Organisation sowohl als IDP als auch als SP fungieren soll.

Die relevanten Aspekte des Security Managements werden in Abschnitt 4.7 diskutiert; diese strukturelle Trennung erfolgt einerseits zur Verbesserung der Übersichtlichkeit und reflektiert andererseits die häufig praktizierte Trennung der fachlichen Zuständigkeiten in größeren Organisationen. Bei einer konkreten Umsetzung müssen zwangsläufig beide Aufgaben parallel berücksichtigt werden.

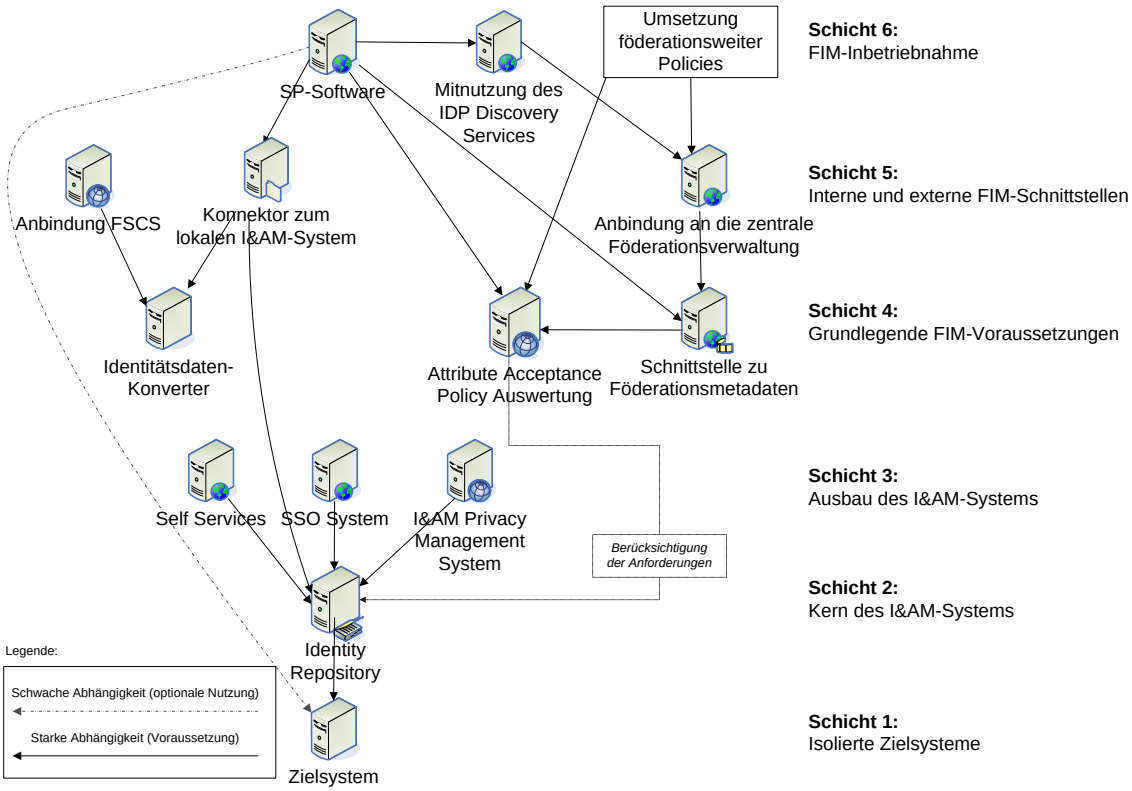


Abbildung 4.24.: SP-seitige Abhängigkeiten bei der Inbetriebnahme der Komponenten

4.6.1. Vorbereitungen bei IDPs und AAs

Identity Provider haben neben der Authentifizierung von Benutzern ebenso wie Attribute Authorities die primäre Aufgabe, als zuverlässige Datenquelle für die an einer Föderation beteiligten Service Provider zu fungieren. Dies schlägt sich in den folgenden sehr grundlegenden Anforderungen nieder, deren Erfüllung in der Praxis jedoch sehr aufwendig werden kann:

- Das eingesetzte Identity Repository muss die benötigten Daten bereitstellen. Hierbei ist zu bedenken, dass die Föderation oder einzelne SPs Daten über Benutzer benötigen können, die für das organisationsinterne I&AM bislang gänzlich irrelevant waren und deshalb aus praktischen Gründen und dem Prinzip der Datensparsamkeit nicht im Identity Repository vorgehalten wurden. Hieraus folgen mehrere Teilaufgaben:
  - Das Datenmodell des Identity Repository muss entsprechend erweitert werden (vgl. Change Management in Abschnitt 4.8). Sofern hierfür keine Orientierung an Standards möglich ist, sollte der bisher organisationsintern angewandte Modellierungsstil beibehalten werden, d. h. dass entsprechende Vorgaben durch die Föderation nur dann direkt im Identity Repository umgesetzt werden sollten, wenn die Nachhaltigkeit des resultierenden Datenmodells sichergestellt ist. Es muss vermieden werden, mittelfristig ein Flickwerk aus Datenmodellen verschiedener Föderationen

zu erhalten, dessen Redundanzfreiheit und organisationsinterne Verwendbarkeit gefährdet sind.

- Gegebenenfalls sind die Datenquellen so anzupassen, dass dort die neu benötigten Benutzerattribute erfasst und gepflegt werden. Im Allgemeinen bedeutet dies auch einen organisatorischen Eingriff, da beispielsweise Antragsformulare anzupassen und Sachbearbeiter entsprechend zu schulen sind, insbesondere wenn die Korrektheit der zusätzlichen Daten sichergestellt werden muss. Ein szenarienspezifisch zu konzipierender Aspekt ist hierbei die gegebenenfalls notwendig werdende Ergänzung des bereits vorhandenen Datenbestands um die neuen Attribute.
- Die Konnektoren zwischen den Datenquellen und dem Identity Repository sind entsprechend anzupassen; dies umfasst insbesondere die Implementierung ggf. notwendiger Datenkonvertierungen sowie geeigneter Plausibilitätsprüfungen.
- Die Self Services sind typischerweise ebenfalls um die neuen Attribute zu erweitern. Dies stellt insbesondere eine gängige Methode dar, die Ergänzung der Daten an Bestandsnutzer zu delegieren, so dass diese z. B. erst nach Eintragen der Daten die entsprechenden Dienste FIM-basiert nutzen können.

Hingegen sind keine Anpassungen notwendig, wenn von der Föderation benötigte Daten aus dem vorhandenen Datenbestand abgeleitet werden können; hierzu kann der beschriebene Identitätsdatenkonverter eingesetzt werden.

- Sicherstellen der geforderten Datenqualität. Analog zu den bislang nicht vorgesehenen Datenfeldern kann der Fall eintreten, dass auf die Qualität der Daten, z. B. im Hinblick auf die Aktualität und Vollständigkeit, organisationsintern weniger Wert gelegt wurde als im Rahmen von Föderations-SLAs vereinbart wird. Entsprechend können sehr aufwendige Prozessanpassungen und umfangreiche Initialkorrekturen notwendig werden.

Die folgenden weiteren Maßnahmen bezüglich der Benutzerdaten sind bereits FIM-zielgerichtet, betreffen jedoch noch I&AM-Komponenten:

- Das im Identity Repository verwendete Datenmodell muss ggf. um die Möglichkeit zur Hinterlegung von Autorisierungsinformationen, wie sie von einem Privilege Management System benötigt werden, erweitert werden. Insbesondere kann es notwendig werden, aus Attributwerten ableitbare Berechtigungen explizit als Autorisierungsinformationen zu speichern; in diesem Fall muss die Konsistenz beider Varianten sichergestellt werden, beispielsweise über einen Konnektor, dessen Quell- und Zielsystem dasselbe Identity Repository ist (sog. **Loopback-Konnektor**).
- Für benötigte Benutzerattribute, die nicht erfasst werden können oder bewusst nicht erfasst werden sollen, können Verweise auf geeignete Attribute Authorities definiert werden; im Hinblick auf die Anforderung [ORG-Verweisgüte] sind geeignete Maßnahmen zu treffen, um für die Qualität der von der AA gelieferten Daten entsprechend bürgen zu können.

Sofern die folgenden beim Einsatz von FIM benötigten Komponenten noch nicht lokal eingesetzt wurden, müssen sie entsprechend nachgerüstet werden:

- Single Sign-On System: Auch wenn die organisationsinternen Dienste nicht SSO-fähig sind, wird für die Benutzerauthentifizierung im Rahmen von FIM die Authentifizierungsfunktionalität eines SSO-Systems benötigt. Gegebenenfalls muss es deshalb eingeführt werden, auch ohne dass lokale Dienste angeschlossen werden.

  Bezüglich der Anforderung [SEC-Benutzerauthentifizierung] ist zu berücksichtigen, dass das implementierte SSO-System alle im Rahmen der Föderation benötigten Authentifizierungsarten unterstützen muss, ggf. also auch Alternativen zur Verwendung von Benutzername/Passwort-Kombinationen.

- Analog sollte ein organisationsinternes Privacy Management System zum Einsatz kommen. Auch wenn im Kontext von FIM primär der Obligation Monitor des PMS benötigt wird, schafft der konsequente organisationsinterne Einsatz eines PMS eine brauchbare Vertrauensbasis gegenüber den Benutzern hinsichtlich der organisationsübergreifenden Weitergabe ihrer Daten.

Vor der im folgenden Abschnitt beschriebenen Inbetriebnahme der FIM-Komponenten ist darüber hinaus die Teilnahme an einer von der Föderation akzeptierten Public-Key-Infrastruktur sicherzustellen. Insbesondere Serverzertifikate neu hinzukommender Komponenten müssen von der CA einer solchen PKI ausgestellt werden.

4.6.2. Migration bei IDPs und AAs

Die Installation, der Test, die Integration und die Inbetriebnahme der FIM-Komponenten orientieren sich stark an den in Abschnitt 4.5.4 gezeigten Abhängigkeiten der Komponenten.

Die nachfolgende Aufzählung der ersten Aktivitäten bezieht sich auf die in Abbildung 4.23 eingezeichnete Schicht 4:

- Die **Installation des FIM Privacy Management Systems** wird primär durch die Konfiguration der Voreinstellungen für die Attribute Release Policies geprägt (vgl. Anforderung [DSA-DefaultARPs]). Obwohl Benutzer diese Policies über das ARP-Managementfrontend einsehen können, ist es in der Regel erforderlich, sie in Prosa zusätzlich in die typischerweise bereits vorhandenen Datenschutzerklärungen aufzunehmen.

  Der Aufwand bei der Inbetriebnahme dieser Komponente hängt weiterhin davon ab, ob ein organisationsinternes PMS vorhanden ist, dessen Obligation Monitor verwendet werden kann. Falls diese Voraussetzung nicht erfüllt ist, müssen entsprechende Bestandteile des FIM Privacy Management Systems zusätzlich in Betrieb genommen werden.

  Ebenso ist zu berücksichtigen, dass für das Management der ARPs durch Benutzer und (ggf. dezentrale) Administratoren mindestens zwei zusätzliche Policy Administration Points hinzukommen, die nicht nur zu betreibende, typischerweise webbasierte Dienste darstellen, sondern durch ihre Anwender einfach aufgerufen werden können müssen. Eine Integration in die gewohnten Umgebungen wie Self Services oder webbasierte Administrationsoberflächen setzt mindestens die Ergänzung entsprechender HTML-Links voraus; Ziel sollte jedoch die transparente Integration in die Self Services oder zumindest mit dem SSO-System sein.

- Die **Inbetriebnahme des Identitätsdatenkonverters** erfordert als wesentlichen Konfigurationsschritt die Implementierung der Konvertierungsregeln zwischen dem lokalen und z. B. dem föderationsweiten Schema. Diese kann entfallen, wenn bereits bekannt ist, dass im Rahmen des Federation Schema Correlation Services geeignete Konvertierungsregeln angeboten werden. In beiden Fällen sollten insbesondere im Hinblick auf das Change Management Testdatensätze und -programme zur Verfügung stehen, anhand derer die korrekte Funktion regelmäßig automatisch überprüft werden kann.
- Die **Installation des FIM-Interaktionsdienstes** weist Parallelen mit der Konfiguration des FIM Privacy Management Systems auf, da auch hierbei neue webbasierte Dienste eingeführt werden, deren zu realisierender Funktionsumfang zum Teil von den Möglichkeiten abhängt, die von den Self Services bereits geboten werden. Für die Teilfunktionalität des dynamischen Anlegens von ARPs muss eine Verbindung zum Policy Repository des FIM Privacy Management Systems geschaffen werden, woraus sich eine zu beachtende zeitliche Abhängigkeit für Tests und Inbetriebnahme ergibt; dabei ist zu berücksichtigen, dass der FIM-Interaktionsdienst erst in der nächsten Phase ausführlich getestet werden kann, wenn die IDP-Software und der Gateway zum lokalen Datenbestand verfügbar sind.
- Die **Schnittstelle zu den Föderationsmetadaten** ist in Betrieb zu nehmen. Analog zum FIM-Interaktionsdienst ergibt sich für die zukünftige Integration föderationsweiter ARPs die Notwendigkeit eines Schreibzugriffs auf das Policy Repository des FIM Privacy Management Systems, dessen Funktionieren mit Testpolicies überprüft werden kann.

Die Arbeiten an der Schnittstelle zu den Föderationsmetadaten ist ein aus technischer Sicht geeigneter Zeitpunkt für die **Aufnahme der Organisation in die Föderation**. Diese besteht wie bereits beschrieben auf technischer Ebene in der Erweiterung der Föderationsmetadaten um die grundlegenden Informationen über den neuen IDP bzw. die neue AA, so dass ggf. die vollständigen Metadaten bereits automatisiert über die Schnittstelle zu den Föderationsmetadaten übermittelt werden können.

Wie Schicht 5 in Abbildung 4.23 zeigt, kann parallel zur mit der technischen Aufnahme in die Föderation verbundenen Wartezeit der Gateway zum lokalen Datenbestand in Betrieb genommen werden. Der Konfigurationsaufwand ist hierbei minimal, da sich diese Komponente primär auf den Identitätsdatenkonverter abstützt, der in dieser Phase wiederum an einen Federation Schema Correlation Service angeschlossen werden kann.

Die in Schicht 6 dargestellte Produktivführung des IDP bzw. der AA gliedert sich in die folgenden Teilschritte:

1. Die in den Föderationsmetadaten enthaltenen **Policies** müssen in das FIM Privacy Management System übernommen werden; dieser technische Prozess ist zu automatisieren, damit Aktualisierungen immer zeitnah durchgeführt werden.
2. Die **IDP-Software** muss in Betrieb genommen werden; wie in Abschnitt 4.4.1.7 erläutert müssen hierbei insbesondere die Accountingoptionen konfiguriert werden, während die Einbettung in die übrige Infrastruktur keinen großen Aufwand darstellt.
3. Im Fall von neuen IDPs sind vorhandene **IDP Discovery Services** darauf zu überprüfen, ob sie den IDP bereits in ihrer Auswahlliste anbieten; dieser Prozess vereinfacht

sich, wenn ein föderationsweiter IDP Discovery Service eingesetzt wird und wird aufwendiger, wenn SPs diese Funktionalität selbst implementieren. Die ermittelte Dauer, bis der neue IDP in jeder Liste von IDPs erscheint, lässt Rückschlüsse auf die Metadatenaktualisierungsfrequenzen der anderen Föderationsteilnehmer zu, die beim späteren Change Management entsprechend berücksichtigt werden sollte.

Die Migration ist zu diesem Zeitpunkt so weit fortgeschritten, dass die Gesamtfunktionalität auch aus Benutzerperspektive getestet und bei Erfolg für alle Benutzer freigegeben werden kann.

Die Funktionalität kann auf Basis der in Schicht 7 eingezeichneten Komponenten noch erweitert werden:

- Die Einführung des **Notifications-Konnektors** ermöglicht das SP-seitige Abonnieren von Benachrichtigungen über Benutzerattributänderungen im Unterschied zu individuellen Lesezugriffen. Sobald diese Funktionalität zum Standardumfang von FIM-Protokollen gehören wird, ist diese Komponente nicht mehr als optional zu betrachten, sondern kann auf Schicht 5 angesiedelt werden und beispielsweise im Rahmen des Gateways zum lokalen Datenbestand als bidirektionaler Konnektor realisiert werden.
- Die Implementierung eines **Privilege Management Systems** ermöglicht dynamische Autorisierungsbestätigungen, die über die Möglichkeiten der statisch im Identity Repository hinterlegten Autorisierungsdaten hinausgehen. In Abhängigkeit von der Nutzungsfrequenz von expliziten Autorisierungsbestätigungen kann die Realisierung dieser Komponente bereits auf Schicht 5 erforderlich sein; in der bislang gängigen Praxis sind Autorisierungsbestätigungen jedoch noch häufig optional, da Autorisierungen entweder SP-seitig aus Benutzerattributen abgeleitet werden oder für verteilte Autorisierung bereits separate Infrastrukturen geschaffen wurden. Beispielsweise ist die Verwendung von SAML Autorisierungsbestätigungen in Shibboleth noch gar nicht vorgesehen.

Darüber hinaus sind die in den Abschnitten 4.7 und 4.8 diskutierten Aspekte zu berücksichtigen.

4.6.3. Vorbereitungen und Migration seitens der Service Provider

Wie bereits aus Abbildung 4.24 hervorgeht, sind die Abläufe bei SPs aufgrund der Komponentenabhängigkeiten ähnlich zu denen bei IDPs und zudem durch die geringere Anzahl FIM-spezifischer Komponenten vereinfacht.

Die Vorbereitungsphase wird weniger durch einen technischen, sondern vielmehr durch den organisatorischen Aufwand bestimmt; beispielsweise ist sicherzustellen, dass die beteiligten IDPs und AAs alle benötigten Benutzerattribute in angemessener Qualität liefern können und z. B. das Einholen der Zustimmung zu den Benutzungsrichtlinien unterstützen. Diese Aspekte sind letztendlich ausschlaggebend dafür, ob ein Dienst bereits über FIM angeboten werden kann oder weiterhin auf lokale Registrierungsverfahren gesetzt werden muss. Die Alternative, dass das lokale I&AM-System und die Dienste so angepasst werden, dass sie mit weniger Daten über Benutzer als bisher betrieben werden können, ist in der Regel nicht mit

angemessenem Aufwand realisierbar oder für den SP zu unattraktiv; ein Kompromiss besteht in der Bereitstellung entsprechender AAs.

Die Migration selbst erfolgt analog zu IDPs; der einzige wesentliche Unterschied neben dem Fehlen der nur IDP-seitig benötigten FIM-Komponenten besteht in der Umsetzung der Attribute Acceptance Policies, die wie erläutert stärker der Aufrechterhaltung der Datenqualität als dem Datenschutz dienen.

Die Einspeisung der über FIM bezogenen Daten ins lokale I&AM-System ermöglicht einen transparenten Parallelbetrieb mit dem bisherigen Registrierungsverfahren. Im einfachsten Fall sind somit keine weiteren Anpassungen notwendig; die Nutzung weiterer FIM-Funktionalitäten wie organisationsübergreifendes Single Sign-On und dezentrale Autorisierungsinfrastrukturen setzt jedoch die FIM-Unterstützung durch die Dienste, insbesondere das SP-seitig eingesetzte Single Sign-On System, voraus.

4.6.4. Vorbereitungen seitens Föderationsverwaltung und Trusted Third Parties

Bei der Föderationsverwaltung ist zwischen ihren technischen bzw. organisatorischen Aufgaben zu unterscheiden. Die technische Kernaufgabe besteht in der Verwaltung der Föderationsmetadaten; bei der Aufnahme neuer Föderationsteilnehmer beschränkt sich diese auf die Eintragung des entsprechenden Kommunikationsendpunkts, da die übrigen Metadaten automatisiert ausgetauscht werden können.

Die übrigen Vorbereitungen hängen stark vom Organisationsmodell der Föderation ab und werden hier deshalb nur stichpunktartig skizziert:

- Es muss entschieden werden, ob die jeweilige Organisation als neuer Teilnehmer in die Föderation aufgenommen wird. Dies umfasst einerseits die Überprüfung der grundlegenden **Qualifikation der Organisation für die Teilnahme**, beispielsweise auf Basis bereit bestehender geschäftlicher Beziehungen zu Bestandsmitgliedern, andererseits muss beispielsweise bei neuen IDPs die Einhaltung von Datengüteparametern sichergestellt werden.
- Das **föderationsweite Datenmodell** muss festgelegt werden. Die Föderationsverwaltung hat hierbei typischerweise die Aufgabe, die Spezifikation zu koordinieren sowie das entstandene Schema zu versionieren und in der Föderation zu veröffentlichen. Zwangsweise orientiert sich das Datenmodell primär an den von den Service Providern benötigten Daten und muss auch im Change Management entsprechend berücksichtigt werden, d. h. es kann sich u. a. auch mit dem Hinzukommen neuer Mitglieder ändern.
- Analog zum föderationsweiten Datenmodell müssen die **föderationsweiten Attribute Release und Attribute Acceptance Policies** spezifiziert werden. Ihr Umfang variiert einerseits mit der Stellung des Föderationsverwaltung in der Föderation und andererseits mit dem von den Föderationsteilnehmern angestrebten Automatisierungsgrad, der erhöht wird, je weniger Policies lokal gepflegt werden müssen.

Die Föderationsverwaltung bildet zudem häufig die **Anlaufstelle für Support** der Föderationsmitglieder und Fehlerbehandlung. Sie stellt exemplarische Konfigurationen für die eingesetzten FIM-Komponenten bereit und überwacht den Status der beteiligten Systeme. Da sich

die hierfür relevanten Konfigurationsaspekte dieser Werkzeuge aus den Föderationsmetadaten ableiten lassen, sind keine weiteren Vorbereitungsmaßnahmen zu treffen.

Analog gilt für weitere Dienste wie den IDP Discovery Service und den Federation Schema Correlation Service, dass aufgrund der automatisierten Ableitung aus den Föderationsmetadaten keine manuellen Eingriffe bei der Aufnahme neuer Föderationsmitglieder notwendig sind.

4.6.5. Berücksichtigung mehrerer Rollen pro Organisation

Ein Sonderfall liegt vor, wenn eine Organisation einer Föderation sowohl als IDP als auch als SP beitreten möchte. Beide Rollen könnten dabei prinzipiell auch unabhängig voneinander betrachtet und sequentiell umgesetzt werden. In diesem Fall empfiehlt sich, zuerst die Ausprägung als IDP zu realisieren; diese ist einerseits komplexer als die Instanziierung der SP-seitigen Architektur und legt somit auch den Grundstein für die SP-spezifischen Komponenten, andererseits wird durch diese Reihenfolge die sofortige transparente Nutzung der Dienste mittels FIM auch für die eigenen Benutzer ermöglicht.

Es bietet sich jedoch an, die jeweiligen IDP- bzw. SP-spezifischen Komponenten auf den Schichten 4 und 5 parallel zu installieren, um Synergien bezüglich der folgenden Konfigurations- und Testaspekte zu nutzen:

- Die Schnittstelle zu den Föderationsmetadaten wird sowohl von IDP- als auch SP-Software benötigt und speist die föderationsweiten Attribute Release bzw. Acceptance Policies ein.
- Die Konfiguration des Gateways zum lokalen Datenbestand bzw. des Konnektors zum lokalen I&AM-System erfolgt nahezu identisch für dasselbe Identity Repository.
- Insbesondere beim Fehlen föderationsweiter Vorgaben können die lokalen Attribute Release und Acceptance Policies auf die eigenen Bedürfnisse zugeschnitten werden und ermöglichen somit einen sanften Übergang zum FIM-basierten Datenaustausch.
- Das manuelle Aktualisieren der Föderationsmetadaten kann zu einem einzigen Schritt zusammengefasst werden.

Über diese Initialkonfiguration hinausgehende Aktivitäten wie die Aufnahme einer Organisation in mehrere Föderationen werden im Rahmen des Change Managements in Abschnitt 4.8 diskutiert.

4.7. Sicherheitsinfrastruktur

In diesem Abschnitt werden die Sicherheitsmaßnahmen für eine integrierte I&AM- und FIM-Infrastruktur diskutiert; die Grundlage hierfür bildet die Erläuterung der Sicherheitsaspekte bei der Beschreibung der einzelnen Komponenten. Die inhärenten Sicherheitseigenschaften der eingesetzten FIM-Protokolle wurden bereits in anderen Arbeiten untersucht und werden hier nicht vertieft (vgl. [HSN05]).

Eingangs werden in Abschnitt 4.7.1 einige FIM-spezifische Angriffsmodelle erläutert, die für die Problemstellung sensibilisieren sollen und zur Bewertung der möglichen Lösungen herangezogen werden können; da FIM noch relativ neu und wenig verbreitet ist, muss davon ausgegangen werden, dass zukünftig noch weitere Angriffsarten hinzukommen werden.

In Abschnitt 4.7.2 wird auf Schutzmaßnahmen auf Netzwerkebene eingegangen; die Schwerpunkte liegen hierbei auf der Bildung von Sicherheitszonen sowie der Selektion und Positionierung von Firewalls. Abschnitt 4.7.3 resümiert im Anschluss die Sicherheitsmaßnahmen auf Applikationsebene mit dem Ziel eines Gesamtüberblicks aus Sicherheitsperspektive.

In den Abschnitten 4.7.4 und 4.7.5 werden abschließend mit dem Auditing und der technischen Umsetzung von Datenschutzregelungen zwei in der FIM-Praxis unerlässliche Aufgaben diskutiert.

4.7.1. Spezifische Angriffsmodelle und Risiken

Die Gefahren durch die Ausnutzung von nicht FIM-spezifischen Angriffen wie Man-in-the-middle-Attacken, Fälschen von DNS-Einträgen und Verwenden unsicherer Verschlüsselungsverfahren werden beispielsweise in den Liberty Alliance Privacy and Security Guidelines [LAPRIV] beschrieben und hier nicht erörtert. Vielmehr werden die FIM-Spezifika kurz dargestellt und einige neue Angriffsmodelle skizziert sowie deren jeweilige Risiken grob abgeschätzt.

Für die beiden primären organisatorischen Rollen ergeben sich durch FIM neben vielen Vorteilen insbesondere die folgenden Sicherheitsrisiken:

- Identity Provider müssen ihren vormals exklusiv **internen Datenbestand** für Zugriffe von außen öffnen. Hierbei droht die inhärente Gefahr, dass zu viele Daten nach außen gegeben werden. Dies stellt einerseits den Worst Case aus Datenschutzsicht und damit auch eine wahrscheinliche Beschädigung der Reputation der Organisation dar; andererseits kann die Auswahl und Zusammensetzung der ihm angehörenden Personen auch die Geschäftsgrundlage des IDPs darstellen – Beispiele hierfür sind die sogenannten Social Networks und Expert Communities (vgl. [JHF03]).
- Service Provider müssen sich auf die von den IDPs und AAs gelieferten Angaben verlassen. Mit der Einführung von FIM entfällt insbesondere die im Business-to-Business-Bereich bislang übliche Überprüfung von amtlichen Ausweisen bei der Beantragung von Berechtigungen für B2B-Dienste. Damit ist im Worst Case unklar, ob die Person, deren vollständiger Datensatz vorliegt, überhaupt existiert oder fingiert ist.

Beide genannten Risiken betreffen in ihrem Kern das erhöhte Vertrauen zwischen IDP und SP, das Voraussetzung für FIM und somit ein möglicher Angriffspunkt ist. Als Angreifer, aber auch als Opfer kommen dabei IDPs, SPs, Benutzer und Externe in Frage.

4.7.1.1. Identity Provider als Angreifer

Der IDP kann als Angreifer gegenüber SPs agieren, wenn beispielsweise seine Systeme kompromittiert wurden oder Administratoren ihre Berechtigungen missbrauchen.

Die bereits angedeuteten offensichtlichsten Missbrauchsarten sind das **Vortäuschen von in der Realität nicht existierenden Identitäten** und die **Manipulation von Berechtigungen** mit dem Ziel, die Nutzung von Diensten zu erschleichen, um beispielsweise Industriespionage betreiben zu können.

Sofern ein IDP bereits eine große Menge regulärer Benutzer hat, liegt die Gefährlichkeit dieser Angriffsarten in der Schwierigkeit, sie zeitnah aufzudecken. Plausibel erscheinende Datensätze fallen bei stichprobenartigen Überprüfungen nicht auf und eventuell notwendige Genehmigungsprozesse für Berechtigungen können von Administratoren durch direkte Schreibzugriffe auf die Datenbestände in der Regel mit minimalem Aufwand umgangen werden.

Die mit diesen Angriffen verbundenen Risiken hängen von den in der Föderation nutzbaren Diensten ab; an ihnen orientieren sich ebenfalls die zu realisierenden Schutzmechanismen, die sich jedoch stärker organisatorisch als technisch auswirken, beispielsweise durch **detailliertes Auditing** oder das **Vier-Augen-Prinzip für administrative Eingriffe**.

Aus Datenschutzperspektive sind darüber hinaus Angriffe auf die Benutzer möglich, da der IDP zur Auswertung der Attribute Release Policies umfassende Informationen darüber erhält, welcher SP wann zu welchem Zweck welche Daten angefordert hat; im Rahmen der Unterstützung der informationellen Selbstbestimmung der Benutzer kann dies sogar gewünscht sein. Offensichtlich muss es jedoch Regelungen geben, die eine unerwünschte Auswertung dieser Daten durch den IDP selbst unterbinden.

Da die IDP-internen Abläufe von außen kaum kontrolliert werden können, ist ein Schutz gegen diese **Eingriffe in die Privatsphären der Benutzer** derzeit nicht realisierbar; analog zur von Mont in [CMP05] vorgeschlagenen Sicherstellung der Erfüllung SP-seitiger Obligationen wäre denkbar, zukünftig zertifizierte Software einzusetzen, die keine unprotokollierten Zugriffe erlaubt und deren Unversehrtheit über von außen überprüfbare Hardwarelösungen wie Trusted Platform Modules (TPM) garantiert wird. Es ist jedoch offen, ob sich Softwarehersteller und IDPs auf den damit verbundenen Aufwand einlassen werden, sofern diese Eigenschaften nicht beispielsweise gesetzlich gefordert werden.

4.7.1.2. Service Provider als Angreifer

Der Einsatz von FIM beugt einigen klassischen SP-seitigen Angriffen partiell vor, da beispielsweise durch Single Sign-On und Single Logout die Nutzungszeiten nachgewiesen und SP-seitig gefälschte Accountinginformationen somit verhindert werden können. Auf andere Gefahren wie die unerwünschte, absichtliche Weitergabe von Benutzerdaten an Dritte hat FIM hingegen keinen direkten Einfluss.

Eine mit FIM einhergehende Missbrauchsmöglichkeit ist jedoch das **Abrufen möglichst umfangreicher personenbezogener Daten** von den IDPs, beispielsweise unter Ausnutzung zu freizügig konfigurierter Attribute Release Policies. Dies kann einerseits Versuche umfassen, mehr als die zur Diensterbringung notwendigen Attribute über Benutzer abzufragen, andererseits auch auf das Auslesen von Informationen über Personen abzielen, die keine bzw. noch keine Benutzer des Dienstes sind.

In Abschnitt 4.4.1.4 wurde bereits diejenige Variante dieses Angriffs, in der ein SP kompromittiert wurde und selbst den Einflüssen eines externen Angreifers ausgesetzt ist, erläutert. Es muss jedoch beachtet werden, dass insbesondere in Privatkundenszenarien auch die SPs

selbst ein starkes Interesse daran haben, möglichst viele Informationen über ihre Benutzer zu akquirieren, um beispielsweise gezielte personalisierte Angebote erstellen zu können.

Die Wahrscheinlichkeit eines solchen Angriffs muss deshalb als sehr hoch eingeschätzt werden; da einmal herausgegebene Daten potentiell unkontrolliert zirkulieren und nicht zurückgerufen werden können, muss der Fokus auf Präventionsmaßnahmen liegen.

4.7.1.3. IDP-seitige Benutzer als Angreifer

Typischerweise zielen Angriffe von Benutzern entweder auf das **Erlangen zusätzlicher Berechtigungen** oder das **Abstreiten der Dienstnutzung** sowie beispielsweise damit verbundener Kosten ab.

Nur durch die FIM-basierte Übertragung von Personendaten entstehen hier keine neuen Missbrauchsmöglichkeiten, sofern die Korrektheit der übertragenen Daten sichergestellt werden kann. Im Hinblick auf Authentifizierungs- und Autorisierungsbestätigungen sind jedoch die folgenden Aspekte zu berücksichtigen:

- Authentifizierungsbestätigungen verlagern die Überprüfung der Benutzeridentität vom SP zum IDP. Falls eine Person die Nutzung eines Dienstes nachträglich abstreitet, muss somit neben der Person und dem SP auch der IDP an der Klärung des Vorfalls mitwirken. Dadurch wächst einerseits auch die Bedeutung starker Authentifizierungsverfahren und beispielsweise entsprechender Passwortpolicies, die „sichere“ Passwörter erzwingen sollen; andererseits werden auch neue **föderationsweite Korrelationsverfahren z. B. für Protokolldateien** benötigt, um beispielsweise erkennen zu können, dass der angeblich selbe Benutzer die Dienste gleichzeitig von verschiedenen Standorten aus genutzt hat.
- Der reine Gebrauch von Autorisierungsbestätigungen ohne Attributsauskünfte entspricht SP-seitig einer anonymen Dienstnutzung, wobei dem IDP vertraut wird, dass nur wirklich dazu berechtigte Benutzer eine entsprechende Autorisierungsbestätigung erhalten. Da der Benutzer auf die Autorisierungsentscheidungen – abgesehen von möglichen herkömmlichen Angriffen auf die entsprechenden Systeme – keinen Einfluss hat, entstehen diesbezüglich auch keine neuen Risiken im Hinblick auf die Überschreitung der eigenen Berechtigungen. Da über den Benutzer außer bezüglich seiner Autorisierung keine Informationen vorliegen und dieser sich im Dienst **quasi anonym** bewegen kann, können Schwierigkeiten bei der **Verfolgung von Missbrauchsfällen** aufkommen.

Darüber hinaus kann der Benutzer die über seinen Client mittelbar abgewickelte Kommunikation manipulieren; wie bereits erläutert sollten die von den FIM-Protokollen zur Verfügung gestellten Signatur- und Verschlüsselungsmechanismen genutzt werden, um ungewollte Änderungen der Nutzdaten erkennen zu können.

4.7.1.4. Externe Angreifer

Für externe Angreifer stellen die FIM-Komponenten, die auch außerhalb einer Organisation erreichbar sein müssen, eine breite Angriffsfläche für herkömmliche Angriffsarten dar; die

Schutzmaßnahmen auf Netzwerkebene, die in Abschnitt 4.7.2 diskutiert werden, haben deshalb nach wie vor eine Berechtigung.

Für das Identity Management spezifische Angriffe zielen in der Regel darauf ab, dass sich der Angreifer als andere Person ausgibt bzw. Dienste unter fremdem Namen nutzt und werden allgemein als **Identitätsdiebstahl** (engl. *identity theft*) bezeichnet (vgl. [MKT05]). Aufgrund des organisationsübergreifenden Single Sign-Ons und der damit verbundenen Nutzung von mehr als einem Dienst werden Angriffe wie das Knacken von Benutzerpasswörtern noch attraktiver. Weitere Angriffe werden zudem dadurch erleichtert, dass die Umleitung vom SP über den IDP Discovery Service zum IDP insbesondere neue und technisch weniger versierte Benutzer leicht verwirren kann; sofern diese Kommunikationsprozesse im Rahmen eines Man-in-the-middle-Angriffs beeinflusst werden können, fällt den Benutzern eine eingeschleuste Umleitung auf eine vom Angreifer präparierte Webseite möglicherweise nicht auf.

Positiv zu vermerken ist jedoch, dass Designschwächen früherer Protokolle im FIM-Umfeld konsequent vermieden werden; beispielsweise werden sogenannte Replay-Attacken, bei denen der Angreifer im Netzwerkverkehr mitgeschnittene Datenpakete erneut an den Server schickt, dadurch vermieden, dass SAML Assertions nicht nur eine begrenzte Gültigkeitsdauer haben, sondern auch eine eindeutige Seriennummer, die nur einmal verwendet werden darf.

4.7.2. Schutzmaßnahmen auf Netzwerkebene

Auf die grundsätzlichen Möglichkeiten zum Einsatz von Paketfilterfirewalls wurde bereits bei der Beschreibung der einzelnen Komponenten eingegangen; die in den Abbildungen eingezeichneten Firewallsymbole stellten dabei die logische Platzierung von Firewalls dar. Gesamtheitlich betrachtet wäre es jedoch sehr ineffizient, für jede I&AM- bzw. FIM-Komponente einen oder mehrere dedizierte Firewalls betreiben zu müssen.

Nachfolgend wird deshalb eine konkrete Strategie zum Aufbau der Netzwerksicherheitsinfrastruktur für I&AM- und FIM-Lösungen beschrieben. In Abschnitt 4.7.2.1 wird die Zuordnung der Komponenten zu verschiedenen Sicherheitszonen erläutert; die Selektion und Positionierung von Firewallkomponenten wird in Abschnitt 4.7.2.2 beschrieben.

4.7.2.1. Zonenbildung

Die Einordnung von Servern in Sicherheitszonen erfolgt üblicherweise auf Basis ihres Schutzbedarfs und ihres Kommunikationsverhaltens; dabei sind zwangsweise Kompromisse zu finden, wenn ein Dienst beispielsweise einen sehr hohen Schutzbedarf hat, aber über das Internet erreichbar sein soll und somit einer potentiell sehr großen Anzahl von Angriffen ausgesetzt ist.

Die erläuterten FIM-Komponenten lassen sich generell in die folgenden vier Schutzzonentypen einteilen:

- **Zonentyp 1 – Interne Server**: Zu dieser Kategorie gehören alle I&AM- und FIM-Komponenten, auf die Benutzer nicht direkt zugreifen und die nicht mit anderen Organisationen kommunizieren. Hierzu gehören die folgenden
  - I&AM-Komponenten:

    - Identity Repository; hierfür wird häufig eine eigene Instanz dieses Zonentyps verwendet, um den zentralen Datenbestand so weit wie möglich abzuschirmen.
    - Konnektoren
    - Quellsysteme, sofern diese nicht zu einer der nachfolgenden Kategorien gehören.
    - Privacy Management System (PAP, PDP, PR und Obligation Monitor)
  - FIM-Komponenten:
    - Privilege Management System (PAP, PDP, PEP und PR), sofern keine Kommunikation mit externen Organisationen notwendig ist; das PMS ist sonst dem Zonentyp 4 zuzuordnen.
    - Notifications-Konnektor
    - SP-seitiger Konnektor zum lokalen I&AM-System
    - Komponente zur Auswertung von Attribute Acceptance Policies
    - IDP-seitige Datenbasis für die Protokollierung von Zugriffen und Wünschen von SPs nach Aktualisierungsbenachrichtigungen, sofern getrennt von der IDP-Software realisiert.

- **Zonentyp 2 – Systeme mit Benutzerinteraktion**: Diesem Zonentyp werden alle Komponenten zugeordnet, mit denen Benutzer interagieren; FIM-Komponenten, mit denen andere Organisationen nicht nur mittelbar über den Benutzerclient, sondern auch direkt kommunizieren können, sind hingegen dem nächsten Zonentyp zuzuordnen. Zu dieser Zone gehören:
  - Dienste (Interne Dienste bei IDPs)
  - Self Services
  - Single Sign-On System
  - IDP Discovery Service (die vom SP initiierte Kommunikation findet ausschließlich mittelbar über den Benutzerclient statt)
  - FIM-Interaktionsdienst
  - FIM Privacy Management System
  - IDP-seitiger Gateway zum lokalen Datenbestand

- **Zonentyp 3 – Systeme mit ein- und ausgehenden organisationsübergreifenden Verbindungen**: In diese Zone gehören alle Komponenten, mit denen andere Föderationsteilnehmer direkt oder mittelbar über den Benutzerclient kommunizieren können. Sie umfasst:
  - IDP-Software
  - SP-Software
  - Dienste (Über Internet nutzbare Dienste bei SPs)
  - Schnittstelle zu den Föderationsmetadaten, die im Push-Verfahren an die Föderationsteilnehmer ausgeliefert werden, sowie die Föderationsverwaltung selbst.
  - Federation Schema Correlation Service (FSCS)

- **Zonentyp 4 – Systeme mit ausschließlich ausgehenden organisationsübergreifenden Verbindungen**: Systeme in dieser Zone müssen zwar nicht von außen

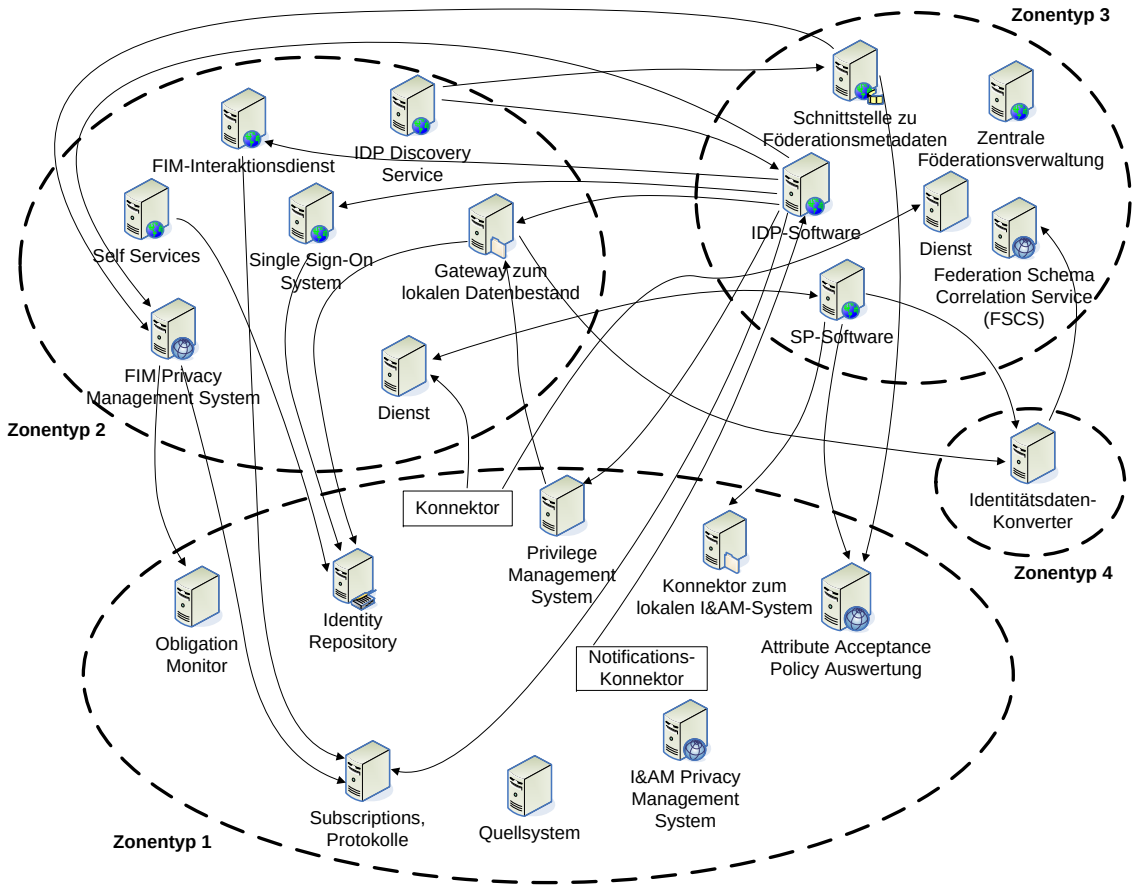


Abbildung 4.25.: Zonentypen und *zonenübergreifende* Kommunikationsbeziehungen

erreichbar sein, aber die Kommunikation mit der Außenwelt initiieren können. Hierzu gehört derzeit lediglich der Identitätsdatenkonverter, der mit dem FSCS Kontakt aufnehmen können muss.

In Szenarien, in denen die Benutzer keinen organisationsinternen lokalen Netzwerken zugeordnet werden können, sondern auf die Dienste über das Internet zugreifen, können die Zonentypen 2 und 3 prinzipbedingt hinsichtlich der möglichen Schutzmaßnahmen nicht klar differenziert werden.

Es ist durch **mehrfache Instanziierung eines Zonentyps** möglich, die Struktur noch weiter zu verfeinern. In der Praxis ist insbesondere davon auszugehen, dass bei der Einführung von FIM auf Basis eines bereits bestehenden I&AM-Systems mindestens Zonentyp 1 neu instanziiert wird, um eine Trennung von den bereits bestehenden Komponenten zu erreichen; die anzuwendenden Schutzmaßnahmen bleiben jedoch dieselben.

Abbildung 4.25 zeigt die Zonenbildung sowie die zonenübergreifenden Kommunikationsabläufe.

4.7.2.2. Firewallauswahl und -positionierung

Wie bereits bei der Erläuterung der einzelnen Komponenten erwähnt, können primär Paketfilterfirewalls und sekundär Application Level Gateway Firewalls (ALGs) effizient zum Schutz der I&AM- und FIM-Infrastruktur eingesetzt werden. ALGs operieren auf Anwendungsebene und sind deshalb eigentlich Abschnitt 4.7.3 zuzuordnen; da sie Firewalls darstellen und in der Praxis häufig von den auch für Paketfilterfirewalls zuständigen Abteilungen betreut werden, wird bereits in diesem Abschnitt auf sie eingegangen.

Das hier vorgestellte Konzept sieht vor, dass insbesondere die **Zonengrenzen** durch Paketfilterfirewalls geschützt werden und darüber hinaus der Zugang zu besonders schützenswerten Komponenten über ALGs kanalisiert wird:

- Paketfilterfirewalls sorgen dafür, dass ein- bzw. ausgehende Verbindungen nur zu bzw. von ausgewählten Diensten (typischerweise identifiziert durch IP-Adresse und TCP-Port) erlaubt werden. Dies entspricht einem **Whitelisting-Ansatz**, d. h. alle nicht explizit erlaubten Verbindungen sind verboten; beispielsweise muss die Maschine, auf der die webbasierten, über HTTPS ansprechbaren Self Services laufen, von allen Benutzerclients aus nur auf Port 443/TCP (Standardport für HTTPS) erreichbar sein.
- ALGs nehmen darüber hinaus eine **Inhaltsanalyse der Nutzdaten** vor und können beispielsweise unerwünschte Anfragen verwerfen; das Erstellen und Verarbeiten komplexer Regelsätze ist jedoch deutlich aufwendiger als bei Paketfilterfirewalls und wirkt sich auch zur Laufzeit stärker auf die Performanz aus. Der Einsatz von ALGs erfolgt deshalb in diesem Umfeld nur in Einzelfällen.

Paketfilterfirewalls stehen mit vergleichbarem Funktionsumfang von verschiedensten Herstellern zur Verfügung. Trotz der negativen Auswirkungen auf das Management empfiehlt sich keine homogene, sondern eine heterogene Zusammenstellung von Paketfilterfirewalls; nur so kann sichergestellt werden, dass beispielsweise neu gefundene und noch nicht behobene Sicherheitslücken in der Firewallsoftware eines Herstellers nur einige, aber nicht alle Zonengrenzen betreffen.

Application Level Gateways müssen, wie ihr Name impliziert, das jeweilige Anwendungsprotokoll (Schicht 7 im ISO/OSI-Referenzmodell) unterstützen; wie bereits beschrieben eignen sich insbesondere **virtuelle Verzeichnisdienste als LDAP-ALGs** und **SOAP-Firewalls** für den Schutz z. B. von IDP- und SP-Software.

Abbildung 4.26 zeigt eine mögliche Realisierungsvariante für die oben genannte Einteilung in vier Zonentypen. In der Praxis sind Abweichungen von dieser vereinfachten Positionierung zu erwarten, die auch durch Randbedingungen wie die Backbonestruktur und Zuordnung von Maschinen zu Serverracks ausgelöst werden, größtenteils jedoch durch Techniken wie virtuelle LANs (VLANs) kompensiert werden können. Das Ziel muss deshalb der Schutz jeder Komponente auf Basis des ihr zugeordneten Zonentyps sowie die Möglichkeit zur Kommunikation zwischen Maschinen, die demselben Zonentyp zugeordnet sind, sein. Die in der Abbildung nummerierten Firewalls haben die folgenden Aufgaben:

- **Firewall 1** stellt die Schnittstelle zum Internet dar und ist der so genannte äußere Firewall in der von den Firewalls 1 und 2 realisierten **demilitarisierten Zone** (DMZ,

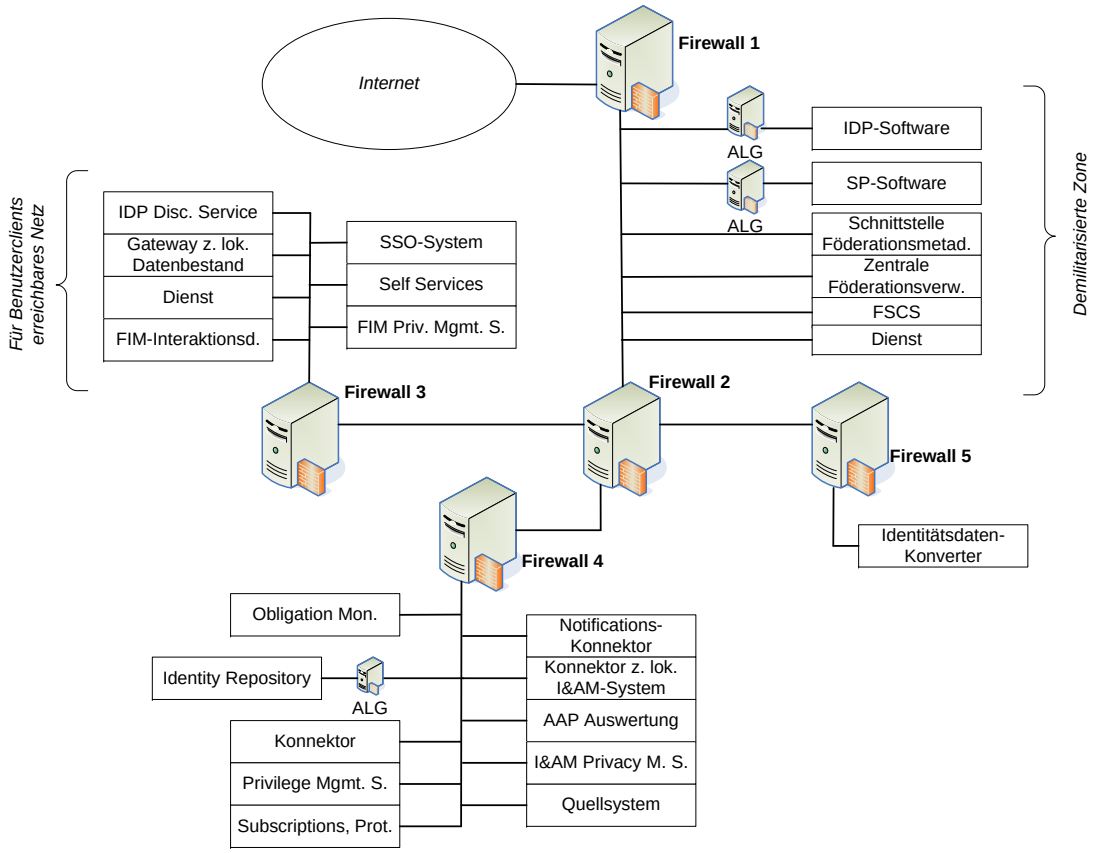


Abbildung 4.26.: Exemplarische Positionierung von Firewalls

Zonentyp 3). Er verhindert beispielsweise IP-Spoofing-Angriffe aus dem Internet und lässt Verbindungen zu den in der DMZ positionierten Servern nur auf den benötigten TCP-Ports zu (hier: HTTPS bzw. SOAP-over-HTTPS auf Port 443 sowie beim Einsatz von Application Servern für die IDP- bzw. SP-Software typischerweise auch Port 8443). Verbindungsversuche aus dem Internet zu den anderen, nicht in der DMZ positionierten Komponenten werden mit folgenden Ausnahmen nicht zugelassen:

  - Bei IDPs, deren Benutzer über das Internet auf die durch Firewall 3 geschützten Dienste zugreifen können müssen, werden entsprechende Verbindungen zugelassen, sofern diese Komponenten nicht auch in der DMZ platziert werden.
  - Bei SPs kann analog auf die Dienste zugegriffen werden, sofern diese nicht ebenfalls in der DMZ platziert werden.

- **Firewall 2** fungiert als so genannter innerer Firewall der DMZ und kontrolliert zudem die Datenflüsse zwischen den internen Netzen untereinander sowie zwischen den internen Netzen und der DMZ bzw. dem Internet (bei Komponenten hinter Firewall 5). Für die Firewalls 3, 4 und 5 sollte wie oben erwähnt ein anderes Produkt eingesetzt werden als für Firewall 2, um ein Kompromittieren des Zugangs zu den internen Netzen durch kombinierte Schutzmaßnahmen weitgehend ausschließen zu können.

- **Firewall 3** schützt die Systeme, mit denen die Benutzerclients kommunizieren (Zonentyp 2). Die Kommunikation erfolgt hier analog zur DMZ, ggf. mit Ausnahme der Dienste selbst, über HTTPS. Eingehende Anfragen werden jedoch nicht aus dem Internet, sondern nur aus den Benutzernetzen, der DMZ sowie den Konnektoren für die Dienste entgegen genommen; es gilt die erläuterte Ausnahme für den Fall, dass Benutzer über das Internet zugreifen. Ausgehende Verbindungen sind nur in die anderen internen Netze sowie die DMZ erlaubt.
- **Firewall 4** schützt Zonentyp 1. Ein- und ausgehende Verbindungen sind nur von bzw. zu den anderen internen Netzen und der DMZ erlaubt. Mit Ausnahme der Konnektoren sind die hier platzierten Systeme in der Regel noch durch weitere, ggf. dedizierte Firewalls geschützt; in der Abbildung ist dies durch einen ALG für das Identity Repository dargestellt.
- **Firewall 5** ist für Zonentyp 4 zuständig und lässt ausgehende Verbindungen der hinter ihm positionierten Systeme ins Internet zu. Eingehende Verbindungen werden nur für (SOAP-over-)HTTPS und nur für die internen Netze sowie die DMZ erlaubt.

Im Inneren jeder Zone können weitere Maßnahmen wie Intrusion Detection Systeme (IDS) eingesetzt werden. Da diesbezüglich keine I&AM- oder FIM-Spezifika zu berücksichtigen sind, wird an dieser Stelle nicht näher darauf eingegangen; es ist jedoch zu bedenken, dass der Einsatz verschlüsselter Kommunikation nicht nur die aus Datenschutzperspektive angestrebte Vertraulichkeit bewahrt, sondern auch die Angriffserkennung durch ein IDS erschweren kann.

4.7.3. Schutzmaßnahmen auf Applikationsebene

Da Identity Management im Allgemeinen als Teilgebiet des Security Managements aufgefasst werden kann und die FIM-Ansätze elementare Bestandteile wie Authentifizierungs- und Autorisierungsmechanismen bieten, steht hier der Schutzbedarf der I&AM- und FIM-Komponenten selbst im Vordergrund, während bei anderen Anwendungen typischerweise der Schutz der Nutzdaten vor unautorisierten Benutzerzugriffen priorisiert wird.

Die wesentlichen Schutzmaßnahmen wurden bei den einzelnen Komponenten bereits erläutert und lassen sich wie folgt zusammenfassen:

1. I&AM- und FIM-Komponenten werden bei jedem Kommunikationsvorgang **authentifiziert**, in der Regel durch Serverzertifikate. Diese Maßnahme stellt sicher, dass eine eingehende Nachricht von einer bekannten, wenn auch nicht implizit vertrauenswürdigen Entität stammt.
2. Die **Integrität von Nutz- und Metadaten**, beispielsweise von Policies, wird über elektronische Signaturen sichergestellt; hierdurch können unerwünschte Modifikationen entdeckt werden. Zudem werden beispielsweise Zeitstempel und Noncen verwendet, um die Gültigkeitsdauer von Nachrichten einzuschränken und ihre nur einmalige Auswertung sicherzustellen.
3. Die Daten werden verschlüsselt übertragen, um ihre Vertraulichkeit zu gewährleisten. Hierzu werden einerseits Kommunikationskanäle verwendet, die die komplette Datenübertragung verschlüsseln; andererseits kann die **Ende-zu-Ende-Vertraulichkeit** bei

mittelbarer Kommunikation über die Verschlüsselung der Nutzdaten selbst erreicht werden.

4. Der Abruf und die Verwendung von Daten werden über **Policies** gesteuert. Im FIM-Umfeld sind hierfür insbesondere die AAPs und ARPs relevant; sie werden durch organisationsinterne Privacy Management Systeme und Privilege Management Systeme ergänzt.

5. Jeder Benutzer wird von seinem IDP mit einem angemessenen Verfahren authentifiziert. Sofern mehrere Verfahren zur Auswahl stehen, kann sich die Selektion des Verfahrens am vom SP gemeldeten Bedarf orientieren.

Trotz dieser Maßnahmen sollte die Konfiguration jeder Komponente so restriktiv gehandhabt werden, dass der Schaden für den Fall, dass eine andere, darauf zugreifende Komponente unbemerkt kompromittiert wurde, minimal gehalten werden kann.

4.7.4. Überwachung und Auditing

Jede I&AM- und FIM-Komponente kann die von ihr bearbeiteten Anfragen und gegebenenfalls deren Ergebnisse protokollieren. Diese Protokolle können prinzipiell auf die folgenden drei Arten ausgewertet werden:

1. **Analysewerkzeuge** wie Intrusion Detection Systeme können die Protokolle **in Echtzeit** auswerten und beispielsweise auf Basis von Signaturen bekannter Angriffe oder von Heuristiken Auffälligkeiten melden oder Kommunikationsvorgänge proaktiv unterbinden (sog. **Intrusion Prevention Systeme**). Wenn beispielsweise ein SP plötzlich damit beginnt, mehr Attribute als bislang üblich von einer Vielzahl von Benutzern abzufragen, könnte IDP-seitig darauf geschlossen werden, dass der SP kompromittiert wurde; als Reaktion könnten die ARPs automatisch so angepasst werden, dass diesem SP keine Daten mehr geliefert werden, bis ein Administrator manuell eingreift.

2. Im Rahmen eines **manuellen Auditings** können die Protokolle stichprobenartig ausgewertet werden; eine Auswertung aller Protokolle ist aufgrund des damit verbundenen Aufwands in der Regel nicht möglich. Gefundene Auffälligkeiten können einerseits zur Verfeinerung des Regelwerks für die automatische Protokollanalyse führen, andererseits jedoch auch Rückschluss auf Konfigurationsfehler geben, die fälschlicherweise zu sicherheitsspezifischen Meldungen führen.

3. Bei **extern gemeldeten konkreten Vorfällen** kann der Hergang anhand der Protokolle nachvollzogen werden; je nach Schwere des Vorfalls können die entsprechenden Protokollauszüge beispielsweise Ermittlungsbehörden als potentielle Beweismittel zur Verfügung gestellt werden.

Unabhängig davon, ob die Auswertung der Protokolle manuell oder automatisch erfolgt, ist zu unterscheiden, ob diese lokal bei der jeweiligen Komponente anfallen, an einer organisationsintern zentralen Stelle zusammenlaufen oder sogar föderationsweit akkumuliert werden:

- Die **Korrelation der Protokolle** mehrerer Komponenten ist für die Gesamtsicht auf eine FIM-Transaktion unerlässlich, wird von den existierenden Werkzeugen bislang jedoch nur unzureichend unterstützt. Sie wird deshalb derzeit lediglich in Einzelfällen und größtenteils manuell durchgeführt.
- Eine **föderationsweite Auswertung** ist aus diesem Grund derzeit ebenfalls noch nicht möglich; sie ist zudem mit weiteren organisatorischen und datenschutzrechtlichen Fragestellungen verbunden. Beispielsweise ist es typischerweise notwendig, alle personenbezogenen Daten in den Protokollen vor der Übermittlung an eine zentrale Auswertungsinstanz hinreichend zu anonymisieren (vgl. auch Anforderung [DSA-Anonymisierung]); diese Maßnahmen können jedoch wiederum die Effektivität und Erkennungsrate der Auswertungsmechanismen beeinträchtigen. Diese Aspekte werden derzeit insbesondere im Umfeld von Netzwerk Intrusion Detection Systemen untersucht (siehe z. B. [LTB06, PP03, PAPL06]; auf Datenschutzaspekte wird insbesondere in [DXZ06] eingegangen).

Ebenso wird auch die Korrelation von Sicherheitsmeldungen auf Netzwerkebene mit denen der I&AM- und FIM-Komponenten derzeit noch nicht unterstützt.

Somit muss auf organisatorischer Ebene geregelt werden, bei welchen außerhalb des gesamten Identity Management Systems eintretenden sicherheitsrelevanten Ereignissen auch dieses prophylaktisch außer Betrieb genommen werden sollte.

4.7.5. Technische Umsetzung von Datenschutzregelungen

Die in Kapitel 2 für I&AM und FIM erläuterten Datenschutzregelungen, die u. a. auf der EU-Datenschutzrichtlinie basieren, können mit der vorgestellten Architektur umgesetzt werden. Die Einzelaspekte wurden bereits bei der Erläuterung der Komponenten dargestellt und werden hier nur knapp zusammengefasst:

- Das I&AM Privacy Management System ermöglicht die Veröffentlichung der so genannten **Online-Datenschutzerklärung** auch in Form von P3P-Policies und hält die zum Zeitpunkt der Datenerfassung geltenden Privacy Policies als Metadaten fest. Der organisationsinterne Zugriff auf die erfassten Daten wird nach verschiedenen Kategorien so genannter *data users* differenziert auf Basis von EPAL-Policies kontrolliert; diese stellen die **zweckgemäße Verarbeitung** der Daten sicher.
- Die IDP-Software stellt im Zusammenspiel mit dem FIM-Interaktionsdienst eine Möglichkeit zur IDP-seitigen Anzeige von SP-seitigen Benutzerrichtlinien zur Verfügung.
- Der organisationsübergreifende Austausch personenbezogener Daten wird über Attribute Release Policies gesteuert. Administratoren haben dabei die Möglichkeit, sinnvolle **Standardfreigaben** vorzugeben, die vom jedem Benutzer individuell verfeinert werden können.

  Bei Bedarf können entsprechende Freigaben interaktiv während der Dienstnutzung konfiguriert werden.

  Langzeit-Obligationen werden über einen Obligation Monitor sowohl organisationsintern als auch -übergreifend unterstützt.

- Die Self Services ermöglichen die Einsicht und die ggf. notwendige Korrektur der eigenen personenbezogenen Daten durch jeden Benutzer. Im Zusammenspiel mit dem FIM-Interaktionsdienst wird die **informationelle Selbstbestimmung** der Benutzer darüber hinaus dadurch unterstützt, dass optional mitprotokolliert und angezeigt werden kann, welche Daten bereits wann an welche SPs übertragen worden sind.

- Schreibzugriffe von SPs auf die beim IDP gespeicherten Benutzerprofile können mit einem **interaktiven Genehmigungsschritt** verbunden werden.

Weitere Aspekte wie das Prinzip der Datensparsamkeit und die Rechtmäßigkeit der Erfassung der Personendaten beim IDP ändern sich gegenüber reinen I&AM-Systemen nicht und werden deshalb in dieser Arbeit nicht vertiefend betrachtet.

4.8. Change Management

Die komponentenübergreifenden und zum Teil architekturweiten Auswirkungen lokaler Änderungen verdeutlichen, dass Modifikationen an der I&AM- und FIM-Infrastruktur nur geplant, koordiniert und nach Abwägung der damit verbundenen Risiken durchgeführt werden dürfen; in Anlehnung an ITIL wird unter Change Management verstanden, dass ein transparenter Prozess existiert, der standardisierte Methoden zur Durchführung von Änderungen verwendet.

Prinzipiell werden hier – ebenfalls analog zu ITIL – zwei Arten von Veränderungen unterschieden:

1. Kleinere, relativ häufige Änderungen, die nach einem bereits bekannten Muster ablaufen und keiner gesonderten Genehmigung bedürfen; sie werden in ITIL als *pre-authorized changes* bezeichnet.

2. Größere Änderungen, deren Auswirkungen komplex und ggf. beim Stellen eines Änderungsantrags noch unbekannt sind. Sie müssen von einem Gremium analysiert und genehmigt werden, das in ITIL als *change advisory board* (CAB) bezeichnet wird.

Im Unterschied zu den organisationsinternen Vorgaben von ITIL ist zu berücksichtigen, dass Änderungen im FIM-Umfeld auch organisationsübergreifende Auswirkungen haben können; je nach Organisationsform der Föderation kann insbesondere der Fall eintreten, dass Änderungen gegen den Willen einer Organisation beschlossen werden können und umgesetzt werden müssen. Dies trifft insbesondere auch auf die Terminplanung für Änderungen zu, die bei ITIL als *forward schedule of changes* (FSC) bezeichnet wird.

In diesem Abschnitt werden nach der Erläuterung der Organisation des FIM Change Managements einige wichtige Änderungsarten mit Auswirkungen auf das FIM-Umfeld unter technischen und organisatorischen Aspekten diskutiert.

4.8.1. Organisation des FIM Change Managements

Die Umsetzung von FIM ist mit der Einführung organisationsübergreifender Prozesse oder zumindest deren IT-Unterstützung verbunden; das organisationsinterne CAB ist deshalb entweder um ständige oder zumindest bei diese Prozesse oder das organisationsinterne Identity Management betreffenden Änderungsanträgen um temporäre Mitglieder mit FIM-Fachwissen zu erweitern. In Abhängigkeit von der Wichtigkeit FIM-unterstützter Prozesse müssen diese CAB-Mitglieder ein Vetorecht erhalten, um lokale Änderungen, die sich ergebende Auswirkungen auf FIM nicht ausreichend berücksichtigen, verhindern zu können.

Für Änderungen mit organisationsübergreifenden Auswirkungen muss ebenfalls ein CAB geschaffen werden; dabei sind die folgenden Fälle zu unterscheiden:

- Eine Änderung betrifft nur *einige, aber nicht alle Föderationsteilnehmer*. Dieser Fall tritt beispielsweise ein, wenn ein SP innerhalb einer Föderation Geschäftsbeziehungen zu ausgewählten IDPs hat und Änderungen an den Autorisierungsmechanismen vorgenommen werden sollen. In diesem Beispiel besteht das CAB aus Vertretern der beteiligten IDPs und des SP, von dem es typischerweise dominiert wird.
- Eine Änderung betrifft die *ganze Föderation*. Die Besetzung und Leitung des CAB hängt in diesem Fall von der Organisationsform der Föderation ab. In der Regel wird das CAB von Vertretern der Föderationsverwaltung geleitet; die Besetzung mit Vertretern der Föderationsteilnehmer und deren Stimmrechte und -gewichte sind szenarienspezifisch festzulegen.
- Eine Änderung betrifft *mehr als eine Föderation*. Diese Fälle sind derzeit noch äußerst selten und umfassen beispielsweise den Zusammenschluss mehrerer Föderationen zu einer einzigen sowie größere Änderungen bei Föderationsteilnehmern, die an mehr als einer Föderation beteiligt sind. Entsprechend kann nicht erwartet werden, dass für solche Änderungen bereits geeignete Prozesse eingeführt worden sind. Ein CAB-ähnliches Gremium ist deshalb bedarfsorientiert einzurichten und nach Abschluss der Änderungen wieder aufzulösen; die Besetzung ist wiederum szenarienspezifisch und könnte neben den Föderationsverwaltungen beispielsweise die primär betroffenen Föderationsteilnehmer umfassen.

Allgemein ist festzuhalten, dass derzeit organisationsübergreifend relevante Änderungen mit Ausnahmen von Phasen wie der Föderationseinrichtung wesentlich seltener auftreten als organisationsinterne; die weitreichenden Auswirkungen und ggf. die Notwendigkeit zur direkten Beteiligung jedes Föderationsteilnehmers führend jedoch dazu, dass nur wenige *pre-authorized changes* definiert werden können. Zudem muss der resultierende FSC entweder mit den Föderationsteilnehmern koordiniert werden, oder die Termine müssen eine mit Sicherheit ausreichende Vorlaufzeit für die lokale Umsetzung der Änderungen bieten; diesbezüglich ist ein prioritätsgesteuerter Kompromiss aus Abstimmungsaufwand und Dauer bis zur Umsetzung zu finden.

4.8.2. In- und Außerbetriebnahme von Komponenten

Die Auswahl und Inbetriebnahme neuer Komponenten wird durch FIM-seitige Randbedingungen wie folgt komplexer:

- Bei der Einführung neuer Datenquellen muss darauf geachtet werden, dass die von ihnen gelieferten Daten nicht nur den organisationsinternen, sondern auch den föderationsweiten Qualitätsansprüchen genügen.
- Analog ist bei SP-seitig neu eingeführten Diensten möglichst auf ihre FIM-Fähigkeit zu achten, um Funktionalitäten wie organisationsübergreifendes Single Sign-On direkt nutzen zu können. Darüber hinaus sind die Metadaten wie in Abschnitt 4.8.3 beschrieben anzupassen.
- Bei der Implementierung eines FIM Privacy Management Systems ist zu berücksichtigen, ob bereits ein I&AM Privacy Management System vorhanden ist, dessen Obligation Monitor geeignete Schnittstellen aufweist.

Bei der Außerbetriebnahme von Komponenten sind die in Abschnitt 4.5 diskutierten Abhängigkeiten organisationsintern zu berücksichtigen:

- Bei IDPs dürfen Datenquellen, die für FIM benötigte Daten liefern, nicht ersatzlos außer Betrieb genommen werden. Die IDP-Software ist in diesem Zusammenhang als Dienst zu betrachten, der die für FIM benötigten Daten aus einem lokalen Identity Repository ausliest und entsprechend im I&AM Change Management berücksichtigt werden muss.
- Analog müssen IDP-seitig das Single Sign-On System sowie das I&AM Privacy Management System erhalten bleiben, auch falls sie organisationsintern nicht mehr benötigt werden, sofern sie nicht durch für FIM geeignete Minimalvarianten ersetzt werden.

Im Hinblick auf die temporäre Außerbetriebnahme von I&AM-Komponenten, beispielsweise zu Wartungszwecken, ist neben dem Single Sign-On System insbesondere das Identity Repository selbst zu berücksichtigen.

Die mögliche Außerbetriebnahme von FIM-Komponenten ist im Föderationskontext zu analysieren; da lediglich der Notifications-Konnektor und das Privilege Management System optionale Komponenten darstellen, hängt es von der Nutzung ihrer Funktionalität in den Föderationen ab, ob sie abgeschaltet werden können.

4.8.3. Änderungen an den Metadaten

Vor dem Hintergrund des Change Managements sind die folgenden drei Arten von föderationsteilnehmerseitig initiierten Metadatenänderungen zu berücksichtigen:

- **Serverzertifikate** haben eine typischerweise auf ein oder zwei Jahre beschränkte Gültigkeitsdauer und müssen somit periodisch erneuert werden. Um Dienstadministratoren von dieser Aufgabe zu entlasten, werden Zertifikate organisationsintern häufig zentral verwaltet. Im FIM-Umfeld ist zu berücksichtigen, dass in den Föderationsmetadaten enthaltene Zertifikate ebenfalls aktualisiert werden müssen.
- Bei der **Einführung neuer Dienste** bzw. bei Änderungen von IP-Adressen bzw. DNS-Namen von Servern für IDP- bzw. SP-Software müssen ebenfalls die Föderationsmetadaten aktualisiert werden; analog zu Zertifikaten ist die Verwaltung von DNS-Einträgen

ebenfalls üblicherweise zentralisiert und wird nicht von den Administratoren der Dienste bzw. FIM-Komponenten selbst übernommen.

- In den Föderationsmetadaten werden darüber hinaus **Kontaktinformationen** von technisch wie organisatorisch Zuständigen pro Föderationsteilnehmer erfasst. Organisationsinterne Änderungen an diesen Zuständigkeiten, die beispielsweise durch Reorganisation oder Personalfluktuation verursacht werden, müssen in den Metadaten nachgezogen werden.

In der Praxis wird insbesondere die dritte Änderungsart häufig übersehen, da es sich dabei im engeren Sinn um keine technische Modifikation handelt. Die Eigenschaft, als FIM-Ansprechpartner zu fungieren, sollte deshalb im I&AM-System explizit festgehalten und bei Änderungen geeignet ausgewertet werden.

Die von der Föderationsverwaltung durchgeführten Metadatenänderungen müssen mit Ausnahme der föderationsweiten Policies nicht vom lokalen Change Management berücksichtigt werden, da sie keine lokalen Eingriffe notwendig machen (vgl. auch Abschnitt 4.8.5). Neue föderationsweite Attribute Release und Acceptance Policies erfordern jedoch neben ihrer föderationsweiten Vereinbarung auch Untersuchungen, inwiefern die neuen Fassungen im Konflikt mit anderen lokalen Policies stehen. Falls dies der Fall ist und föderationsseitig keine Nachbesserungen möglich sind, müssen die lokalen Policies angepasst oder andere Konsequenzen in Erwägung gezogen werden.

4.8.4. Änderungen an der Komponentenkonfiguration

Aufgrund der Vielzahl an Möglichkeiten, die Konfiguration der einzelnen Komponenten zu modifizieren, können hier nicht alle Fälle diskutiert werden. Ein Teil der möglichen Änderungen ist darüber hinaus nicht FIM-spezifisch; beispielsweise sind Änderungen z. B. an IP-Adresse oder DNS-Eintrag des Identity Repository zwar nicht in den Föderationsmetadaten, aber in den Konfigurationen der darauf zugreifenden FIM-Komponenten zu berücksichtigen. Diese auch bei anderen Diensten zu berücksichtigenden Aspekte werden hier jedoch nicht vertieft.

Relevante und durchaus komplexe Auswirkungen haben **Änderungen am organisationsintern eingesetzten Datenmodell**; hierbei ist zu unterscheiden zwischen

- **Erweiterungen**, z. B. des LDAP-Schemas. Diese Änderungen sind in der Regel unkritisch, da beispielsweise vorhandene I&AM-Konnektoren nur dann angepasst werden müssen, wenn Zielsysteme die neuen Datenfelder benötigen. Analog gilt für die FIM-Komponenten und insbesondere den Identitätsdatenkonverter bzw. die beim Federation Schema Correlation Service (FSCS) hinterlegten Konvertierungsregeln, dass Änderungen nur dann erforderlich sind, wenn das Datenfeld auch für andere Föderationsteilnehmer relevant ist. Im Hinblick auf die Sicherstellung der Datenqualität gelten dieselben Aussagen wie für die Inbetriebnahme neuer Quellsysteme.

- **Modifizieren** von Attributen, d. h. von Namensgebung, Syntax oder Semantik. Von dieser Änderung sind bereits organisationsintern diejenigen direkt auf das Identity Repository zugreifenden Dienste sowie diejenigen Konnektoren betroffen, die eines der

modifizierten Attribute verarbeiten; zu den betroffenen Diensten gehören insbesondere auch die Self Services. Änderungen dieser Art werden deshalb möglichst vermieden, sind aber beispielsweise beim Umstieg auf andere I&AM-Softwareprodukte bei starker Orientierung an das von ihnen vorgegebene Schema kaum zu vermeiden.

Bezüglich der FIM-Komponenten sind derartige Änderungen nicht nur in den Regelsätzen für den Identitätsdatenkonverter nachzuziehen, sondern auch in den bereits bestehenden ARPs, AAPs, Obligationen und der Datenbasis, in der die von SPs gewünschten Aktualisierungsbenachrichtigungswünsche eingetragen sind.

Bereits kleine, unscheinbare Modifikationen können deshalb mit einem sehr hohen Aufwand verbunden sein; um zu vermeiden, dass alle Änderungen auf einmal durchgeführt werden müssen, kann deshalb ein zweistufiges Vorgehen gewählt werden, bei dem erst eine Erweiterung des Datenmodells vorgenommen wird, die parallel zu den bisherigen Datenfeldern gepflegt wird, und bei dem nach sukzessiver Umstellung aller betroffenen Systeme die alten Datenfelder entfernt werden.

- **Löschen** eines Attributs. Diese Änderung darf offensichtlich nur durchgeführt werden, wenn das Attribut weder organisationsintern noch von einem anderen Föderationsteilnehmer benötigt wird. Die Konfiguration der Konnektoren und der Konvertierungsregeln für den FIM-Einsatz müssen entsprechend angepasst werden. ARPs, AAPs und Aktualisierungsbenachrichtigungswünsche sollten ebenfalls adaptiert werden; dies kann ggf. jedoch auch noch nachträglich erfolgen. Obligationen, die sich ausschließlich auf dieses Attribut beziehen, werden mit seiner Löschung hinfällig. Um Probleme bei der Abarbeitung komplexerer Obligationen zu vermeiden, werden zu löschende Attribute jedoch für eine ausreichende Übergangszeit lang lediglich nicht mehr von den anderen Komponenten genutzt und aus dem Identity Repository erst dann gelöscht, wenn sie sicher nicht mehr benötigt werden.

Vergleichbare Änderungen, die SP-seitig an Diensten statt am Identity Repository vorgenommen werden, müssen außer im entsprechenden Konnektor ebenfalls in den (dienstspezifischen) AAPs berücksichtigt werden.

Für **Änderungen am föderationsweiten Schema** gelten analoge Aussagen:

- Beim **Hinzufügen** von Attributen ist bei IDPs bzw. AAs organisationintern zu klären, ob die gewünschten Informationen bereitgestellt werden können. Falls dies der Fall ist, sind neben den Konvertierungsregeln auch die ARPs entsprechend zu erweitern. SP-seitig ist die Möglichkeit zur Verwendung zu klären sowie die AAPs ggf. anzupassen. Meist sind nachträglich hinzugefügte Attribute als *optional* und nicht als *mandatory* gekennzeichnet, um bereits vorhandene IDPs und AAs nicht auszuschließen.

- Wie im organisationsinternen Fall gilt, dass **Modifikationen** bestehender Attributsspezifikationen möglichst zu vermeiden sind, sofern es sich nicht um Korrekturen oder Verfeinerungen handelt, die dem praktisch bereits etablierten Gebrauch Rechnung tragen. Im Allgemeinen sind von einer derartigen Änderung zwar nur die im FSCS hinterlegten Konvertierungsregeln betroffen; diese müssen jedoch von allen betroffenen Föderationsteilnehmern rechtzeitig umgestellt werden – der FSCS kann diesen Umstellungsprozess unterstützen, indem er eine Möglichkeit zum synchronen Wirksamwerden mehrerer geänderter Regelsätze bereitstellt.

- Das **Löschen** von Attributen aus dem föderationsweiten Schema ist, sofern es sich um wirklich nicht mehr benötigte Attribute handelt, unkritisch, so dass lediglich die Konvertierungsregeln sowie eventuell noch vorhandene Aktualisierungsbenachrichtigungswünsche bereinigt werden sollten.

Offensichtlich sind Änderungen am föderationsweiten Schema ebenfalls föderationsweit zu koordinieren, wohingegen bei lokalen Änderungen lediglich die eigenen sowie die lokal bekannten föderationsseitigen Anforderungen berücksichtigt werden müssen.

4.8.5. Änderungen an der Föderationszusammensetzung

Die Fluktuation der Föderationsteilnehmer stellt lediglich für die Föderationsverwaltung eine explizit zu bearbeitende Änderung da; in den bisher üblichen Föderationen tritt das Hinzukommen neuer Föderationsteilnehmer wesentlich häufiger ein als das Ausscheiden. Die Kriterien, die neu in eine Föderation aufzunehmende Organisationen erfüllen müssen, sind stark szenarienspezifisch und werden hier nicht vertieft.

Wie in Abschnitt 4.1.2 erläutert wurde, ermöglicht die Zugehörigkeit zu einer Föderation zwar die prinzipielle FIM-basierte Kommunikation mit den anderen Föderationsteilnehmern, ist aber nicht zwangsweise mit besonderen Berechtigungen verbunden. Die Nutzung der Dienste neuer SPs sowie das Akzeptieren von Benutzerdaten von neuen IDPs bzw. AAs bleibt den bereits bestehenden Föderationsteilnehmern somit frei überlassen; hiervon abweichende Regelungen können bei Bedarf über föderationsweite Policies umgesetzt werden.

Für diese Veränderungen sind deshalb geeignete Voreinstellungen für ARPs und AAPs zu treffen, die bei Bedarf ebenso wie die über das IDP-seitige Privilege Management System verwalteten Berechtigungen von Benutzern zu erweitern sind.

Sonderfälle stellen Veränderungen bei den föderationsweit genutzten Trusted Third Party Services dar:

- **Änderungen an der zentralen Föderationsverwaltung** sollten aus Sicherheitsgründen zumindest manuell von jedem Föderationsteilnehmer bestätigt werden müssen.
- Bei der **Einführung eines neuen IDP Discovery Services** sollten die Benutzer über die legitime Veränderung informiert werden; dies kann sowohl IDP- als auch SP-seitig erfolgen.
- Eine **Migration des FSCS** muss zumindest in den Konfigurationen der eingesetzten Identitätsdatenkonverter nachgezogen werden. Da ein FSCS prinzipiell auch föderationsübergreifend bzw. -unabhängig agieren kann und Änderungen wie bei der Föderationsverwaltung aus Sicherheitsgründen bestätigt werden sollten, ist eine automatische Verteilung der Informationen über den Kommunikationsendpunkt des FSCS mittels der Föderationsmetadaten nur bedingt sinnvoll.

Die Gründung und das Auflösen einer Föderation stellen Spezialfälle der Beschreibungen im nächsten Abschnitt dar.

4.8.6. Änderungen an den eigenen Föderationsmitgliedschaften

Die Schritte zur Aufnahme einer Organisation in die erste Föderation wurden bereits in Abschnitt 4.6 erörtert. Sie sind für die Aufnahme in weitere Föderationen entsprechend wiederholt anzuwenden, wobei die benötigten Komponenten bereits vorhanden sind und lediglich geeignet konfiguriert werden müssen:

- IDPs und AAs müssen die Verfügbarkeit der benötigten Daten in entsprechender Qualität sicherstellen.
- Attribute Release und Acceptance Policies müssen angepasst werden, sofern die bereits vorhandenen Voreinstellungen ungeeignet erscheinen.
- Die Konvertierungsregeln müssen dem Schema der neuen Föderation angepasst und über den entsprechenden FSCS publiziert werden.
- Die Organisation muss in die Metadaten der neuen Föderation aufgenommen werden.
- Sofern dies noch nicht der Fall ist, muss bei Service Providern die SP-Software so umgestellt werden, dass sie Benutzer an einen multi-federation-fähigen IDP Discovery Service weiterleitet.

Das Ausscheiden aus einer Föderation ist hierzu invers: Mit der Austragung aus den Föderationsmetadaten verliert eine Organisation ihren Mitgliedsstatus und die FIM-basierte Kommunikation wird unterbunden, sofern die entsprechenden Kommunikationspartner nicht noch beide Mitglied in einer anderen Föderation sind. Daran schließt sich das Entfernen nicht mehr benötigter Konvertierungsregeln und Policies an.

Die Auswirkungen eines Föderationsaustrittes auf den Datenbestand sind szenarienspezifisch zu untersuchen: IDP-seitig kann beispielsweise auf die Erfassung föderationsspezifischer Daten wieder verzichtet werden. SPs können es ihren über die ehemalige Föderation akquirierten Benutzern optional freistellen, ihre Dienste mit lokalen Kennungen weiterhin zu verwenden.

Der Austritt aus einer Föderation ist darüber hinaus typischerweise auch ein Auslöser für nicht FIM-spezifische Prozesse wie das Stellen abschließender Rechnungen.

4.9. Architekturmuster

Im Umfeld des Software Engineerings bezeichnen Entwurfsmuster (engl. *design patterns*) generisch verwendbare Lösungsansätze für häufig auftretende Problemstellungen (vgl. [BMR+98]). Architekturmuster werden dabei auf einer hohen Abstraktionsebene eingesetzt, um den prinzipiellen Aufbau von komplexen Systemen zu vermitteln (vgl. [Bos00]).

Diese grundlegende Idee wird nachfolgend dazu verwendet, um die flexible, funktionsbedarfsorientierte Kombination der erläuterten Komponenten zu demonstrieren. Nach einer Abgrenzung gegenüber anderen Arbeiten werden mehrere Architekturmuster vorgestellt, die zusammen das Komponentenspektrum weitgehend abdecken und die Ausgangsbasis für die Referenzarchitekturen im nächsten Abschnitt bilden; aus diesem Grund entwickeln sich die hier behandelten Architekturmuster bewusst vom Kleinen ins Große, obwohl noch weitere Ausprägungen in den verschiedenen Komplexitätsstufen möglich wären.

4.9.1. Abgrenzung gegenüber verwandten Arbeiten

Die Popularität von Entwurfsmustern und die Sensibilisierung von Softwareentwicklern für Securityaspekte hat dazu geführt, dass derzeit verschiedene Formen von *Identity Management Patterns* aufkommen, die mit den hier erarbeiteten jedoch nicht direkt vergleichbar sind:

- Gädke et al. beschreiben in mehreren Publikationen „Bausteine“ für Federated Identity Management [BuiBl1, BuiBl2]. In diesen Arbeiten werden grundlegende Methoden zur Modellierung von Sicherheitsdomänen in der Unified Modeling Language (UML) dargelegt, wobei zwischen Identity Providern und Service Providern unterschieden und auf die Anwendung von Single Sign-On eingegangen wird. Eine mit der Beschreibung der Komponenten in diesem Konzept vergleichbare Betrachtung der einzelnen Bausteine erfolgt nicht, da der Schwerpunkt auf der UML-Modellierung liegt.
- Als *Identity Patterns*[4] wird eine sich in Entwicklung befindende Programmierbibliothek für Java bezeichnet, die u. a. zur Verarbeitung von SAML Assertions und SPML Nachrichten verwendet werden können soll. Dabei erfolgt eine Orientierung an den so genannten Core Security Patterns [SNL05]. Es handelt sich dabei folglich um implementierungsnahe Entwurfsmuster, jedoch nicht um Architekturmuster im hier verwendeten Sinn.
- Das Identity Management Forum der Open Group[5] arbeitet nach eigenen Angaben an *Identity Management Design Patterns*; der letzte Bericht der Arbeitsgruppe[6] lässt darauf schließen, dass FIM zwar durchaus berücksichtigt werden soll, das Ergebnis jedoch primär auf die Vermittlung von Grundlagen abzielen soll.

Die nachfolgend vorgestellten Architekturmuster beziehen sich ausschließlich auf die im Rahmen des Architekturkonzepts vorgestellten Komponenten; sie sollen die problemorientierte Auswahl von Komponenten zeigen und deren Zusammenspiel resümieren. Zwangsläufig können mit den vorgestellten Architekturmustern nicht alle Problemstellungen gelöst werden und auch für die genannten Probleme können alternative Lösungsvarianten existieren; es bietet sich jedoch an, konkrete Szenarien im Hinblick auf die mögliche Eignung der Architekturmuster zu untersuchen, bevor Lösungen von Grund auf neu konzipiert werden.

4.9.2. Architekturmuster 1: Organisationsinternes Identity Repository

Die Bereitstellung eines Identity Repository ist eine grundlegende Voraussetzung für die Anbindung der FIM-Komponenten. Wie in Abbildung 4.27 dargestellt ist, wird das Identity Repository mittels Konnektoren aus mindestens einer Datenquelle gespeist und kann von beliebig vielen dafür geeigneten Zielsystemen direkt genutzt werden.

Dabei sind folgende Aspekte zu berücksichtigen:

- Da Konnektoren im Push- oder Pullverfahren arbeiten können, ist die Aufrufrichtung nicht vorgegeben.

[4] `https://identitypatterns.dev.java.net/`
[5] `http://www.opengroup.org/idm/`
[6] `https://www.opengroup.org/conference-live/uploads/40/11007/Forum_Reports.pdf`

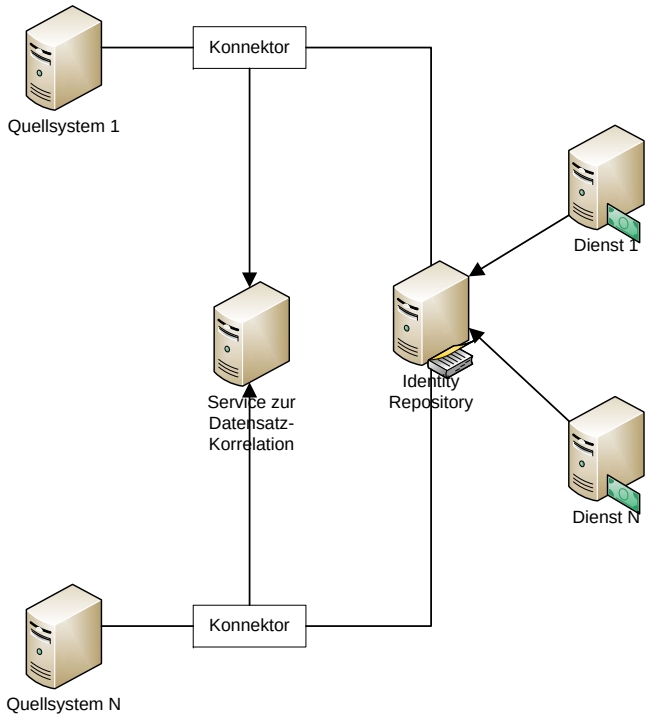


Abbildung 4.27.: Architekturmuster 1: Organisationsinternes Identity Repository

- Bei mehr als einer Datenquelle ist anzustreben, dass die Datensätze korreliert im Identity Repository hinterlegt werden. Die dazu notwendigen Schritte sind von den Konnektoren zu realisieren und werden ggf. über entfernte Funktionsaufrufe, z. B. in Form von Web Services, eingebunden.
- SP-seitig ist eventuell kein Identity Repository notwendig, beispielsweise wenn der SP nur genau einen Dienst ausschließlich über FIM anbietet.

Ohne Beschränkung der Allgemeinheit wird im Folgenden davon ausgegangen, dass zur Realisierung des Identity Repository und der Konnektoren ein LDAP-basiertes Meta-Directory eingesetzt wird.

4.9.3. Architekturmuster 2: Anbindung proprietärer organisationsinterner Dienste

Dieses Architekturmuster betrifft Dienste, die an ein vorhandenes Identity Repository nicht direkt angeschlossen werden können, da sie entweder gar keine externen Datenbestände unterstützen oder das im Identity Repository verwendete Datenformat ungeeignet für sie ist.

Entsprechend können zwei Realisierungsvarianten eingesetzt werden:

1. Abbildung 4.28 zeigt im oberen Teil die Verwendung eines Konnektors zur Einspeisung der relevanten Benutzerdaten vom Identity Repository in den lokalen Datenbestand des

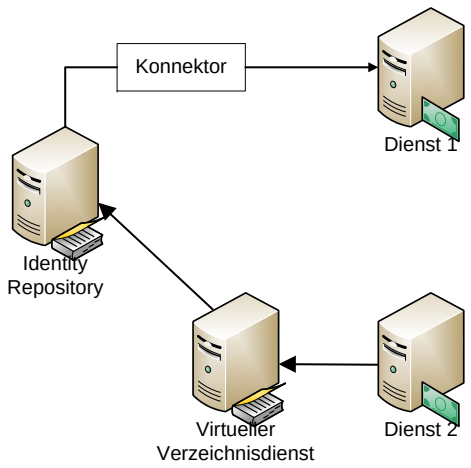


Abbildung 4.28.: Architekturmuster 2: Anbindung proprietärer organisationsinterner Dienste

Dienstes. Wie in Abschnitt 4.5.1 erläutert wurde, eignen sich rein provisioningsystembasierte I&AM-Systeme nicht für den Einsatz im FIM-Umfeld und werden hier deshalb nicht berücksichtigt.

2. In unteren Teil der Abbildung wird der Einsatz eines virtuellen Verzeichnisdienstes als Konverter zwischen den Datenformaten des Identity Repository und des Dienstes gezeigt. Es kann, insbesondere wenn auch eine Lastverteilung erwünscht wird, alternativ ein dediziertes Identity Repository mit einem dem Dienst angepassten Schema verwendet werden; in der Regel ist der damit verbundene Aufwand für einen einzigen Dienst jedoch nicht gerechtfertigt.

Mit zunehmender Verbreitung von I&AM-Systemen und damit verbundener Anpassung und Flexibilisierung von Diensten ist davon auszugehen, dass diese Form der Anbindung im Allgemeinen nur noch für Legacysysteme benötigt wird.

4.9.4. Architekturmuster 3: Benutzerfreundliche Gestaltung des I&AM-Systems

Abbildung 4.29 zeigt die Erweiterung des grundlegenden I&AM-Systems um Self Services und ein Single Sign-On System. Dadurch können sich wie bei den Beschreibungen der beiden Komponenten erläutert neben der Benutzerfreundlichkeit auch die Datenqualität und Sicherheit erhöhen.

I&AM-Systeme mit Self Services und SSO-System oder zumindest Unified Login stellen die derzeit am weitesten verbreiteten organisationsinternen Identity Management Lösungen dar; dieses Architekturmuster stellt somit die organisationsinterne Basis für die unten erläuterten Referenzarchitekturen dar.

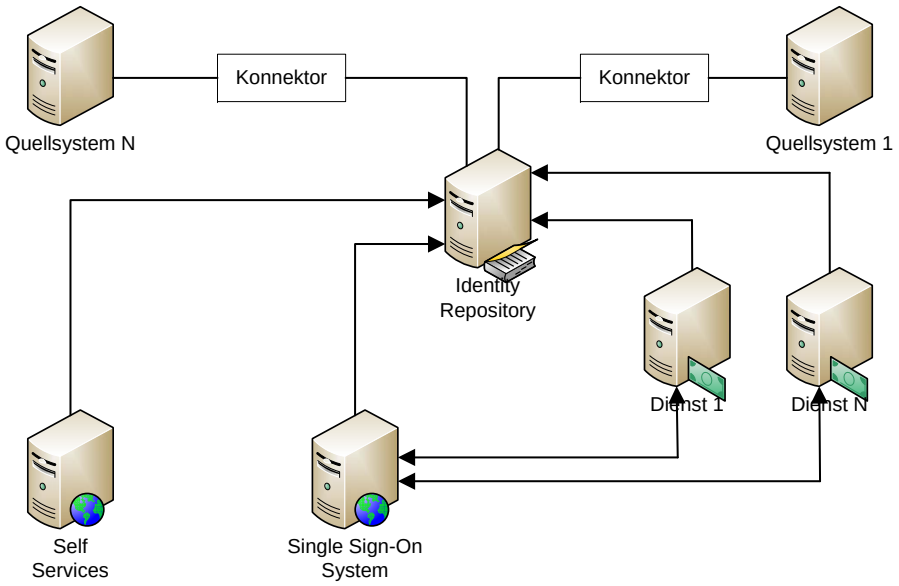


Abbildung 4.29.: Architekturmuster 3: Benutzerfreundliche Gestaltung des I&AM-Systems

4.9.5. Architekturmuster 4: Organisationsübergreifendes Single Sign-On

Organisationsübergreifendes Single Sign-On durch Authentifizierungsbestätigungen ist insbesondere in der Einführungsphase, wenn Benutzer des IDP bereits lokale Kennungen bei SPs haben, der häufigste FIM-Anwendungsfall.

Zur Schaffung dieser Möglichkeit sind im einfachsten Fall wie in Abbildung 4.30 dargestellt lediglich IDP- und SP-Software ohne die weiteren FIM-Komponenten notwendig; die IDP-Software leitet Authentifizierungsanfragen an das vorhandene SSO-System weiter und die SP-Software kommuniziert direkt mit den von den Benutzern gewünschten Diensten. Es ist zu beachten, dass IDP-seitig keine Überprüfung von Attribute Release Policies durchgeführt wird, so dass die ggf. gewünschte Einschränkung der Kommunikation der IDP-Software mit nur bestimmten SPs z. B. durch Firewalls sichergestellt werden muss. Aufgrund der beim SP lokal vorhandenen Kennungen kann davon ausgegangen werden, dass der jeweils zuständige IDP bereits bekannt ist und nicht erst zu Beginn der Dienstnutzung ermittelt werden muss, so dass auf den IDP Discovery Service und zentral verwaltete Metadaten verzichtet werden kann. Diese SSO-Konstellation entspricht im Wesentlichen dem Primärziel der „Phase One“ der Liberty Alliance (vgl. Abschnitt 3.2.2).

4.9.6. Architekturmuster 5: Bilaterales FIM

Ein nicht untypisches Szenario liegt vor, wenn lediglich *ein* Identity Provider und *ein* Service Provider über FIM miteinander Daten austauschen wollen, so dass der Betrieb einer Föderationsverwaltung unnötigen Aufwand darstellen würde. Dieser Fall tritt insbesondere in Entwicklungs- und Testumgebungen ein, in denen Dienste an FIM angepasst und wiederholt ausschließlich von Benutzern eines IDPs aufgerufen werden.

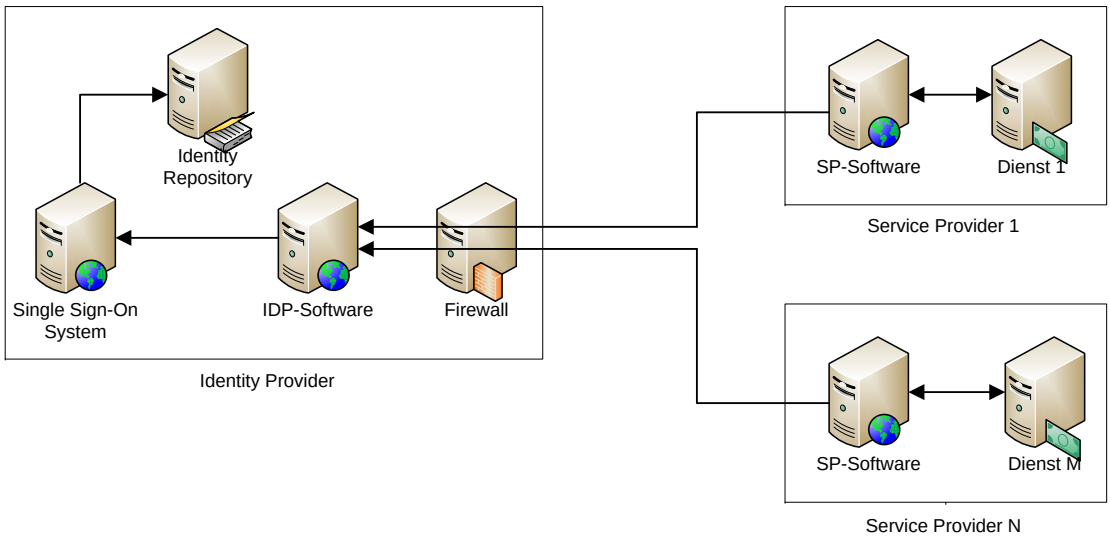


Abbildung 4.30.: Architekturmuster 4: Organisationsübergreifendes Single Sign-On

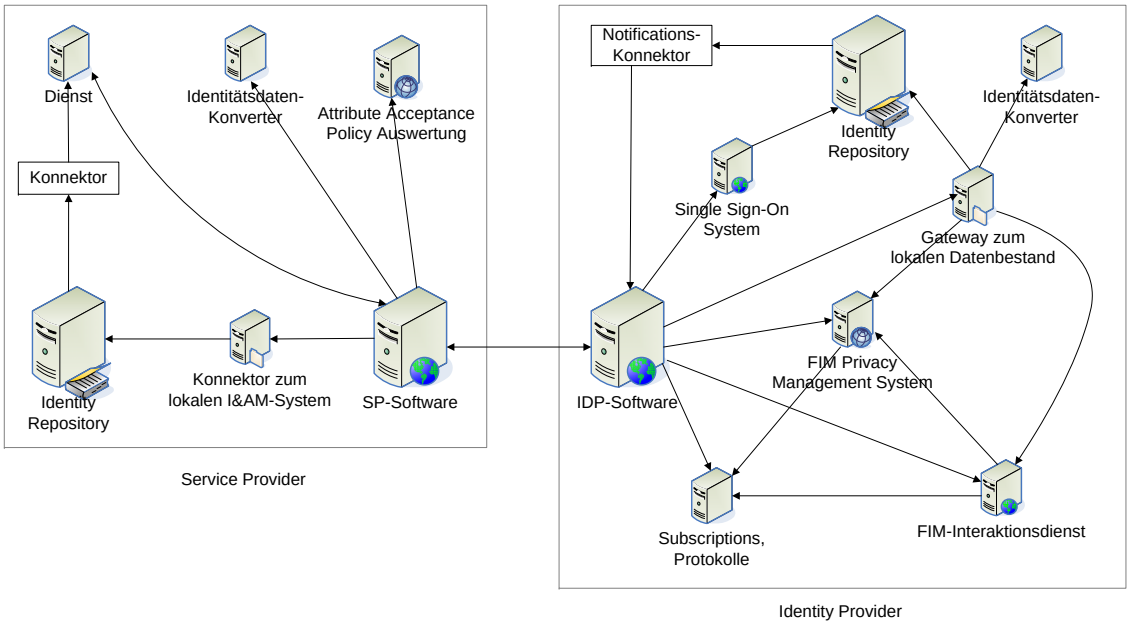


Abbildung 4.31.: Architekturmuster 5: Bilaterales FIM

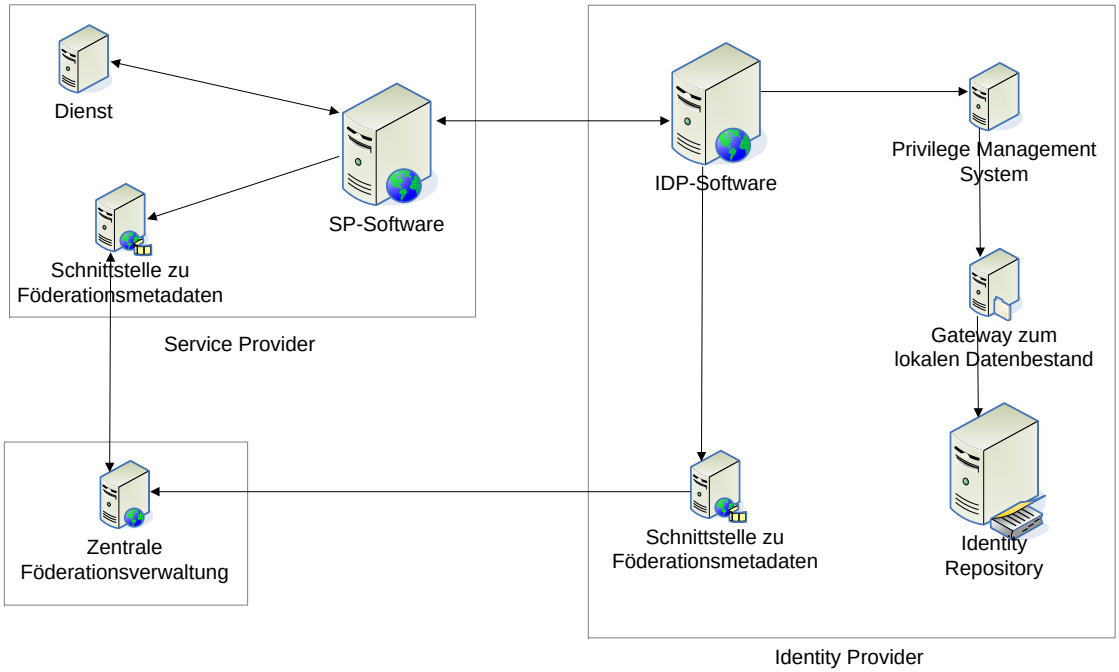


Abbildung 4.32.: Architekturmuster 6: Verteilte Autorisierungsinfrastruktur auf FIM-Basis

In diesem Kontext kann vereinfachend angenommen werden, dass neben Authentifizierungsbestätigungen nur allgemeine Attributsauskünfte benötigt werden, in den Attribute Release Policies jedoch auf Langzeit-Obligationen verzichtet werden kann. Abbildung 4.31 zeigt das resultierende Architekturmuster, in dem insbesondere auf die föderationsweiten Dienste verzichtet werden kann. Es wird jedoch auch deutlich, dass bereits für solche Minimalföderationen ein Großteil der technischen Komponenten benötigt wird; dies reflektiert den bereits diskutierten Aspekt, dass letztendlich jede FIM-Transaktion genau zwei Föderationsteilnehmer involviert und das Konzept von Föderationen eine stärker organisatorische als technische Grundlage für FIM bildet.

4.9.7. Architekturmuster 6: Verteilte Autorisierungsinfrastruktur auf FIM-Basis

FIM kann effizient dafür eingesetzt werden, bislang nur lokal verwendete Autorisierungssysteme zu koppeln. Dabei kann wie in Abbildung 4.32 dargestellt auf die FIM-Komponenten, die nicht im Zusammenhang mit Autorisierungsbestätigungen stehen, verzichtet werden.

Es kann, wenn nur diese Funktionalität benötigt wird, auch auf den Einsatz des FIM Privacy Management Systems verzichtet werden; dementsprechend sind auch föderationsweite Policies bezüglich der Freigabe von Autorisierungsbestätigungen unüblich, so dass die Schnittstelle zu den Föderationsmetadaten nur von der IDP- und der SP-Software benötigt wird.

4.10. Referenzarchitekturen

Auf den Architekturmustern aufbauend werden nachfolgend Referenzarchitekturen für die verschiedenen Rollen, die Organisationen in Föderationen einnehmen können, erarbeitet.

Aufgrund ihrer Komplexität bilden dabei die Identity und Service Provider den Schwerpunkt; sie werden in den Abschnitten 4.10.1 und 4.10.2 behandelt. Attribute Authorities stellen eine Teilmenge der Funktionalität von IDPs bereit; die entsprechende Referenzarchitektur wird in Abschnitt 4.10.3 vorgestellt und in Abschnitt 4.10.4 gegenüber den Authorization Providern abgegrenzt.

Eine sehr einfache Referenzarchitektur für Trusted Third Parties wird in Abschnitt 4.10.5 gezeigt; dies ist darauf zurückzuführen, dass die diskutierten föderationsweiten Dienste nahezu monolithisch aufgebaut sind. Bei der praktischen Umsetzung muss die Komplexität des TTP-Dienstes entsprechend berücksichtigt werden.

In Abschnitt 4.10.6 wird die Kombination der IDP- mit der SP-Referenzarchitektur beschrieben, um die Skalierbarkeit der Gesamtarchitektur zu demonstrieren; auf eine Vermischung weiterer Rollen wird verzichtet, da die prinzipielle Möglichkeit hierzu gewährleistet ist, sich daraus jedoch keine weiteren funktionalen Eigenschaften oder architekturellen Besonderheiten ergeben.

4.10.1. Referenzarchitektur Identity Provider

Die Referenzarchitektur für Identity Provider ist in Abbildung 4.33 dargestellt. Im linken Teil sind die I&AM-Komponenten angesiedelt, die im Wesentlichen auf Architekturmuster 3 zurückzuführen sind. Da der IDP im FIM-Kontext als Datenquelle fungiert, stehen die Quellsysteme im Vordergrund; IDP-interne I&AM-Zielsysteme sind in diesem Zusammenhang optional und wurden zur Verbesserung der Übersichtlichkeit nicht explizit dargestellt.

Den Self Services, dem Single Sign-On System und dem I&AM Privacy Management System kommen die bereits erläuterten Rollen zu, die im FIM-Umfeld weiter gestärkt werden. Sie sind somit sowohl im Hinblick auf Benutzerfreundlichkeit als auch auf die volle Ausschöpfung der FIM-Funktionalität unverzichtbar.

Die beteiligten FIM-Komponenten sind in der Abbildung im rechten Teil eingezeichnet. Die gesamtheitliche Koordination übernimmt dabei die IDP-Software, über die sämtliche FIM-Anfragen abgewickelt werden. Weitere zentrale Aufgaben übernehmen der Gateway zum lokalen Datenbestand und das FIM Privacy Management System: Der Gateway kanalisiert die Zugriffe auf das Identity Repository und steuert die Datenkonvertierung; das FIM Privacy Management System kontrolliert die Freigabe der Daten, bildet die Schnittstelle zum I&AM Privacy Management System und berücksichtigt föderationsweite Policies.

Der Möglichkeit zur Interaktion mit dem Benutzer ist wie erläutert unter anderem aus Datenschutzgründen essentiell; die Realisierung über eine dedizierte Komponente ermöglicht die erörterte differenzierte Behandlung von Situationen, in denen der Benutzer, über den Anfragen gestellt werden, nicht verfügbar ist.

Über die Integration des Privilege Management Systems können die Möglichkeiten verteilter Autorisierungsinfrastrukturen auf Basis von Autorisierungsbestätigungen genutzt werden

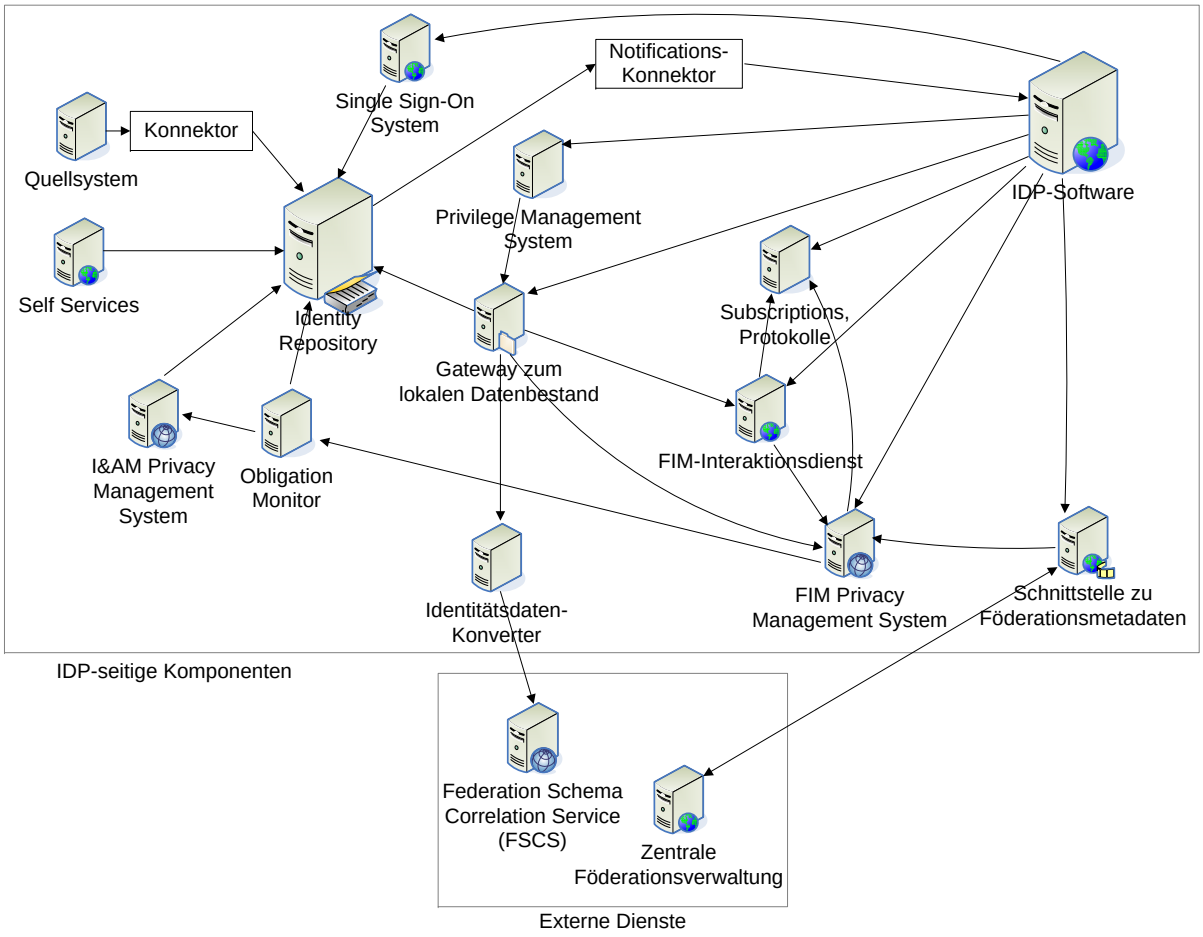


Abbildung 4.33.: Referenzarchitektur für Identity Provider

(vgl. Architekturmuster 6). Sofern das verwendete FIM-Protokoll Aktualisierungsbenachrichtigungen unterstützt, ermöglicht der Notifications-Konnektor im Zusammenspiel mit der IDP-Software und deren Subscriptions-Datenbasis die kontinuierliche organisationsübergreifende Konsistenzhaltung der Benutzerdaten.

4.10.2. Referenzarchitektur Service Provider

Abbildung 4.34 zeigt die Referenzarchitektur für Service Provider. Analog zum IDP ist links ein I&AM-System dargestellt, bei dem der Schwerpunkt auf den Diensten statt auf den Datenquellen liegt. Sofern mehrere Dienste angeboten werden, die nicht ausschließlich über FIM genutzt werden können, sollte ein Single Sign-On System eingesetzt werden. Die SP-seitigen Self Services sind notwendig, um Benutzern die Konfiguration beispielsweise dienstspezifischer Parameter zu ermöglichen, die nicht bei ihrem IDP vorgehalten werden. Dem SP-internen I&AM Privacy Management System kommt zur Kontrolle der zweckgemäßen Verarbeitung der Benutzerdaten eine wichtige Rolle zu.

Die FIM-Funktionalität wird von den in der Abbildung rechts dargestellten Komponenten

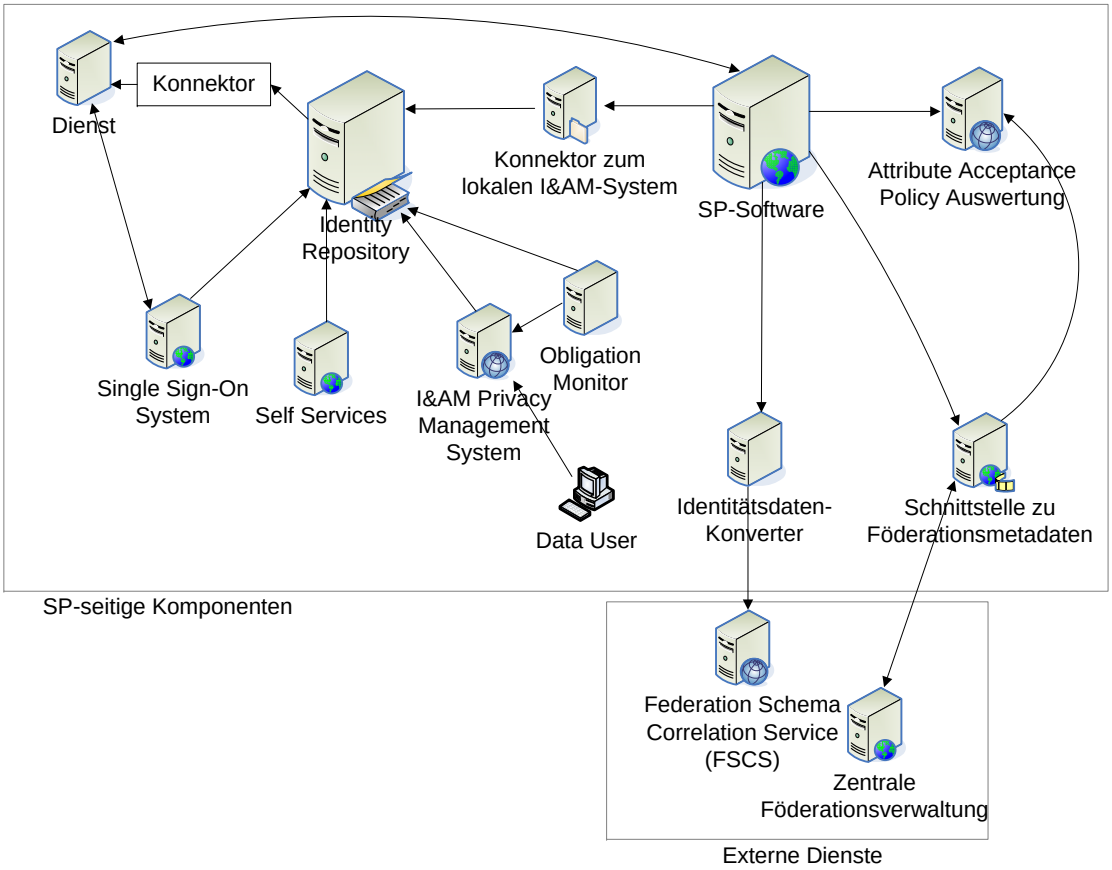


Abbildung 4.34.: Referenzarchitektur für Service Provider

erbracht. Alle FIM-Transaktionen werden von der SP-Software koordiniert; der Konnektor zum lokalen I&AM-System bildet die Schnittstelle zum Identity Repository. Komplementär zum IDP-seitigen FIM Privacy Management System, das die Attribute Release Policies auswertet, wird SP-seitig die Komponente zur Auswertung der Attribute Acceptance Policies eingesetzt. Der Identitätsdatenkonverter und die Schnittstelle zu den Föderationsmetadaten werden funktional analog zum IDP eingesetzt.

4.10.3. Referenzarchitektur Attribute Authority

In Abbildung 4.35 ist die Referenzarchitektur für Attribute Authorities dargestellt. Sie entspricht der Referenzarchitektur für Identity Provider, wobei jedoch z. B. auf Authentifizierungs- und Autorisierungskomponenten verzichtet wird.

Entsprechend fehlen das Single Sign-On System und das Privilege Management System. Auf die Self Services wird in der Referenzarchitektur ebenfalls verzichtet, da Attribute Authorities im Allgemeinen auch Informationen bereitstellen können, auf die ein Benutzer keinen direkten Einfluss hat.

Ferner sind einige der Komponenten als optional gekennzeichnet, da ihre Verwendung bei At-

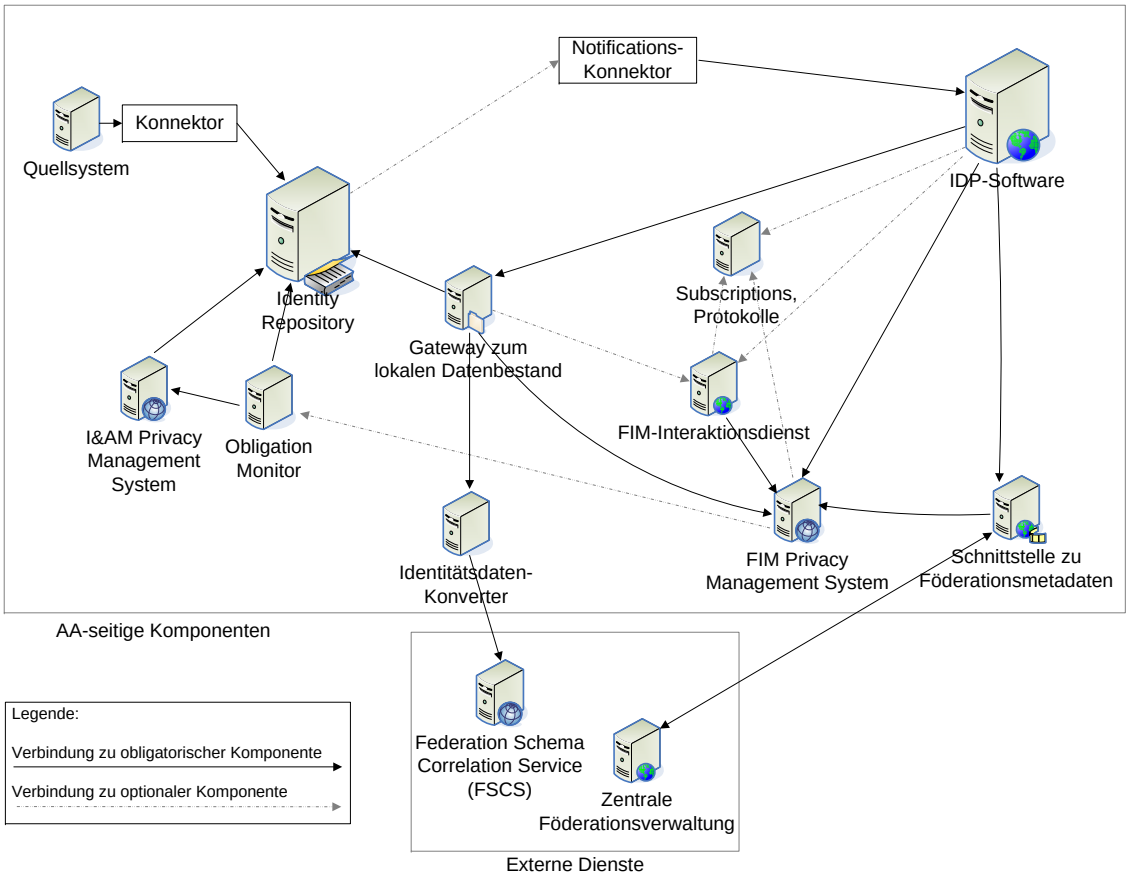


Abbildung 4.35.: Referenzarchitektur für Attribute Authorities

tribute Authorities derzeit als unüblich betrachtet werden kann: In der Regel werden Daten von AAs bei Bedarf abgerufen, so dass auf den Notifications-Konnektor und die Subscriptions-Datenbasis verzichtet werden kann; ebenso ist der Einfluss des Benutzers auf den Datenabruf meist stark begrenzt, so dass zumindest Langzeit-Obligationen und ggf. auch die Interaktion mit dem Benutzer entfallen können. Ein typisches Beispiel ist die Bonitätsprüfung eines Kunden durch eine AA vor Abschluss des Bestellvorgangs beim SP: In diesem Fall wird keine der optionalen Komponenten benötigt.

4.10.4. Referenzarchitektur Authorization Provider

Die in Abbildung 4.36 dargestellte Referenzarchitektur für Authorization Provider basiert im Wesentlichen auf Architekturmuster 6; sie unterscheidet sich davon lediglich durch die Berücksichtigung von Datenfreigaberegelungen, die ggf. auch durch die föderationsweiten Metadaten vorgegeben werden können.

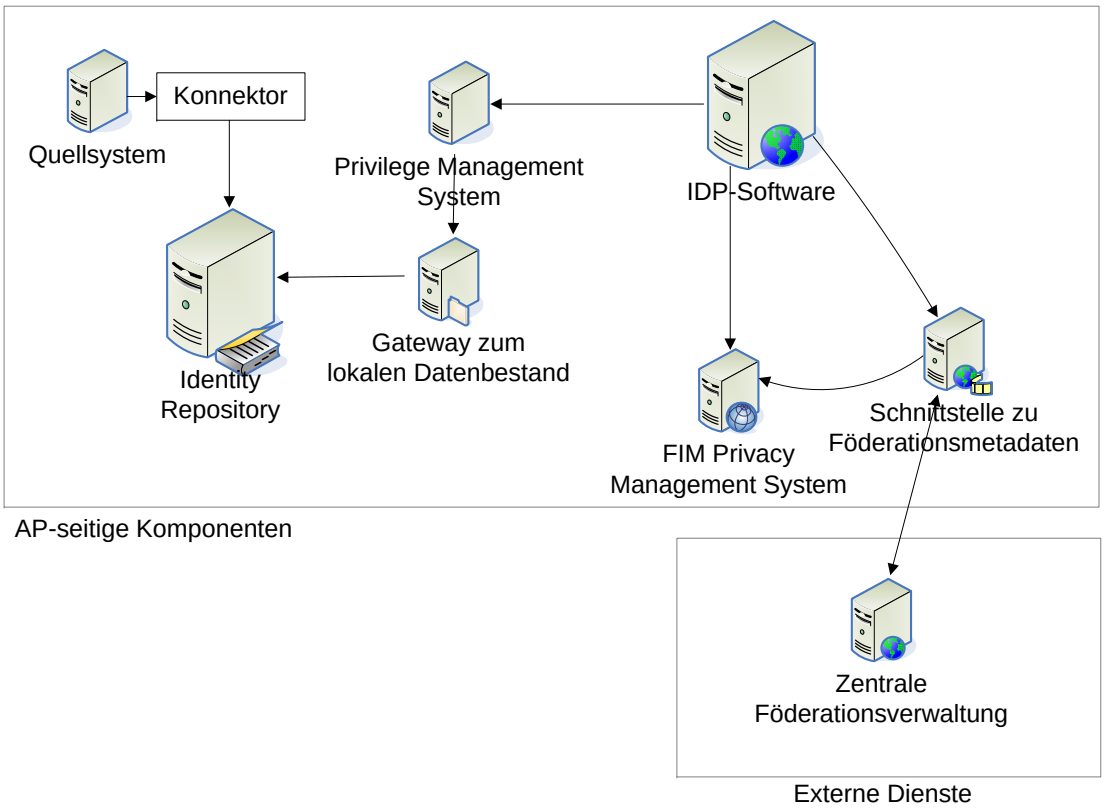


Abbildung 4.36.: Referenzarchitektur für Authorization Provider

4.10.5. Referenzarchitektur Trusted Third Party

Aufgrund der verschiedensten Möglichkeiten für Trusted Third Party Dienste zeigt Abbildung 4.37 lediglich eine einfache, allgemeine Architektur: Der TTP-Service ist von außen über Web Services erreichbar und berücksichtigt die Föderationsmetadaten, beispielsweise um Anfragen nur von Föderationsteilnehmern entgegenzunehmen. Der Dienst selbst wird auf Basis eines Datenbestandes erbracht, der entsprechend administriert werden kann.

Diese grundlegende Architektur kann auf den Federation Schema Correlation Service, den IDP Discovery Service und die zentrale Föderationsverwaltung selbst mit entsprechenden kleineren Anpassungen angewendet werden. Andere, in dieser Arbeit nicht näher betrachtete TTP-Services können selbstverständlich auch als komplexe verteilte Systeme realisiert werden; in diesen Fällen sind die Systeminterna, die in der Abbildung links neben dem TTP-Frontend dargestellt werden, entsprechend anzupassen.

4.10.6. Kombination der Referenzarchitekturen

Für den häufigen Fall, dass eine Organisation sowohl Identity Provider als auch Service Provider ist, wird die Kombination der beiden Referenzarchitekturen in Abbildung 4.38 dargestellt; die ebenfalls mögliche Kombination anderer Rollen wird hier aus den bereits genannten Grün-

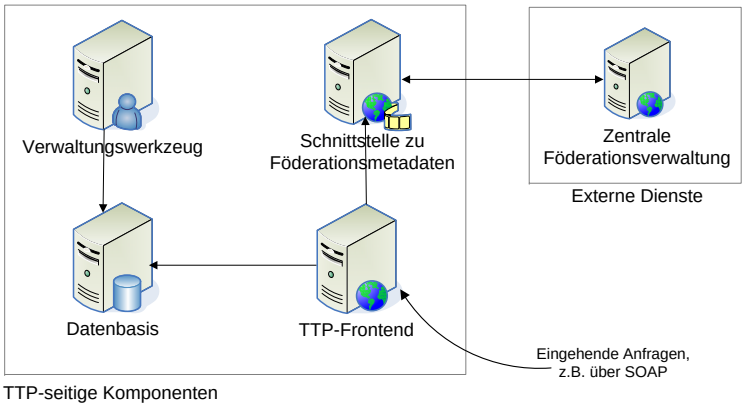


Abbildung 4.37.: Referenzarchitektur für Trusted Third Parties

den nicht vertieft.

Eine offensichtliche Anforderung an die Wahrnehmung beider Rollen ist, dass lediglich ein einziges lokales I&AM-System und insbesondere nur ein Identity Repository benötigt werden soll. Wie in der Abbildung dargestellt wird diese Anforderung ohne Zusatzaufwand erfüllt, auch wenn die Organisation in verschiedenen Föderationen als IDP bzw. SP auftritt. Ausschlaggebend hierfür ist die Entkoppelung der Zugriffe auf die lokalen Datenbestände über den Konnektor zum lokalen I&AM-System bzw. den Gateway zum lokalen Datenbestand. Aufgrund der ähnlichen Funktionsweise dieser beiden Komponenten liegt es – wie ebenfalls bereits erörtert wurde – nahe, sie zu einer gemeinsamen Instanz zusammenzufassen; in der Abbildung ist dies durch das gestrichelte Oval in der Mitte angedeutet.

Analog dazu können das FIM Privacy Management System und die dazu komplementäre Komponente zur Auswertung der Attribute Acceptance Policies ebenfalls zu einer Komponente zusammengefasst werden; dies ist in der Abbildung wiederum als Oval rechts unten dargestellt und insbesondere dann sinnvoll, wenn für ARPs und AAPs wie im Werkzeugkonzept in Kapitel 5 vorgesehen dieselbe Policysprache zum Einsatz kommt.

4.11. Bewertung auf Basis des Kriterienkatalogs

Zur Bewertung der erläuterten Architektur und zur Verdeutlichung der noch ungelösten Fragestellungen wird nachfolgend der in Kapitel 2 definierte Anforderungskatalog herangezogen. Bezugnehmend auf Abbildung 3.5 auf Seite 152 werden nur diejenigen Anforderungen genannt, die nicht bereits von allen FIM-Ansätzen unterstützt werden, da sich durch das vorgelegte Konzept diesbezüglich keine Verschlechterungen ergeben.

Bei den *essentiellen* Anforderungen ergeben sich folgende Veränderungen:

- [**FA-Interaktion**] Die FIM-Interaktionskomponente wurde IDP- und AA-seitig verpflichtend eingeführt. Sie orientiert sich bezüglich der technischen Umsetzung an der Liberty Alliance; ihre Aufgaben im Rahmen von FIM-Transaktionen wurden jedoch konkreter spezifiziert.

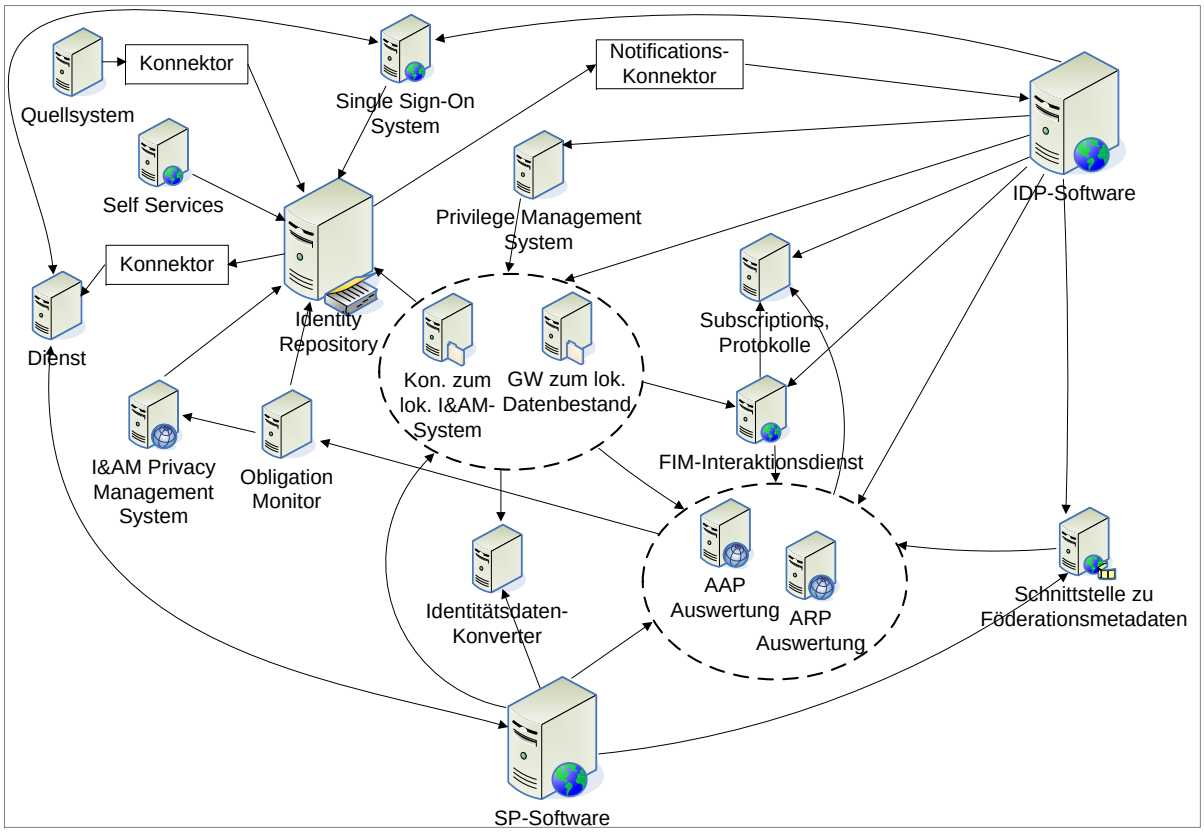


Abbildung 4.38.: Kombination der Referenzarchitekturen

- [**DSA-ARPs**] Die Berücksichtigung von Attribute Release Policies wurde ebenfalls IDP- und AA-seitig verpflichtend eingeführt. Die von dem in Abschnitt 5.3 vertiefend diskutierten FIM Privacy Management System bereitgestellten Möglichkeiten gehen deutlich über die bisherigen Konzepte der Liberty Alliance und die Umsetzung in Shibboleth hinaus.

Die Situation bei den *wichtigen* Anforderungen verhält sich wie folgt:

- [**FA-Konnektor**] Mit der SP-seitigen Einführung des Konnektors zum lokalen I&AM-System und der IDP-/AA-seitigen Verwendung des Gateways zum lokalen Datenbestand wird diese Anforderung voll erfüllt.
- [**FA-Korrelation**] Die Funktionalität zur SP-seitigen Korrelation von Benutzerdatenbeständen kann wie in I&AM-Systemen in den Konnektor zum lokalen I&AM-System integriert werden. Die von einigen FIM-Ansätzen bereitgestellten Mechanismen zur benutzergesteuerten Korrelation können ergänzend eingesetzt werden.
- [**FA-Schema**] Über den Identitätsdatenkonverter, der in Abschnitt 5.2 vertiefend erläutert wird, können die mittels FIM übertragenen Daten in das lokal verwendete Schema konvertiert werden; die Anforderung wird somit voll erfüllt.

- [**FA-Schreibzugriff**] Die Schnittstellen für Schreibzugriffe sind in dieser Architektur vorgesehen und es wurden die entsprechenden Datenflüsse und Benutzerinteraktionen beschrieben.

- [**FA-Updates**] Das von der Liberty Alliance bereitgestellte Konzept der *Subscriptions & Notifications* wurde mit dem Notifications-Konnektor konkretisiert, der als optionale IDP- bzw. AA-seitige Komponente eingeführt wurde.

- [**NFA-Dokumentation**] Da insbesondere SAML, die Liberty Alliance und Shibboleth die Grundlagen des Architekturkonzepts darstellen, wird diese Anforderung als erfüllt bewertet.

- [**NFA-Management**] Mit der Integration der über FIM akquirierten Benutzerdatensätze in das SP-seitige I&AM-System wurde der Grundstein für eine Weiterverwendung der bislang eingesetzten Managementwerkzeuge gelegt. Darüber hinaus wurden die Managementaspekte der FIM-Komponenten skizziert. Da keine vertiefende Betrachtung erfolgte, wird diese Anforderung als partiell erfüllt angesehen.

- [**NFA-Usability**] Über das Zusammenspiel von Attribute Release Policies und Interaktion mit dem Benutzer wurden die Grundzüge festgelegt, die flexibler als die bisherigen Ansätze sind (vgl. Abschnitt 3.6). Die konkrete Gestaltung von Benutzeroberflächen wurde jedoch bewusst nicht untersucht, so dass die Anforderung als nur partiell erfüllt gelten kann.

- [**SEC-Auditing**] Die SP-seitige Nachvollziehbarkeit, welche Benutzer von welchen IDPs stammen und welche Dienste sie nutzen, wird einerseits über die Integration ins I&AM-System ermöglicht, andererseits wurden die Möglichkeiten zur Protokolldateiauswertung erläutert. Die Anforderung wird damit ebenso wie von der Liberty Alliance, WS-Federation und Shibboleth erfüllt.

- [**SEC-IDP-Systemsicherheit**] Die Maßnahmen zur Absicherung der IDP-seitigen Komponenten und insbesondere der IDP-Software wurden erläutert; analog zur Liberty Alliance, WS-Federation und Shibboleth wird die Anforderung somit erfüllt.

- [**SEC-Integration**] Die Integration in Netzwerksicherheitsinfrastrukturen wurde bei jeder Komponente sowie in Abschnitt 4.7 dargelegt.

- [**ORG-Datennutzung**] Durch die Einspeisung der Daten ins SP-seitige I&AM-System wird ihre Weiterverarbeitung durch andere Prozesse prinzipiell ermöglicht. Die Anforderung wird dadurch weitgehender unterstützt als bei den bisherigen FIM-Ansätzen, aufgrund der nicht vollständigen Betrachtung hier jedoch als nur partiell erfüllt gewertet.

- [**ORG-Föderationsmodelle**] Das Architekturmodell schränkt die möglichen Föderationsmodelle nicht ein; die Anforderung gilt somit wie bei den anderen Ansätzen (bis auf Shibboleth) als erfüllt.

- [**ORG-Migration**] Als Bestandteil der Integrationsmethodik wurde in Abschnitt 4.6 ein entsprechender Migrationspfad aufgezeigt.

- [**ORG-Registrierung**] Diese Anforderung wird durch die Interaktionsmechanismen mit dem Benutzer und die Einspeisung ins SP-seitige I&AM-System analog zur Liberty Alliance erfüllt.

- [**ORG-SLAs**] Durch die Trennung der Möglichkeit zur FIM-basierten Kommunikation durch die Eintragung in die Föderationsmetadaten und die differenzierte Vergabe von Berechtigungen an Organisationen, z. B. in Form von ARPs und AAPs, werden die Vereinbarung von Dienstgüteparametern und deren Überwachung ermöglicht und gefördert. Die Inhalte und das Management von SLAs wurden jedoch nicht vertieft, so dass die Anforderung nur partiell erfüllt wird.

- [**ORG-Supportprozesse**] Die Auswirkungen auf und die Integration in die IT Service Support Prozesse wurden in Abschnitt 4.8 am Beispiel des sehr wichtigen Change Management Prozessen erläutert. Eine entsprechende Analyse bezüglich der anderen Prozesse bleibt bewusst Nachfolgearbeiten überlassen, so dass diese Anforderung nur partiell erfüllt wird.

- [**DSA-DefaultARPs**] Analog zu Shibboleth werden von der in Abschnitt 5.3 spezifizierten FIM Privacy Management Komponente administrative Voreinstellungen für ARPs ermöglicht, deren Flexibilität im Hinblick auf verteilte Administration die bisherigen Möglichkeiten wesentlich erweitert.

- [**DSA-Schreibzugriff**] Die FIM-Interaktionskomponente sieht den Anwendungsfall vor, dass Benutzer den Inhalten von SP-seitig initiierten Schreibzugriffen auf die bei IDPs bzw. AAs hinterlegten Profile zustimmen können sollen. Die Anforderung wird somit erfüllt.

Für die empfehlenswerten Anforderungen ergeben sich die folgenden Konsequenzen:

- [**FA-Abhängigkeiten**] Durch die Einspeisung der Benutzerdaten in das I&AM-System werden SP-interne Dienstabhängigkeiten implizit erfüllt (vgl. Abschnitt 4.4.9).

- [**FA-AccountLinking**] Für die initiale Verknüpfung von Benutzerkennungen bei IDP und SP kann neben den von den FIM-Ansätzen bislang schon angebotenen Möglichkeiten auch auf die Korrelation im Konnektor zum lokalen I&AM-System zurückgegriffen werden (vgl. Anforderung [FA-Korrelation]). Die Anforderung wird somit erfüllt.

- [**FA-Delegation**] Die Delegation von Berechtigungen wurde wie die übrigen Interna des Privilege Management Systems in diesem Konzept nicht betrachtet, aber auch nicht erschwert. Die Anforderung wird jedoch noch nicht erfüllt.

- [**FA-IDP-Antwortvorschlag**] Der Interaktionsschritt zur Abstimmung der vom IDP gelieferten Antwort auf Anfragen mit dem Benutzer ist im Workflow, der in Abschnitt 4.4.3.2 beschrieben wird, vorgesehen. Die zu verwendenden Algorithmen und Benutzeroberflächen wurden jedoch nicht diskutiert, so dass die Anforderung nur ansatzweise erfüllt wird; diesbezüglich wäre beispielsweise eine Orientierung an UCIM-Systemen möglich.

- [**FA-Identitätswahl**] Das in Abschnitt 5.3 vorgestellte ARP-Konzept unterstützt mehrere Identitäten und Rollen pro Person, zwischen denen beispielsweise beim Authentifizierungsvorgang über das SSO-System ausgewählt werden kann. Implikationen, die sich aus der Verwaltung mehrerer Identitäten bei einem einzigen IDP ergeben können, wurden jedoch nicht ausreichend untersucht, so dass die Anforderung nur als partiell erfüllt angesehen wird.

- [**FA-Import/Export**] Der Im- und Export von Attributszertifikaten wurde wie bei den anderen FIM-Ansätzen nicht explizit betrachtet, so dass diese Anforderung nicht erfüllt wird. Es bietet sich an, diese Funktionalitäten als FIM-spezifische Erweiterungen der Self Services zu realisieren, wobei die Zusammenhänge mit der Anforderung [FA-IDP-Antwortvorschlag] zu berücksichtigen sind.

- [**FA-Pull&Push**] Die Funktionalität, Daten sowohl in einem Push- als auch in einem Pull-Verfahren übertragen zu können, ist analog zu SAML vorgesehen (vgl. Abschnitt 4.4.1.1). Die Anforderung wird somit erfüllt.

- [**FA-UserOffline**] Durch die parallele Unterstützung direkter und über den Benutzerclient mittelbarer Kommunikation wird die Anforderung erfüllt; die Auswirkungen, die sich durch fehlende Interaktionsmöglichkeiten zwangsweise ergeben, wurden ebenfalls diskutiert.

- [**FA-Zusatzdaten**] Die Bereitstellung föderationsspezifischer Benutzerattribute wurde im Rahmen des Integrationskonzepts skizziert; die entsprechenden Aspekte der organisationsinternen Datenmodellierung und ihr Zusammenspiel mit den ARPs müssten jedoch noch vertiefend untersucht werden, so dass diese Anforderung nur partiell erfüllt wird.

- [**SEC-ARPs**] Die Anforderung wird durch das in Abschnitt 5.3 vorgestellte Werkzeugkonzept erfüllt.

- [**SEC-Benutzerauthentifizierung**] Diese Anforderung wird erfüllt, da die IDP-Software bei Anfragen zu Authentifizierungsbestätigungen Anforderungen hinsichtlich des zu verwendenden Authentifizierungsverfahrens entgegennehmen kann (vgl. Abschnitt 4.4.1.1).

- [**SEC-Benutzerkreis**] Da die Attribute Release Policies von der IDP-Software auch auf Authentifizierungsbestätigungen angewandt werden, wird diese Anforderung ohne Einschränkungen erfüllt.

- [**SEC-Genehmigung**] Die Unterstützung SP-seitiger Genehmigungsworkflows wurde nicht explizit betrachtet; die Anforderung wird somit nicht erfüllt. Die Einspeisung ins lokale I&AM-System bildet den Ausgangspunkt für weiterführende Betrachtungen.

- [**SEC-Trust**] Die Umsetzung einer differenzierten Berechtigung von SPs zum Abruf von Daten beim IDP und bei AAs wird durch das in Abschnitt 5.3 vorgestellte ARP-Konzept erleichtert. Es wurden jedoch keine Methoden zur dynamischen Parametrisierung der so formalisierten Vertrauensbeziehungen untersucht, da diese Gegenstand anderer Arbeiten sind; die Anforderung wird derzeit somit nur partiell erfüllt.

- [**SEC-Unleugbarkeit**] In Abschnitt 4.7.1 wurde erläutert, dass die organisationsübergreifende Korrelation von FIM-Protokolldaten derzeit noch nicht möglich ist. Die Anforderung wird somit ebenso wenig wie von den anderen Ansätzen erfüllt.
- [**SEC-Workflowentkopplung**] Die Entkopplung IDP- und SP-seitiger Workflows wird auf Basis der erfüllten Anforderungen [FA-Pull&Push] und [FA-UserOffline] sowie die Einspeisung der Daten ins SP-seitige I&AM-System ohne Einschränkungen ermöglicht.
- [**SEC-Übertragungswege**] Wie bei der Beschreibung der davon betroffenen Komponenten erläutert wurde, wird sowohl die direkte als auch die über den Benutzerclient mittelbare Kommunikation ermöglicht.
- [**ORG-Trust**] Das der Architektur zugrundeliegende, in Abschnitt 4.1.2 beschriebene Verständnis von Föderationen zielt genau auf die hier geforderte individuelle Bestimmung des Vertrauensgrades zwischen Föderationsteilnehmern ab.
- [**ORG-Verweisgüte**] In Abschnitt 4.4.1.1 wurde gezeigt, dass Garantien bezüglich der Qualität der von einer AA gelieferten Daten durchaus im Rahmen der Anfragebearbeitung in entsprechende Attributsauskünfte aufgenommen werden können. Die Anforderung wird jedoch nur partiell erfüllt, da die Methoden zur Bestimmung des Vertrauensgrades analog zur Anforderung [SEC-Trust] nicht untersucht wurden.
- [**DSA-Anonymisierung**] Der Fall, dass Benutzerdaten z. B. für statistische Auswertungen anonymisiert weitergegeben werden sollen, wurde nicht explizit betrachtet, so dass die Anforderung nicht erfüllt wird. Als Ausgangsbasis für entsprechende weiterführende Arbeiten kann der Identitätsdatenkonverter herangezogen werden, der mit geeigneten anonymisierenden Konvertierungsregeln parametrisiert werden müsste.
- [**DSA-Attributszertifikate**] Analog zu [FA-Import/Export] wird diese Anforderung noch nicht erfüllt.
- [**DSA-Delegation**] Die benutzerkontrollierte Weitergabe von personenbezogenen Daten durch SPs an Dritte wird durch die vorgestellte Architektur weder explizit ermöglicht noch verhindert, sondern dem eingesetzten FIM-Ansatz überlassen. Die Anforderung wird somit aufgrund der Anlehnung an SAML als nicht erfüllt bewertet.
- [**DSA-Obligationen**] Das in Abschnitt 5.3 vorgestellte ARP-Konzept unterstützt Obligationen; darüber hinaus wurde die Anbindung an den Obligation Monitor eines Privacy Management Systems erläutert.
- [**DSA-Selbstbestimmung**] Das optionale Festhalten der Information, welcher SP wann welche Daten abgerufen hat, und die Einsichtnahme in diese Daten durch Benutzer werden von der IDP-Software, der FIM-Interaktionskomponente sowie ggf. den Self Services voll unterstützt.
- [**DSA-Unlinkability**] Die Verwendung einmaliger Pseudonyme wird durch die IDP-Software ohne Einschränkungen ermöglicht.
- [**DSA-Zustimmung**] Die IDP-Software bietet im Zusammenspiel mit der FIM-Interaktionskomponente die Möglichkeit zur Einholung der Zustimmung des Benutzers zu den entsprechenden Richtlinien der SP-seitig angebotenen Dienste; die Anforderung wird somit erfüllt.

In Abbildung 4.39 wird diese Bewertung den Ergebnissen von Kapitel 3 gegenübergestellt. Sie zeigt, dass zumindest auf konzeptioneller Ebene alle essentiellen Anforderungen ganz und alle wichtigen Anforderungen mindestens partiell erfüllt werden können. Für viele der noch nicht bzw. noch nicht vollständig erfüllten Anforderungen wurden mögliche Ansatzpunkte von Folgearbeiten skizziert.

Die Verbesserungen hinsichtlich des Erfüllungsgrades der Anforderungen ergeben sich einerseits durch die aufgezeigte Integration von FIM-Komponenten in I&AM-Infrastrukturen; andererseits wurden gezielt neue, in den bisherigen FIM-Ansätzen nicht vorgesehene Komponenten eingeführt, die zusätzlich benötigte Funktionalität bereitstellen. Der Identitätsdatenkonverter und das FIM Privacy Management System, die in diesem Kapitel als Black Box betrachtet wurden, werden im nächsten Kapitel detaillierter spezifiziert.

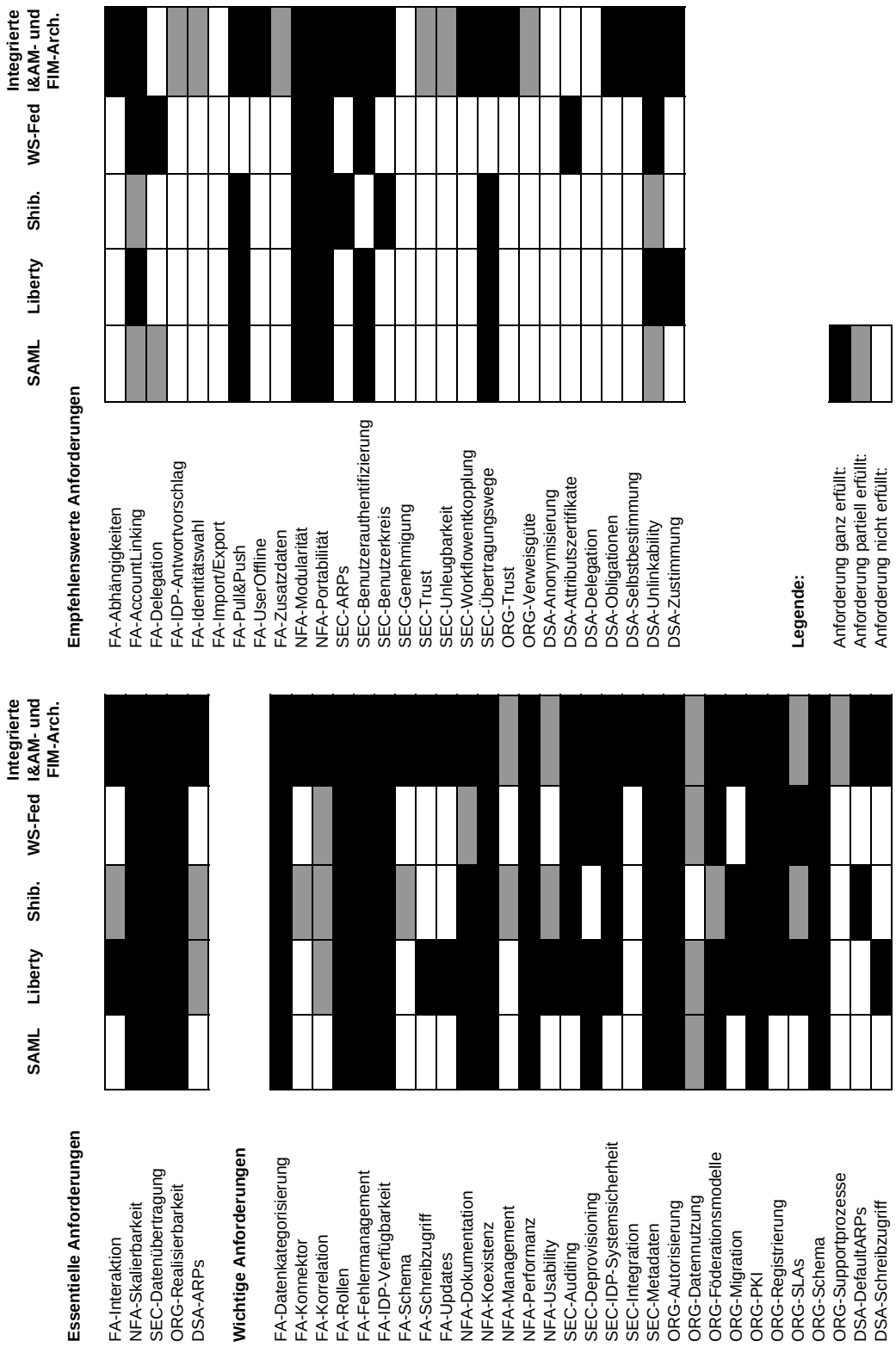


Abbildung 4.39.: Bewertung des Architekturkonzepts auf Basis des Kriterienkatalogs

Kapitel 5.

FIM-Werkzeugkonzepte

Inhalt dieses Kapitels

In dem in Kapitel 4 erörterten Architekturkonzept wurden mehrere neue FIM-Komponenten eingeführt und einige der in den FIM-Industriestandards bereits spezifizierten Komponenten funktional erweitert. Der Schwerpunkt der Betrachtung lag dabei auf der grundlegenden Funktionalität, den Schnittstellen zu und dem Zusammenspiel mit den anderen Komponenten sowie der Integration in das Security und Change Management. In diesem Kapitel werden einige **ausgewählte dieser neuen FIM-Komponenten** im Detail spezifiziert, wobei in Abschnitt 5.1 zunächst die Selektion dieser Komponenten und die Zielsetzung der Werkzeugkonzepte erläutert werden.

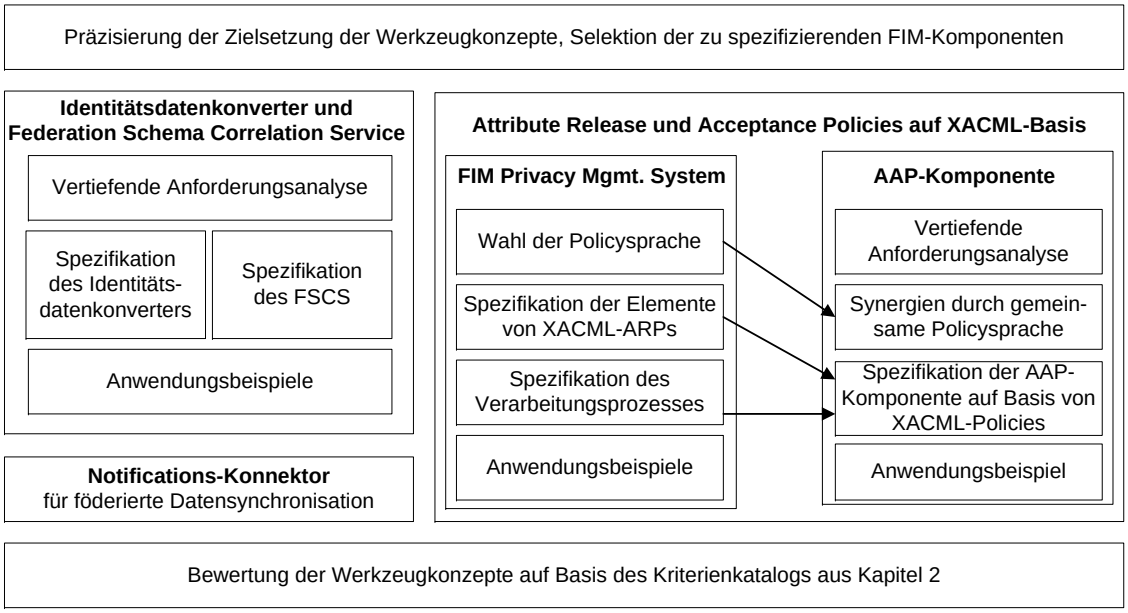


Abbildung 5.1.: Vorgehensmodell in diesem Kapitel

Eine wesentliche Rolle im Hinblick auf die Flexibilität und Skalierbarkeit der FIM-basierten Kommunikation spielen der **Identitätsdatenkonverter** und seine enge Kooperation mit dem **Federation Schema Correlation Service**; beide Komponenten werden in Abschnitt 5.2 vertieft.

Die Steuerung von Datenfreigaben erfolgt über die bereits erläuterten Attribute Release Policies (ARPs); in Abschnitt 5.3 wird nach einer eingehenden Analyse der relevanten Anforderungen und potentieller Lösungsansätze darauf eingegangen, wie die sehr flexible Policysprache XACML effektiv für die **Modellierung und Umsetzung von ARPs** eingesetzt werden kann. Dabei wird neben der Spezifikation der genauen, ARP-spezifischen Verwendung der einzelnen Policyelemente auch der Workflow bei der Auswertung der ARPs spezifiziert. In Abschnitt 5.4 wird dieses Konzept auf die SP-seitig eingesetzten Attribute Acceptance Policies (AAP) übertragen und verdeutlicht, wie Synergien durch die **Nutzung einer gemeinsamen Policysprache für ARPs und AAPs** ausgenutzt werden können.

Zur Sicherstellung der organisationsübergreifenden Datenkonsistenz spielt die föderierte Datensynchronisation eine elementare Rolle; in Abschnitt 5.5 werden deshalb das Innenleben des **Notifications-Konnektors** und die von ihm angestoßenen Datenflüsse spezifiziert.

In Abschnitt 5.6 erfolgt schließlich eine zusammenfassende Bewertung dieser neuen Komponenten auf Basis des Kriterienkatalogs, bei der im Unterschied zur Übersicht am Ende von Kapitel 4 vertiefend auf die relevanten Anforderungen an die hier spezifizierten neuen FIM-Komponenten eingegangen wird.

Abbildung 5.1 zeigt eine Zusammenfassung des Vorgehensmodells in diesem Kapitel.

5.1. Präzisierung der Zielsetzung der Werkzeugkonzepte

In Abbildung 4.4 auf Seite 170 wird wie bereits erläutert dargestellt, an welchen Stellen diese Arbeit in bestehende FIM-Ansätze eingreift. In Kapitel 4 wurden die unverändert übernommenen und die nur konfigurationsseitig angepassten Komponenten bereits so beschrieben, dass eine weiter vertiefende Betrachtung zu keinen wesentlichen neuen Ergebnissen führen würde. Aus diesem Grund konzentriert sich dieses Kapitel auf solche Komponenten, die im Rahmen dieser Arbeit stärker modifiziert bzw. neu eingeführt wurden.

In der folgenden Übersicht wird begründet, warum nachfolgend nur auf ausgewählte und nicht alle dieser Komponenten eingegangen wird:

- Die IDP- und die SP-Software wurden jeweils um einige Zusatzfunktionen ergänzt, die eine bessere Unterstützung der bereits vorhandenen lokalen Bestandteile organisationsübergreifender Geschäftsprozesse ermöglichen. Hierzu gehören beispielsweise der Schreibzugriff auf IDPs, durch den die SP-lokale Datenhaltung abgelöst werden kann, und das Einholen der Zustimmung zu den SP-seitigen Benutzerrichtlinien, die Prozesse zur Benutzerregistrierung bei SPs unterstützt. Da jedoch Schreibzugriffe wie beschrieben analog zu Lesezugriffen gehandhabt werden und die Übertragung der Benutzerrichtlinien vom SP zum IDP keine weiteren FIM-spezifischen Besonderheiten aufweist, erübrigt sich eine eingehendere Betrachtung außerhalb eines konkreten Implementierungskonzepts.

- Die Schnittstelle zu den Föderationsmetadaten und die zentrale Föderationsverwaltung wurden im Wesentlichen um die Unterstützung eines Push- anstelle eines Pull-Verfahrens und um die Möglichkeit zur Distribution föderationsweiter ARPs und AAPs ergänzt. Die Umsetzung eines Push-Verfahrens für die Verteilung und dezentrale Aktualisierung von Datenbeständen ist nicht FIM-spezifisch, so dass diesbezüglich ggf. auf Lösungen aus anderen Bereichen zurückgegriffen werden kann. Föderationsweite Policies werden im Rahmen von ARPs und AAPs berücksichtigt (siehe Abschnitt 5.3).

- Der **Notifications-Konnektor** stellt wie bereits im Architekturkonzept beschrieben einen FIM-spezifischen Sonderfall herkömmlicher I&AM-Konnektoren dar, anhand dessen das **Zusammenspiel von I&AM- und FIM-Komponenten** gut veranschaulicht werden kann. Zudem wird durch ihn eine in FIM-Standards noch nicht vorgesehene bzw. nicht konkretisierte Funktionalität ermöglicht; er wird deshalb in Abschnitt 5.5 spezifiziert.

- Der FIM-Interaktionsdienst wird wie in Kapitel 4 erläutert bewusst nicht vertieft, da sein Schwerpunkt auf der Gestaltung von Benutzeroberflächen unter Usabilityaspekten und somit nicht im Fokus dieser Arbeit liegt.

- Für den IDP-seitigen Gateway zum lokalen Datenbestand und das Zusammenspiel der SP-Software mit dem SP-seitigen Konnektor zum lokalen I&AM-System gilt analog, dass ihre Arbeitsweise im Architekturkonzept bereits ausführlich dargestellt wurde; eine Besonderheit besteht in der Verwendung des Identitätsdatenkonverters, auf den nachfolgend eingegangen wird.

- Der **Identitätsdatenkonverter** und der **Federation Schema Korrelation Service** stellen neu eingeführte Komponenten dar, die das gesamte **Architekturkonzept maßgeblich prägen**. Auf sie wird deshalb in Abschnitt 5.2 genauer eingegangen.

- Das IDP-seitige **FIM Privacy Management System** und die SP-seitige **Komponente zur Auswertung von Attribute Acceptance Policies** wurden auf Basis der Policysprache XACML **von Grund auf neu konzipiert**. Die exakte Verwendung von XACML und die internen Schritte zur Auswertung aller für eine Anfrage relevanten Policies werden deshalb für ARPs und AAPs in den Abschnitten 5.3 und 5.4 erläutert.

Der Detaillierungsgrad der Spezifikationen in den nachfolgenden Abschnitten soll vergleichbar mit einem Fachkonzept als Vorstufe eines Implementierungskonzeptes dienen und die konkrete Verwendung der jeweiligen Komponente im Sinn des Gesamtkonzepts ermöglichen. Während in diesem Kapitel nicht auf konkrete FIM-Lösungen und -Produkte eingegangen wird, werden die prototypischen Implementierungen und die dabei auftretenden Einschränkungen in Kapitel 6 beschrieben.

Im Hinblick auf die im Architekturkonzept definierten Schnittstellen zu den anderen Komponenten muss bewusst sein, dass die hier vorgestellten Werkzeugkonzepte eine mögliche, aber nicht die einzige Lösungsvariante für die genannten Aufgaben darstellen. Insbesondere im stärker umforschten Bereich des Privacy Managements wird deshalb auf Alternativkonzepte für Teilprobleme verwiesen und diskutiert, welche Vorteile die hier erarbeitete ARP- und AAP-Gesamtlösung mit sich bringt.

5.2. Identitätsdatenkonverter und Federation Schema Correlation Service

Diese Komponente wird in der Gesamtarchitektur genau dann benötigt, wenn mindestens einer der Föderationsteilnehmer intern ein von den anderen abweichendes Datenmodell verwendet. Wie bereits in Abschnitt 3.8 erläutert wurde, ist im Allgemeinen von vielen heterogenen Datenmodellen auszugehen, die sich zwar teilweise nur minimal – z. B. bezüglich der Namensgebung von Attributen – voneinander unterscheiden mögen, aber die uneingeschränkte Interoperabilität dennoch verhindern. Der Identitätsdatenkonverter ist somit offensichtlich eine essentielle Komponente. Mit zunehmender Anzahl von Föderationen, an denen eine Organisation beteiligt ist, und der entsprechenden Vielzahl potentieller FIM-Kommunikationspartner steigt zwangsweise auch die Anzahl der zu pflegenden Konvertierungsregeln; der damit verbundene Managementaufwand wird durch den Federation Schema Correlation Service (FSCS), der als Trusted Third Party Service fungiert, reduziert.

Zur Konkretisierung der grundlegenden Problematik und des Lösungskonzepts werden in Abschnitt 5.2.1 **Anforderungen** an den Konverter und den FSCS definiert; die **Spezifikation** der beiden Komponenten ist Gegenstand der Abschnitte 5.2.2 und 5.2.3. Abschließend werden in Abschnitt 5.2.4 einfache konkrete **Anwendungsbeispiele** gegeben.

5.2.1. Anforderungen an den Identitätsdatenkonverter und den FSCS

In den nachfolgenden Abschnitten 5.2.1.1 bis 5.2.1.3 werden Anforderungen an den Identitätsdatenkonverter, den FSCS sowie ihr Zusammenspiel hergeleitet. Dazu werden die **Spezifika des FIM-Kommunikationsverhaltens** und die notwendige **Funktionalität auf Datenkonvertierungsebene** untersucht sowie grundlegende Anforderungen an die **Wiederverwendbarkeit von Konvertierungsregeln** analysiert.

5.2.1.1. Spezifika der FIM-Kommunikation

Der Identitätsdatenkonverter widmet sich der bei verteilten Systemen klassischen Aufgabe, dass sich Absender und Empfänger unabhängig vom gewählten Kommunikationsprotokoll und den darunter liegenden Netzwerkschichten auf die Syntax und Semantik der übertragenen Nutzdaten einigen müssen. Hierzu bestehen die beiden grundlegenden Möglichkeiten, dass entweder einer der Kommunikationspartner das Format des anderen beherrschen muss oder dass beide auf ein gemeinsames drittes Datenübertragungsformat zurückgreifen. Die letztere Variante ist in der Praxis meist besser geeignet und weiter verbreitet, da sie bei einer großen Anzahl an Kommunikationspartnern und unterschiedlichen lokalen Datenformaten besser skaliert – jeder der n Teilnehmer muss nur die Konvertierung der Daten von bzw. in *ein* Format unterstützen und nicht bis zu $n - 1$ verschiedene.

Dieser Ansatz entspräche im FIM-Kontext der **Definition eines föderationsweiten Datenmodells**, das von allen Föderationsteilnehmern unterstützt werden muss. In der Praxis sind jedoch **weitere Randbedingungen und komplexere Konstellationen** zu berücksichtigen:

- Eine Organisation kann an mehr als einer Föderation teilnehmen. Die dabei zum Einsatz kommenden föderationsweiten Datenmodelle können sich bereits bezüglich der Auswahl der definierten Attribute unterscheiden, so dass im Allgemeinen davon ausgegangen werden muss, dass pro Föderation ein anderes Datenmodell eingesetzt wird, auch wenn **partielle Überlappungen** nicht unwahrscheinlich sind. Die föderationsübergreifende, globale Verwendung eines einzigen gemeinsamen Datenmodells ist hingegen aus heutiger Sicht utopisch, da in der Praxis zur Aufwandsreduktion meist **minimale**, aber somit zwangsweise **anwendungsdomänenspezifische Lösungen** angestrebt werden und **konfliktäre Anforderungen** nicht auszuschließen sind.
- Das Kommunikationsverhalten zwischen den Föderationsteilnehmern darf nicht außer Acht gelassen werden: Die Daten werden **primär zwischen IDPs** bzw. AAs **und SPs** ausgetauscht; sekundär ergeben sich **vereinzelte Datenflüsse zwischen SPs** aufgrund von Dienstabhängigkeiten und Delegationen, wohingegen IDPs und AAs untereinander gar nicht kommunizieren, sofern die jeweiligen Organisationen nicht parallel auch als SPs fungieren – für diese Teilnehmerpaare sind entsprechend auch keine Datenkonvertierungen erforderlich. Abbildung 5.2 zeigt ein einfaches Beispiel, anhand dessen deutlich wird, dass die Kommunikationsbeziehungen in Föderationen mit Ausnahme von Delegationen als **bipartiter Graph** dargestellt werden könnten.
- Die Definition eines föderationsweiten Datenmodells stellt bei einer größeren Anzahl an Föderationsteilnehmern eine nicht triviale Herausforderung dar: Die rein technische

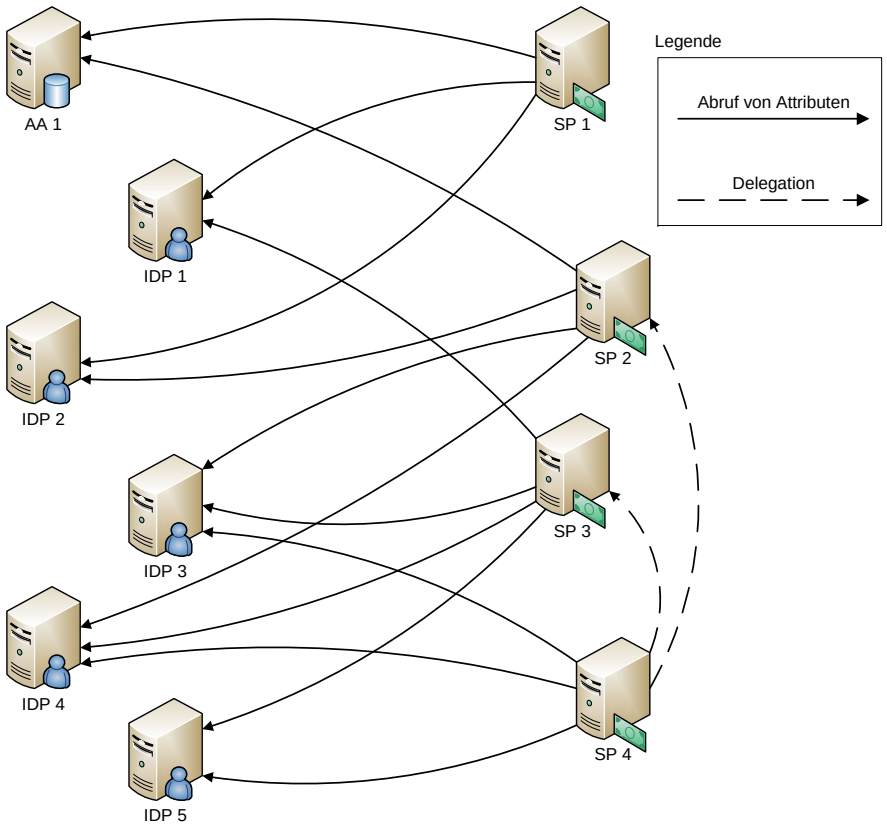


Abbildung 5.2.: Einfaches Beispiel für das charakteristische FIM-Kommunikationsverhalten

Aufgabe einer gemeinsamen Datenmodellierung rückt in der Praxis häufig durch organisatorische und unternehmenspolitische Randbedingungen in den Hintergrund, z. B. indem das Beharren auf eigenen Vorschlägen mit der Vorrangstellung der eigenen Organisation oder den ansonsten anfallenden Implementierungskosten begründet wird.

Analoge Argumente gelten einerseits, wenn Föderationen sehr dynamisch bzw. offen gestaltet sind, und andererseits, wenn wichtige Service Provider in eine Föderation aufgenommen werden sollen, die sich dem dort gewählten Datenmodell aber nicht anpassen können oder wollen. In einigen Szenarien ergibt sich in der Praxis zudem das Problem, dass FIM zwar eine Verbesserung, aber keine Notwendigkeit darstellt, so dass keine zwingenden Argumente für eine rasche Konsensbildung vorliegen.

- Die Vielfalt an in der Föderation vertretenen Datenmodellen kann wiederum dadurch eingeschränkt werden, dass **Teilmengen der Föderationsteilnehmer** lokal identische Datenformate einsetzen; zwei praktische Beispiele hierfür sind Firmen mit I&AM-Lösungen vom selben Hersteller ohne eigene Anpassungen und Hochschulen, die eine gemeinsame I&AM-Lösung erarbeiten: Am CODEX-Projekt sind beispielsweise alle Universitäten und Fachhochschulen des Bundeslands Thüringen beteiligt.[1]

[1] Siehe `http://www.tu-ilmenau.de/metadirectory`.

Bereits diese Randbedingungen verdeutlichen, dass der nahe liegende und praktisch weit verbreitete Ansatz, bei dem sich alle Föderationsteilnehmer auf ein gemeinsames Schema einigen, zwar hinreichend, aber nicht zwangsweise notwendig oder optimal ist. Er stellt eine theoretisch elegante Lösung dar, ist jedoch an Auflagen geknüpft, die in der Praxis nicht immer mit angemessenem Aufwand erfüllt werden können. Die hier erarbeitete Lösung geht einen Schritt weiter, da die folgenden Anforderungen an sie gestellt werden:

- Es müssen **beliebig viele Föderationen**, die optional ein gemeinsames Schema definiert haben, unterstützt werden.
- Darüber hinaus muss die Lösung für **bi- und multilaterale Kooperationen** und weitere **Sonderfälle** innerhalb von Föderationen, bei denen sich einzelne Teilnehmer nicht dem gemeinsamen Datenmodell anschließen, verwendet werden können.
- Im Idealfall werden die oben genannten Besonderheiten FIM-basierter Kommunikation berücksichtigt, indem beispielsweise die **Wiederverwendbarkeit definierter Konvertierungsregeln durch andere Föderationsteilnehmer** gefördert wird.

Die vormals sehr strikte organisatorische Anforderung zur föderationsweiten Umsetzung eines gemeinsamen Schemas wird somit durch technische Anforderungen an die Funktionalität des Identitätsdatenkonverters gelockert. Es ist offensichtlich, dass szenarienspezifisch der am besten geeignete **Kompromiss durch die Kombination beider Lösungsansätze** anzustreben ist, um den Gesamtaufwand zu minimieren.

5.2.1.2. Funktionalität auf Datenkonvertierungsebene

Der Identitätsdatenkonverter hat im Hinblick auf seine Integration in die IDP- und SP-seitig ablaufenden Datenflüsse die grundlegende Aufgabe,

- eingehende Anfragen vom entweder föderationsweiten oder providerspezifischen ins lokal verwendete Format umzuwandeln, und
- ausgehende Antworten wiederum vom lokalen ins Format der Gegenseite zu konvertieren.

An einer FIM-Transaktion sind somit genau zwei, im Allgemeinen verschiedene Datenmodelle beteiligt. Asymmetrische Sonderfälle, bei denen die Antwort in ein anderes Format konvertiert wird als das für die Anfrage verwendete, werden hier nicht betrachtet, obwohl die erarbeitete Lösung die Möglichkeit dazu bietet; diese Funktionalität wird z. B. dann benötigt, wenn der Anfragestellende im Namen eines Dritten agiert (vgl. Abschnitt 4.4.1.1).

Auf funktionaler Ebene entspricht die Konvertierung von Anfragen und Antworten einer szenarienspezifisch festzulegenden **Kombination der folgenden Grundoperationen**:

1. **Umbenennen von Attributen**: Datenfelder können bei Absender und Empfänger schlichtweg unterschiedlich benannt sein, beispielsweise `Nachname` vs. `surname`. Die Werte dieser Attribute werden bei der Umbenennung nicht verändert.

2. **Syntaktische Umformungen**: Die Datenfelder sind bei Absender und Empfänger mit unterschiedlicher Syntax definiert worden. Beispiele umfassen die Interpretation einer innerdeutschen Postleitzahl als Zahl bzw. als Zeichenkette und Datumsangaben wie `15.04.2007` bzw. `2007-04-15`. Die Umformung basiert somit primär auf der einfachen Manipulation von Zeichenketten sowie der semantikerhaltenden Umwandlung von Datentypen, z. B. von *integer* in *string*.

3. **Inhaltliche Umformungen**: Eingriffe dieser Art können zur Erhaltung der Semantik im Zielformat notwendig sein und werden auch für die Überbrückung komplexerer Unterschiede in den Datenmodellen benötigt:

   - Ein typisches Beispiel ist die Verwendung unterschiedlicher Sprachen für die Nutzdaten auf Absender- und Empfängerseite, beispielsweise die Benennung eines Studiengangs als *Informatik* bzw. als *computer science*. Die Ableitung des Resultats muss sich im Allgemeinen auf **Abbildungstabellen** stützen, deren Einsatz aufgrund der **meist diskreten Attributswertemengen** durchaus sinnvoll, aber mit dem Aufwand für die kontinuierliche Pflege verbunden ist.
   - Häufig ergibt sich der Wert eines Zielattributs aus den Werten mehrerer Quellattribute. In einfachen Fällen kann beispielsweise der vollständige Name einer Person aus Titel, Vor- und Nachname durch Konkatenation unter Verwendung eines Leerzeichens als Separator gebildet werden. Umgekehrt muss es möglich sein, ein Quellattribut auf mehrere Zielattribute aufzuteilen bzw. einen Eingabewert an mehreren Stellen der Ausgabe verwenden zu können.

Offensichtlich ist die Forderung zur Bereitstellung dieser Grundoperationen nicht FIM-spezifisch. Dennoch ist zu berücksichtigen, dass in vielen Konnektorenframeworks von I&AM-Produkten und den wenigen verfügbaren FIM-Implementierungen bislang nur die als **Attributsmapping** bezeichnete Umbenennung von Attributsnamen ohne Berücksichtigung der Attributsinhalte möglich ist. Die Betonung der dynamischen syntaktischen und inhaltlichen Umformung der Daten unterscheidet sich somit deutlich vom herkömmlichen Vorgehen, bei dem dedizierte Identity Repositories für die Teilnahme an Föderationen eingesetzt werden.

5.2.1.3. Wiederverwendbarkeit von Konvertierungsregeln

Die bislang übliche Vereinbarung eines föderationsweit gemeinsamen Datenmodells zielt darauf ab, den **Aufwand für die Implementierung von Konvertierungsregeln** zu minimieren. Der bei n Föderationsteilnehmern theoretisch im Worst Case notwendige Aufwand zur Spezifikation von $n \cdot (n-1) = O(n^2)$ Konvertierungsregelsätzen spielt aufgrund des bereits erläuterten FIM-Kommunikationsverhaltens in der Praxis keine Rolle: Er würde nur genau dann eintreten, wenn es in einer Föderation außer genau einem IDP nur SPs gäbe, die zudem alle untereinander kommunizieren.

Viel häufiger tritt im FIM-Umfeld jedoch der Fall ein, dass beispielsweise j der k IDPs einer Föderation bereits dasselbe Datenmodell verwenden, dieses jedoch vom föderationsweiten oder SP-spezifischen Datenmodell abweicht. Offensichtlich ist in dieser Konstellation anzustreben, dass die erforderlichen **Konvertierungsregeln nur einmal und nicht mehrfach unabhängig voneinander** implementiert, getestet und gepflegt werden müssen.

Analog dazu kann die Formulierung von Konvertierungsregeln von *einem* lokalen Datenmodell in verschiedene, aber einander ähnliche andere Datenmodelle einen partiell stark repetitiven Charakter annehmen, der u. a. zu unerwünschter Redundanz führt.

An die Einsetzbarkeit und Wiederverwendbarkeit der Konvertierungsregeln werden deshalb die folgenden Anforderungen gestellt:

- Konvertierungsregeln sollten beliebig miteinander kombiniert werden können, um insbesondere ihre **Transitivität** auszunutzen zu können: Eine sequentielle Abarbeitung der Konvertierungen $a \rightarrow b$ und $b \rightarrow c$ entspräche der Konvertierung $a \rightarrow c$, ohne dass diese explizit implementiert werden muss. Gibt es für alle Attribute a_i aus dem Datenmodell A ein $x_i \in X$, so dass $a_i \rightarrow x_i$ und $x_i \rightarrow c_i$ existieren, kann A vollständig in C überführt werden:
  - X ist im einfachsten Fall das föderationsweite Datenmodell.
  - Die Rückrichtung $C \rightarrow A$ kann im Allgemeinen nicht durch inverse Einzeloperationen abgeleitet werden, da jede Umformung mit einem **Informationsverlust** behaftet sein kann. Sowohl $A \rightarrow C$ als auch $C \rightarrow A$ müssen deshalb im Allgemeinen explizit spezifiziert werden.
  - X kann selbst aus der sequentiellen Transformation mehrerer Datenmodelle entstanden sein, d. h. für jede Folge $a_i \rightarrow \ldots \rightarrow z_{j-1} \rightarrow z_j \rightarrow z_{j+1} \rightarrow \ldots \rightarrow c_i$ existiert ein äquivalentes x_i mit $a_i \rightarrow x_i \rightarrow c_i$.
  - Die Anwendbarkeit einer Transformation kann optional auf eine **eingabeseitig diskrete Wertemenge** eingeschränkt werden; Ketten von Konvertierungsregeln sind dann nur für die Schnittmenge der jeweils unterstützten Eingaben anwendbar.
  - Das korrekte Funktionieren kann nur bei Konvertierungsregeln ohne Informationsverlust durch kombinierte Hin- und Rücktransformation überprüft werden; im Allgemeinen müssen deshalb geeignete Testdatensätze definiert und mit dem explizit definierten erwarteten Ergebnis verglichen werden.
- Die Konvertierungsregeln sollen zur Förderung der Wiederverwendbarkeit über ein in den Federation Schema Correlation Service (FSCS) integriertes **organisationsübergreifendes Repository** zur Verfügung gestellt werden können:
  - Im Hinblick auf Datenhoheit und -schutz sollen die eigentlichen **Datenkonvertierungen immer lokal** beim Föderationsteilnehmer durchgeführt werden; lediglich die Konvertierungsregeln können über den FSCS veröffentlicht werden. Diese Möglichkeit zum dezentralisierten Betrieb ist beispielsweise auch eine explizit postulierte Anforderung bei der Integration in die Liberty Alliance Architektur.
  - Der FSCS ist ein TTP-Service, der föderationsweit oder sogar föderationsübergreifend aus logischer Sicht zentral angeboten werden kann. Im Hinblick auf seine Verfügbarkeit und seine Rolle als möglicher Single Point of Failure sind folgende Maßnahmen zu unterstützen:
    * Der Dienst muss redundant auslegbar und von mehreren Organisationen parallel betreibbar sein; der aus logischer Sicht zentrale Dienstbetrieb kann z. B. über die im Architekturkonzept vorgestellten Hochverfügbarkeitsmaßnahmen gewährleistet werden (vgl. Abschnitt 4.3.1.7).

- Der bei einem Föderationsteilnehmer eingesetzte Identitätsdatenkonverter muss mindestens die von ihm benötigten Regeln lokal zwischenspeichern können; hierfür ist ein geeignetes **Cachingverfahren** für die vom FSCS gelieferten Daten zu implementieren.

In den nächsten beiden Abschnitten werden der FSCS und der Identitätsdatenkonverter genauer spezifiziert.

5.2.2. Spezifikation des Federation Schema Korrelation Services

In diesem Abschnitt werden der Aufbau der Konvertierungsregeln, die den Identitätsdatenkonvertern vom FSCS angebotene Funktionalität sowie die Schnittstellen zur Dienstnutzung näher erläutert.

5.2.2.1. Aufbau und Speicherung von Konvertierungsregelsätzen

Dem Identitätsdatenkonverter, der durch den FSCS unterstützt wird, liegt die Idee zugrunde, die Konvertierung auf Basis der standardisierten **Transformationssprache XSLT** [XSLT] zu realisieren. Einerseits erübrigt sich dadurch die Spezifikation einer eigenen Sprache für Konvertierungsregeln, andererseits steht die Möglichkeit zum Einsatz von XSLT bereits bei den I&AM-Konnektorenframeworks einiger Hersteller zur Verfügung, so dass bei der Implementierung auf schon vorhandenes Wissen, Erfahrung und erprobte Entwicklungsumgebungen und Testwerkzeuge zurückgegriffen werden kann.

XSLT unterstützt u. a. die drei benötigten Grundoperationen; nachfolgend werden die Transformation der Nutzdaten in XML, das zur Speicherung der Konvertierungsregeln verwendete Format sowie die benötigten Metadaten diskutiert, die vom FSCS vorgehalten werden müssen.

Format der zu konvertierenden Daten Die grundlegenden Möglichkeiten zur Modellierung von Identitätsdaten wurden bereits in Abschnitt 2.1.2.4 erläutert. Im Folgenden wird von einer *flachen* Modellierung ausgegangen, da diese in der Praxis weiter verbreitet ist. Bei alternativ bereits in XML vorliegenden Daten kann ebenfalls eine Transformation in das hier vorgestellte Format notwendig werden, um beispielsweise die eventuell vorhandenen Angaben nicht benötigter XML-Namespaces zu entfernen; dieser Aspekt wird hier nicht vertieft, da die meisten XML-Beispiele in dieser Arbeit zur Verbesserung der Lesbarkeit auf die Angaben der XML-Namespaces gänzlich verzichten.

Abbildung 5.3 zeigt die Umformung der von einem Identity Repository gelieferten Daten in das für die Konvertierung benötigte XML-Format beim Einsatz eines LDAP-Servers bzw. einer relationalen Datenbank als Identity Repository. Die Umwandlung der LDAP-Attributsnamen bzw. Datenbankspaltennamen ist dabei wie dargestellt trivial und wird hier nicht näher beschrieben; sie muss wie unten erläutert vom Identitätsdatenkonverter durchgeführt werden.

Datenstruktur zur Speicherung von Konvertierungsregeln Wie bereits erläutert wurde, kann es bei n Föderationsteilnehmern ohne Definition eines gemeinsames Datenmodells prinzipiell notwendig werden, separate Konvertierungsregelsätze für bis zu $n - 1$ andere Föderationsteilnehmer zu definieren:

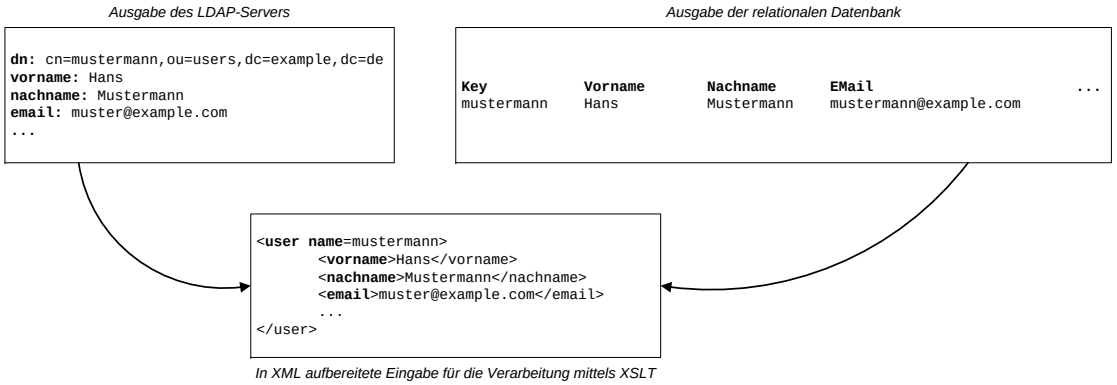


Abbildung 5.3.: Aufbereitung der vom Identity Repository gelieferten Daten in XML

- Dies gilt auch für den Fall, dass ein SP mehr als einen Dienst anbietet, solange er wie im Architekturkonzept vorgesehen genau ein I&AM-System verwendet. Die Anzahl benötigter Konvertierungsregelsätze ist somit an der Anzahl der Föderationsteilnehmer und nicht an der Anzahl der Dienste zu messen.
- Zu den n Datenmodellen können im vorliegenden Fall noch weitere hinzukommen, beispielsweise wenn sich das föderationsweite Datenmodell mit keinem der bereits eingesetzten deckt. Es wird angenommen, dass die Anzahl dieser zusätzlichen Datenmodelle sehr klein gegenüber n ist.

Es ist ferner zu beachten, dass die Konvertierung in **Abhängigkeit von der aktuellen Rolle einer Organisation** unterschiedlich ausfallen kann, dass also für Y als IDP und Z als SP andere Regeln gelten können als für Y als SP und Z als IDP, da unterschiedliche Attributsmengen relevant sein können. Zudem ist zu berücksichtigen, dass für die Konvertierung einer Anfrage im Allgemeinen andere Regeln notwendig sind als für die Umwandlung einer Antwort.

Insgesamt lassen sich somit FSCS-seitig sämtliche **Konvertierungsregelsätze** wie in Abbildung 5.4 dargestellt in einer Matrix speichern, deren Spalten die Empfänger (SPs) bzw. deren Zeilen die Absender (IDPs bzw. AAs) von FIM-Antworten (hier primär allgemeinen Attributsauskünften) repräsentieren:

- Die **Matrix ist sehr häufig nur dünn besetzt**, insbesondere wenn überwiegend ein föderationsweites Datenmodell genutzt wird bzw. wenn an der Föderation viele IDPs und AAs teilnehmen, die untereinander nicht kommunizieren müssen. Zur Speicherung der Matrix könnten entsprechend die für dünn besetzte Matrizen bekannten Techniken eingesetzt werden (vgl. [SPARSE]); um im Umfeld des Identity Managements bereits vorhandene Speichermöglichkeiten nutzen zu können, wird im Folgenden von einer Speicherung der Matrix in einem LDAP-Server ausgegangen:
  - Die Umwandlung der Matrix in den Directory Information Tree (DIT) erfolgt wie in Abbildung 5.5 dargestellt durch eine **zeilenweise Serialisierung**; im DIT stellen

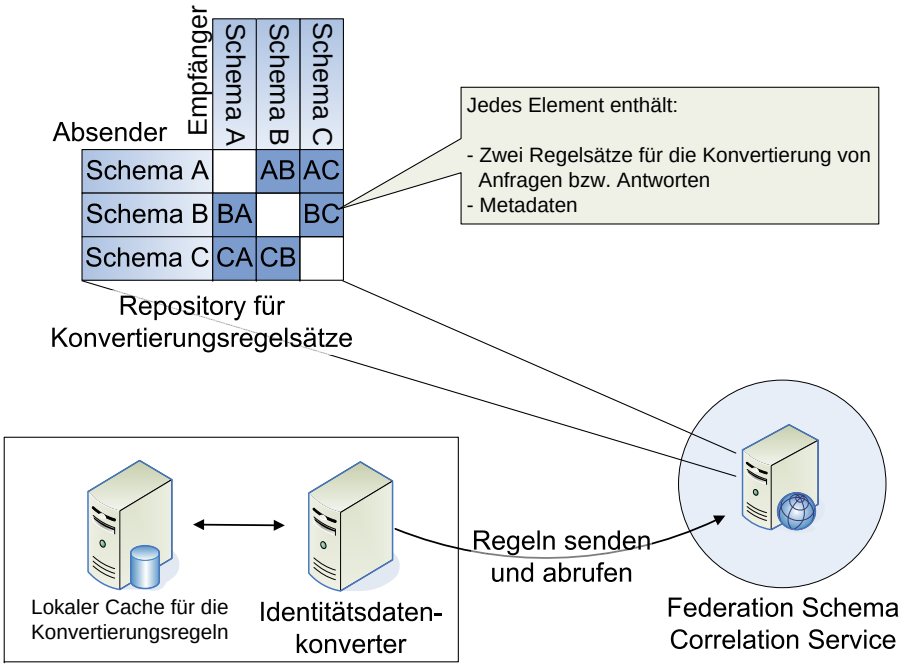


Abbildung 5.4.: Speicherung aller Konvertierungsregelsätze in einer Matrix

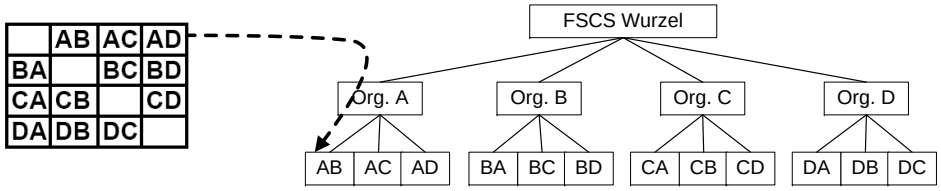


Abbildung 5.5.: Zeilenweise Serialisierung der Matrix zur Speicherung in einem LDAP-Server

also die Absender die Knoten auf der ersten Ebene und die Tupel (Absender, Empfänger) die Blätter dar. Dadurch werden nicht nur die zu einem Absender gehörenden Regelsätze gruppiert, sondern es ist optional durch die Vergabe von LDAP Access Control Lists sehr einfach möglich, beispielsweise jedem Teilnehmer nur Schreibzugriff auf die zu ihm als Absender gehörenden Regeln zu gewähren, indem diese Berechtigung für den entsprechenden gesamten Teilbaum vergeben wird.

– Dieses Verfahren bietet sich auch im Hinblick auf den Speicherplatzverbrauch an, da unbesetzte Matrixelemente nicht explizit gespeichert werden.
– Es kann davon ausgegangen werden, dass die resultierende Performanz für Lese- und Schreibzugriffe bei den aktuellen Föderationsgrößen ($n << 1000$) mehr als ausreichend ist, da heutige LDAP-Server für die Verwaltung mehrerer Millionen Objekte geeignet sind. Gerade mit größer werdendem n ist zudem mit einer im-

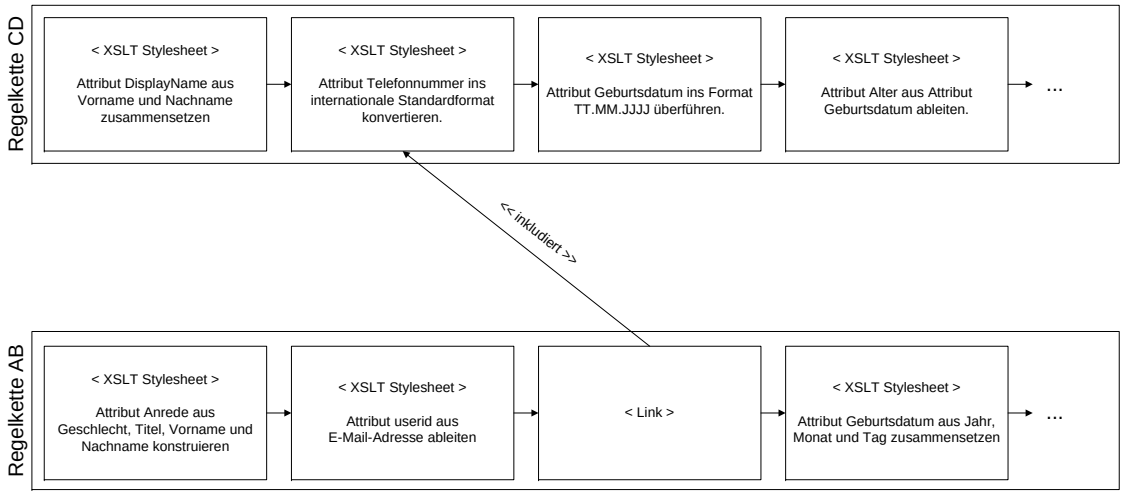


Abbildung 5.6.: Regelketten mit XSLT Stylesheets oder Verweisen als Feldelementen

mer relativ dünner werdenden Besetzung der Matrix zu rechnen; basierend auf der Annahme, dass für jedes neu hinzukommende Föderationsmitglied die Regelsätze für die Konvertierung ins bzw. vom föderationsweiten Schema aufgenommen werden und in manchen Fällen einige bilaterale Konvertierungsregelsätze hinzukommen, kann für die Anzahl zu verwaltender Konvertierungsregelsätze somit ein realer Gesamtspeicheraufwand von $\Theta(n)$ angenommen werden.

- Die Matrixelemente M_{AB} sind Instanzen komplexer Datentypen, die folgende Angaben enthalten:
  - Die anzuwendenden Datenkonvertierungsregeln werden in Feldern (Arrays) gespeichert, die als **Konvertierungsregelketten** bezeichnet werden: Jedes als **Konvertierungsregel** bezeichnete Feldelement kann wie in Abbildung 5.6 dargestellt entweder ein **XSLT-Stylesheet** und damit die konkrete Kodierung einer Konvertierungsregel oder einen **Verweis (Link) auf eine Konvertierungsregel** eines beliebigen anderen Konvertierungsregelsatzes enthalten. Hierfür bietet sich in Analogie zu den Föderationsmetadaten ein URI-basierter Adressnamensraum der Form `https://fscs1/idp1/sp1/response/arrayindex` an.

    Hierdurch wird gewährleistet, dass mehrere Konvertierungsregeln sequentiell abgearbeitet werden können, wodurch der Grundstein für **modulare Konvertierungsregelsätze** gelegt wird. Durch die Möglichkeit zum Verweis auf an anderer Stelle gespeicherte Konvertierungsregeln wird deren redundanzfreie Wiederverwendbarkeit ermöglicht; wie unten erläutert wird, ist es dabei sogar denkbar, dass Konvertierungsregeln im Rahmen von Third Party Services implementiert und mit minimalem Aufwand genutzt werden können.
  - Für die Konvertierung von Anfragen und Antworten werden wie in Abbildung 5.7 verdeutlicht zwei getrennte Regelketten verwendet, da beide Operationen wie oben erläutert im Allgemeinen nicht invers zueinander sind.
  - Zusätzlich werden die unten erläuterten Metadaten festgehalten.

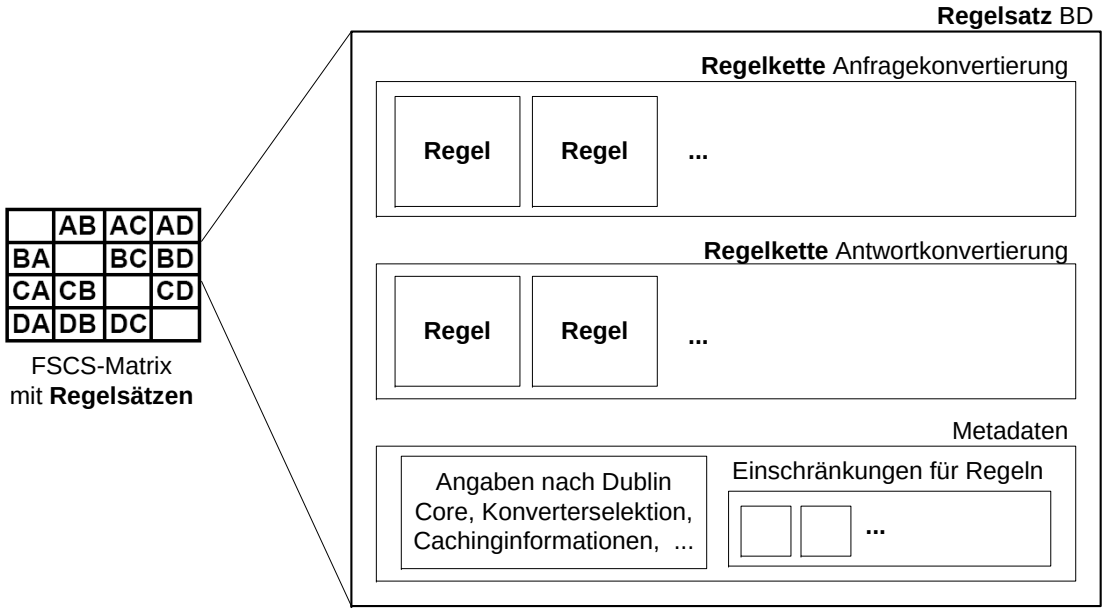


Abbildung 5.7.: Speicherstruktur zur Differenzierung der Begriffe Regelsatz, Regelkette und Regel

Dabei ist zu berücksichtigen, dass A bzw. B nicht nur andere Föderationsteilnehmer, sondern auch z. B. das föderationsweite Datenschema identifizieren können.

In Abschnitt 5.2.4 werden konkrete Beispiele für den Einsatz von XSLT-Stylesheets zur Datentransformation gegeben; auf die sich durch XSLT ergebenden weiteren Möglichkeiten wird an dieser Stelle nicht näher eingegangen, da zu dieser Thematik umfassende Literatur existiert – beachtenswert ist jedoch die von vielen XSLT-Prozessoren gebotene Möglichkeit, eigenen (Java-) Code einbinden zu können, wodurch manche Transformationen einfacher und effizienter implementiert werden können.

Diese Matrix kann funktional mit der Attribute Correspondence Matrix bei der Schemakoordination in föderierten Datenbankmanagementsystemen verglichen werden (siehe Abschnitt 3.8.4); durch die Unterstützung weiterer Grundoperationen neben der Umbenennung von Attributen (bzw. Spalten in Datenbanktabellen), die Verwendung von Regelketten statt einzelner Regeln und die Integration der für den Betrieb notwendigen Metadaten geht die hier vorgestellte Methode jedoch deutlich über diesen ursprünglichen Ansatz hinaus.

Es sollte bedacht werden, dass die Ausschöpfung der ermöglichten Flexibilität eine **potentielle Fehlerquelle** darstellt; beispielsweise können fremde Konvertierungsregeln, auf die im Rahmen einer Regelkette verwiesen wird, ohne eigenes Zutun gelöscht oder modifiziert werden, so dass die Konvertierung zukünftig fehlschlagen würde. Im Rahmen einer Implementierung sollten deshalb geeignete Einschränkungen und Hilfsmittel realisiert werden, die einen Kompromiss aus redundanzfreier Regelspeicherung und zuverlässigem Betrieb ermöglichen. Einen wesentlichen Beitrag hierzu leisten auch die nachfolgend beschriebenen Metadaten.

Relevante Metadaten In jedem Matrixelement werden wie oben beschrieben Metadaten zusätzlich zu den eigentlichen Konvertierungsregelketten vorgehalten. Dabei handelt es sich im Einzelnen um

- grundlegende Informationen, beispielsweise die Angabe des Autors des Regelsatzes sowie ggf. der Quelle, aus der ein Regelsatz abgeleitet wurde. Alle diesbezüglich möglichen Metadatenelemente sind im so genannten Dublin Core Metadata Standard[2] spezifiziert und werden hier nicht näher betrachtet.

- die Angabe, ob die Konvertierung vom IDP/AA oder SP durchzuführen ist. Aus offensichtlichen Gründen muss sichergestellt werden, dass dieselben Datenkonvertierungsregeln nur einmal und nicht doppelt angewendet werden; entsprechend ist es prinzipiell auch ausreichend, wenn nur eine der beiden an der FIM-Transaktion beteiligten Organisationen den Identitätsdatenkonverter zur Verfügung hat, wodurch die Einführung dieser Komponente in existierende Föderationen erleichtert wird.

- Informationen, die das Caching seitens der involvierten Identitätsdatenkonverter unterstützen. Hierzu gehören eine Versionsnummer, die sich bei jeder Änderung erhöhen muss, samt Zeitstempel der letzten Änderung sowie die Angabe des voraussichtlichen Gültigkeitszeitraums:

  - Wenn der Beginn des Gültigkeitszeitraums in der Zukunft liegt und eine ältere Version des Regelsatzes bereits vorhanden war, so stellt der FSCS die neue Version erst ab dem angegebenen Zeitpunkt zur Verfügung (vgl. Abschnitt 4.8.3 bzgl. synchronem Wirksamwerden von Änderungen beim organisationsübergreifenden Change Management).
  - Das Ende des Gültigkeitszeitraums wird analog zum Protokoll DNS nicht als absoluter, sondern als relativer Zeitpunkt angegeben. Der Identitätsdatenkonverter, der einen Regelsatz im Cache vorhält, kann somit gezwungen werden, die anhaltende Gültigkeit z. B. jeweils nach spätestens 7 Tagen zu prüfen. Bei der Suche nach Änderungen wird er zudem wie in Abschnitt 5.2.2.2 beschrieben vom FSCS unterstützt.

- Einschränkungen bezüglich der erlaubten Eingabewertemenge pro Konvertierungsregel (d. h. pro XSLT-Stylesheet); sofern eine Regel nicht für alle möglichen Eingabewerte geeignet ist, sind die mit Einschränkungen verbundenen Attribute und deren zulässige diskrete Eingabewerte aufzuzählen.

  Die daraus für die ganze Regelkette resultierenden Einschränkungen ergeben sich aus der Vereinigungsmenge der Einschränkungen der einzelnen Regeln, wobei hinsichtlich der erlaubten Eingabewerte pro Attribut die Schnittmenge zu bilden ist. Die explizite Speicherung der Einschränkungen in der Granularität einzelner Regeln ist erforderlich, da diese im Rahmen von Verweisen auf einzelne Konvertierungsregeln anderer Regelketten berücksichtigt werden müssen.

Der Zugriff auf die beim FSCS gespeicherten Daten wird im nächsten Abschnitt beschrieben.

[2] `http://dublincore.org/`

5.2.2.2. Vom FSCS angebotene Funktionalität

Der FSCS fungiert als Server und nimmt Anfragen von den Identitätsdatenkonvertern entgegen; diesen wird die folgende Grundfunktionalität angeboten:

- **Management der eigenen Konvertierungsregelsätze**:
  - Im einfachsten Fall umfasst dies das Anlegen, Modifizieren und Löschen der zur jeweiligen Organisation gehörenden Zeile der oben erläuterten Matrix.
  - Sofern eine direkte Pflege der eigenen Konvertierungsregelsätze durch Dritte ermöglicht werden soll, muss eine Möglichkeit zur Definition von Access Control Lists vorhanden sein; die dritte Partei kann die betroffenen Matrixzellen nach entsprechender Freischaltung ebenfalls modifizieren.
- **Auslesen von Konvertierungsregelsätzen**; hierfür existieren Selektionskriterien verschiedener Granularität:
  - Auflisten der den FSCS nutzenden Organisationen; diese Angabe wird benötigt, um einzelne Matrixelemente dem oben angegebenen Namensschema gemäß gezielt ansprechen zu können.
  - Auslesen eines einzelnen Matrixelements bzw. Regelsatzes; dies ist die grundlegendste Zugriffsart.
  - Auslesen der kompletten Matrix: Hierdurch wird primär der initiale Aufbau eines Caches durch einen Identitätsdatenkonverter unterstützt. Es ist zu beachten, dass möglicherweise ACLs verwendet werden, die auch Leseoperationen nur ausgewählten Teilnehmern erlauben.
  - Auslesen einer Liste von Matrixelementen, die sich seit einem frei wählbaren Zeitpunkt geändert haben; die Identitätsdatenkonverter können ihre Caches auf Basis dieser Information gezielt aktualisieren, ohne die Matrix vollständig neu abrufen zu müssen.

Die erläuterte Funktionalität ist für den Betrieb der Identitätsdatenkonverter ausreichend, wenn durch manuelle Überprüfung sichergestellt wird, dass alle benötigten Regelsätze vorhanden sind. Darüber hinaus können Zusatzfunktionen angeboten werden, durch die das Erstellen der erforderlichen Konvertierungsregelsätze erleichtert wird:

- Sofern für die FIM-basierte Kommunikation zwischen den Organisationen A und C noch keine Konvertierungsregelketten definiert wurden und auch beispielsweise kein föderationsweites Schema genutzt werden kann, kann der FSCS unter der Ausnutzung der Transitivität der Konvertierungsregelsätze eine Liste von B_i zurückliefern, für die $A \rightarrow B_i \rightarrow C$ möglich wäre.

  Hierzu ist prinzipiell ein Graph zu konstruieren, dessen Knoten die beteiligten Organisationen sind, von denen jedes Paar (X, Y) genau dann über eine ungewichtete Kante verbunden wird, wenn bereits ein entsprechender Konvertierungsregelsatz $X \rightarrow Y$ definiert worden ist. Anschließend kann beispielsweise auf Basis eines Algorithmus zur Bestimmung der kürzesten Pfade zwischen A und C eine Liste potentieller Kombinationen

von Konvertierungsregelsätzen erstellt werden, die manuell eingehender zu untersuchen sind.

Diesbezüglich ist zu beachten, dass die vollständige, d. h. alle Attribute abdeckende Lösung im Allgemeinen nicht vollständig automatisiert gefunden werden kann, da die oben erläuterten Metadaten keine Auskunft darüber geben, zu welchem Grad an Vollständigkeit eine Regelkette zwei Datenmodelle ineinander überführt: Es kann Attribute a_j und c_j geben, deren Konvertierung von $a_i \rightarrow b_i \rightarrow c_i$ nicht abgedeckt wird, so dass $a_j \rightarrow c_j$ nachträglich ergänzt werden muss. Eine Automatisierung der Entscheidung über die Vollständigkeit der ermittelten Abbildungen würde umfangreiche zusätzliche Metadaten erforderlich machen, die präzise spezifizieren, aus welchen Attributen das Schema A besteht und welche Attribute a_i in welche b_i von Schema B überführt werden; der derzeit damit verbundene manuelle Annotationsaufwand würde den Nutzen jedoch deutlich übersteigen. Für Weiterentwicklungen wäre denkbar, die hierfür benötigten Metadaten automatisiert aus den Konvertierungsregelsätzen abzuleiten; aufgrund der möglichen Komplexität von XSLT-Stylesheets[3] erscheint dies jedoch nur für einfachere Konvertierungsregelsprachen mit angemessenem Aufwand realisierbar.

- Für neue Teilnehmer verbleibt der Initialaufwand zur Definition mindestens eines Konvertierungsregelsatzes, beispielsweise in ein föderationsweites Schema oder in das Schema einer anderen Organisation, für die bereits relevante weitere Regelsätze definiert wurden.

  Der FSCS kann diesen Schritt unterstützen, indem er bekannte Werkzeuge zur Schemakoordination zentral anbietet:

  - Einfache Ansätze umfassen die Synonymsuche auf Basis der Attributsnamen; z. B. sind die Attribute `lastname`, `surname` und `familyname` in der Regel äquivalent.
  - Fortgeschrittene Ansätze analysieren zusätzlich zur Schemaspezifikation Beispieldatensätze und vergleichen sie mit bekannten Mustern (vgl. [ELBA07]).
  - Zukünftig könnten insbesondere auch ontologiebasierte Verfahren zum Einsatz kommen, sofern die anfragende Organisation ihr lokales Datenmodell in geeigneter Form dokumentiert hat.

  Vom FSCS können folglich initiale Zuordnungen und Abbildungsregeln vorgeschlagen werden, die jedoch manuell geprüft und ggf. korrigiert und erweitert werden müssen.

Für den FSCS sind weitere Einsatzmöglichkeiten denkbar, z. B. die Aufbereitung des gesamten Regeldatenbestandes in Form einer gut lesbaren Dokumentation, auf die hier jedoch nicht weiter eingegangen wird, da sie die Kernfunktionalität nicht FIM-spezifisch erweitern würden.

5.2.2.3. Kommunikationsschnittstelle und organisatorische Aspekte

Wie bereits im Architekturkonzept erläutert wurde, werden die oben genannten Funktionen über eine Web Services Schnittstelle bereitgestellt; hierdurch wird auch die Möglichkeit zur starken Authentifizierung der jeweiligen Gegenstelle impliziert.

[3] Die Turing-Vollständigkeit von XSLT wurde 2004 von Kepser bewiesen.

Aufgrund der folgenden organisatorischen Aspekte sind ggf. noch weitere Kommunikationspartner des FSCS zu berücksichtigen:

- Im einfachsten Fall erfolgt die **Autorisierung zur Nutzung** des FSCS durch die Sicherstellung der Föderationszugehörigkeit, die durch eine Auswertung der Metadaten einer oder mehrerer Föderationen erreicht werden kann. Somit muss der FSCS mit den entsprechenden Föderationsverwaltungen kommunizieren können und kann hierfür beispielsweise die im Architekturkonzept beschriebene Schnittstellenkomponente einsetzen (siehe Abschnitt 4.4.11).

  Sofern der FSCS jedoch auch von Organisationen genutzt werden können soll, die an keiner der dem FSCS bekannten Föderationen teilnehmen, oder falls Einschränkungen bezüglich des Teilnehmerkreises realisiert werden sollen, muss eine geeignete FSCS-lokale Benutzerverwaltung eingesetzt werden, die wie die Rechteverwaltung mit dem zur Speicherung der Regelsätze verwendeten LDAP-Server kombiniert werden kann.

- Um zu vermeiden, dass der FSCS zu einem Single Point of Failure wird, kann der Dienst **repliziert und mehrfach parallel** betrieben werden. Durch den Einsatz von LDAP-Servern als Datenspeicher können deren Datenbestände wie in Abschnitt 4.3.1.7 beschrieben repliziert werden, wobei hinsichtlich Schreibzugriffen wiederum die Master-Fähigkeit der Replikate berücksichtigt werden muss.

Die technische Funktionalität zur Pflege von Regelsätzen durch Dritte ermöglicht beispielsweise die Einrichtung föderationsweiter Kompetenzzentren, die neuen Föderationsteilnehmern Hilfestellung leistet; im kommerziellen Umfeld können dadurch auch kostenpflichtige Dienste integriert werden, die eine Alternative zum Aufbau lokalen Fachwissens zur Nutzung dieser FIM-Komponente darstellen.

5.2.3. Spezifikation des Identitätsdatenkonverters

Die Funktionsweise des Identitätsdatenkonverters wird nachfolgend anhand der Verarbeitungsschritte beim Eingang einer Anfrage erläutert:

1. Der Anfrage an den Identitätsdatenkonverter wird neben den betroffenen Attributen und ggf. deren Werten auch die Information übergeben, ob es sich um eine FIM-Anfrage bzw. -Antwort handelt und welcher Kommunikationspartner beteiligt ist, so dass daraus der benötigte Konvertierungsregelsatz und die richtige der beiden darin enthaltenen Regelketten bestimmt werden können.

2. Die übergebenen Nutzdaten, die in Form von Attributnamen und -werten vorliegen, müssen wie in Abschnitt 5.2.2.1 demonstriert ins XML-Format überführt werden.

3. Es muss überprüft werden, ob für die Anfrage geeignete Konvertierungsregelketten vorhanden sind. Dabei sind die folgenden Fälle zu unterscheiden:

   - Wenn der Identitätsdatenkonverter noch keinen lokalen Datenbestand hat, so wird zuerst die gesamte Matrix vom FSCS abgerufen und in einem Cache vorgehalten.

- Wenn für die beiden involvierten Kommunikationspartner (IDP/AA bzw. SP) und die Kommunikationsrichtung (Aufruf des Konverters für eingehende bzw. ausgehende Daten) eine Regelkette vorhanden ist, so werden zuerst die Metadaten des Regelsatzes überprüft: Sollte seine Gültigkeitsdauer überschritten worden sein, wird er in der aktuellen Version vom FSCS anfordert.

  Dieser Vorgang ist auch für alle Regelsätze zu wiederholen, deren Regeln im Rahmen der ermittelten Regelkette über Verweise inkludiert werden.
- Sofern keine Regelkette explizit definiert wurde, wird auf die Konvertierung von einem bzw. in ein vorab ausgewähltes föderationsweites Schema ausgewichen.

  Wenn hiervon abweichend Daten nicht konvertiert, sondern unverändert durchgeschleust werden sollen, ist zu beachten, dass eine entsprechende „leere“ Regelkette explizit angelegt werden muss, um die beiden Varianten „Verwenden eines gemeinsamen Schemas“ und „unverändertes Durchschleusen“ voneinander unterscheiden zu können. Eine Konvertierungsregel zum nur seltener benötigten Durchschleusen entspricht einem trivialen XSLT-Stylesheet, das die gesamte Eingabe unverändert in die Ausgabe übernimmt.

  Sofern auch kein zu verwendender Standardregelsatz definiert wurde, liegt eine Fehlersituation vor, die zum Abbruch führt.

4. Die gefundene Regelkette wird anhand der Metadaten auf Eignung für die konkret vorliegenden Eingabewerte überprüft; für den Fall, dass mindestens ein Eingabewert aufgrund der definierten Einschränkungen nicht mit den verfügbaren Konvertierungsregeln konvertiert werden kann, muss vorab festgelegt worden sein, ob der Konvertierungsprozess abgebrochen werden soll oder ein unvollständiges Ergebnis in Kauf genommen wird.
5. Die einzelnen XSLT-Stylesheets der ermittelten Regelkette werden sequentiell auf die in XML vorliegenden Eingabedaten angewandt; wie in Kapitel 6 beschrieben wird, kommt hierzu ein standardkompatibler XSLT-Prozessor wie Xalan [XALAN] zum Einsatz.
6. Das Ergebnis der Transformationen liegt ebenfalls in XML vor und muss wieder in das von den anderen lokalen Komponenten verwendete Format, z. B. die LDAP-typischen Attributsnamen und -wertepaare konvertiert werden.

Bei der Implementierung und beim Einsatz des Identitätsdatenkonverters ist zwangsweise zu berücksichtigen, dass seine **Performanz ein kritischer Erfolgsfaktor** für die Abwicklung eines Großteils der FIM-Transaktionen ist. Die Verwendung von XML und XSLT entspricht somit dem aktuellen Stand der Technik, ist im Hinblick auf den Datendurchsatz jedoch erfahrungsgemäß nur suboptimal. Bei der Realisierung sind entsprechend die folgenden Optimierungsansätze in Erwägung zu ziehen:

- Der Cache für die Konvertierungsregelsätze sollte lokal auf der Maschine des Identitätsdatenkonverters vorgehalten und nicht z. B. in eine externe Datenbasis ausgelagert werden.
- Ein asynchron zu Anfragen an den Identitätsdatenkonverter laufender Prozess sollte eine kontinuierliche Aktualisierung des Caches vornehmen, so dass der Fall, dass dieser während der Bearbeitung einer Anfrage veraltete Regelsätze enthält, möglichst selten eintritt.

- Es sollte ein XSLT-Prozessor eingesetzt werden, der mit präkompilierten XSLT-Stylesheets arbeiten kann; analog zur Übersetzung von Java-Quelltext zu Java-Bytecode werden die XSLT-Anweisungen dabei in ein Binärformat übersetzt, in dem sie effizienter abgearbeitet werden können.

Da in die Abarbeitung von XSLT-Stylesheets prinzipiell auch externe Daten wie das aktuelle Datum mit einfließen können, ist ein darüber hinausgehendes Cachen der ermittelten Antworten im Allgemeinen nicht möglich und sollte nur verwendet werden, wenn sichergestellt ist, dass lediglich eine Teilmenge der XSLT-Funktionalität genutzt wird, so dass die Konvertierungsregeln für dieselbe Eingabe immer dieselbe Ausgabe liefern. Für die hier typischerweise vorliegenden Daten wird diese Anforderung jedoch meist erfüllt.

5.2.4. Anwendungsbeispiele

In Anlehnung an die Publikation [HoRe05a], in der die Motivation für den Identitätsdatenkonverter dargestellt wurde, werden nachfolgend zwei einfache Beispiele für die Verwendung von XSLT-Stylesheets zur Datentransformation gezeigt. Das erste Beispiel demonstriert dabei die Problematik unterschiedlicher Namensgebungen für Attribute und die Notwendigkeit syntaktischer Umformungen; das zweite Beispiel zeigt die Modifikation des Inhalts auf Basis in XSLT realisierter Abbildungstabellen für diskrete Attributswerte.

5.2.4.1. Beispiel 1: Differierende Attributsnamen und -syntax

Ein Service Provider (SP) möchte durch eine Anfrage beim Identity Provider (IDP) das Geburtsdatum des Benutzers in Erfahrung bringen, um diesem personalisierte Dienste anzubieten; es wird im Folgenden davon ausgegangen, dass die Attribute Release Policies diese Anfrage zulassen.

Bezüglich der IDP- und SP-seitig eingesetzten Datenmodelle treten dabei die folgenden Unterschiede auf:

- Der SP verwendet zur Speicherung des Geburtsdatums das Attribut `DOB` (engl. Akronym für *date of birth*) und erwartet das im englischsprachigen Raum weit verbreitete Datumsformat `YYYY-MM-DD`, d. h. Jahr, Monat und Tag mit jeweils vier bzw. zwei Stellen mittels eines Minuszeichens separiert.
- Der IDP verwendet hingegen drei getrennte Attribute `birth_day`, `birth_month` und `birth_year` für denselben Zweck.

Eine Anfrage nach dem Attribut `DOB` würde ohne den Einsatz des Identitätsdatenkonverters also bereits daran scheitern, dass dieses Attribut IDP-seitig unbekannt ist; im Identitätsdatenkonverter wird die Anfrage nach diesem Attribut wie folgt in XML dargestellt:

```
1 <remoterequest user="mustermann" sp="sp.example.com">
2     <attribute>DOB</attribute>
3 </remoterequest>
```

Die Anwendung des folgenden XSLT-Stylesheets führt zur Zerlegung des einen angefragten in die drei lokal betroffenen Attribute:

```
<xsl:template match="/">
    <localrequest>
        <xsl:apply-templates select="remoterequest/attribute"/>
    </localrequest>
</xsl:template>

<xsl:template match="request/attribute">
    <xsl:if test=". = 'DOB'">
        <attribute>birth_day</attribute>
        <attribute>birth_month</attribute>
        <attribute>birth_year</attribute>
    </xsl:if>
</xsl:template>
```

Sie führt somit zu dieser Ausgabe, die im Rahmen des lokalen Auslesens der benötigten Benutzerattribute eingesetzt wird:

```
<localrequest>
    <attribute>bd_day</attribute>
    <attribute>bd_month</attribute>
    <attribute>bd_year</attribute>
</localrequest>
```

Vor der Rückgabe der ermittelten Antwort an den SP wird wiederum der Identitätsdatenkonverter durchlaufen. Die Eingabe enthält in diesem Fall die lokal verwendeten Attribute und ihre Werte:

```
<user name="mustermann">
    <birth_year>1967</birth_year>
    <birth_month>03</birth_month>
    <birth_day>25</birth_day>
</user>
```

Durch das folgende XSLT-Stylesheet werden die drei einzelnen Attribute zum vom SP benötigten Attribut `DOB` kombiniert:

```
<xsl:template match="/">
    <localresponse>
        <xsl:attribute name='user'>
            <xsl:value-of select="user/@name"/>
        </xsl:attribute>
        <xsl:apply-templates select="user/birth_year"/>
    </localresponse>
</xsl:template>

<xsl:template match="user/birth_year">
    <DOB>
        <xsl:value-of select="concat(
            normalize-space(.), '-',
            normalize-space(../birth_month), '-',
            normalize-space(../birth_day))"/>
    </DOB>
</xsl:template>
```

Die Ausgabe enthält entsprechend lediglich die folgenden Daten:

```
<localresponse user="mustermann">
    <DOB>1967-03-25</DOB>
</localresponse>
```

Die Anfrage kann somit im gewünschten Format korrekt beantwortet werden.

5.2.4.2. Beispiel 2: Inhaltliche Modifikation von Attributswerten

In diesem Beispiel wird die bereits demonstrierte Umbenennung von Attributen mit der Modifikation der Attributswerte verknüpft:

- Der IDP speichert die Nationalität eines Benutzers im Attribut `nationality` und verwendet als diskrete Wertemenge den entsprechenden ISO-Standard, also beispielsweise *DE* für Deutschland.[4]
- Der SP verwendet hingegen das Attribut `citizenship` und in diesem Fall den Wert `German`.

Die Transformation der eingehenden Anfrage erfolgt dabei wie im ersten Beispiel; die Eingabe für die Konvertierung der Antwort enthält analog dazu die folgenden Angaben:

```
<user name="mustermann">
    <nationality>DE</nationality>
</user>
```

Das folgende XSLT-Stylesheet zeigt die Verwendung einer fest in die XSLT-Anweisungen einkodierten Abbildungstabelle:

```
<xsl:template match="/">
    <localresponse>
        <xsl:attribute name='user'>
            <xsl:value-of select="user/@name"/>
        </xsl:attribute>
        <xsl:apply-templates select="user"/>
    </localresponse>
</xsl:template>

<xsl:template match="user">
    <citizenship>
        <xsl:choose>
            <xsl:when test="nationality = 'DE'">German</xsl:when>
            <xsl:when test="nationality = 'FR'">French</xsl:when>
            <!-- ... weitere Tabelleneintraege ... -->
            <xsl:otherwise>unknown</xsl:otherwise>
        </xsl:choose>
    </citizenship>
</xsl:template>
```

Je nach eingesetztem XSLT-Prozessor kann die Tabelle dabei auch in eine externe Datei ausgelagert werden bzw. es kann z. B. eigener Java-Code eingebunden werden, wodurch eine elegantere und wartungsfreundlichere Programmierung ermöglicht wird. Die Ausgabe ist davon unabhängig wie folgt aufgebaut:

```
<localresponse user="mustermann">
    <citizenship>German</citizenship>
</localresponse>
```

Für reale Szenarien eingesetzte XSLT-Stylesheets werden üblicherweise dadurch komplexer, aber auch effizienter, dass sie nicht nur einzelne Attribute, sondern Mengen logisch zusammengehörender Attribute bearbeiten; damit mehrere XSLT-Stylesheets sinnvoll hintereinander ausgeführt werden können, ist jedes davon so zu gestalten, dass die jeweils irrelevanten Attribute unmodifiziert durchgeschleust werden.

[4] Siehe ISO-3361-1, Kodierliste ALPHA-2

5.3. FIM Privacy Management System auf Basis von XACML-Policies

Kein anderer Aspekt des Identity Managements wird so häufig und kontrovers diskutiert wie der **Datenschutz**. Bei der Akquisition und Verarbeitung personenbezogener Daten entstehen potentiell **Interessenskonflikte** zwischen Dienstanbietern und Nutzern: Erstere können detaillierte Kundenprofile beispielsweise für ein möglichst attraktives, personalisiertes Dienstangebot ausnutzen, wohingegen letztere einen Missbrauch ihrer Daten, beispielsweise durch unerwünschte Weitergabe an Dritte, befürchten. Die Datenschutzgesetze und andere juristische Auflagen werden oft einerseits als zu restriktiv, andererseits als veraltet und den Anforderungen der modernen Informationsgesellschaft nicht mehr gewachsen bezeichnet; auch darf der Schutz der Daten von für die Thematik nicht sensibilisierten Personen nicht vergessen werden.

Aus offensichtlichen Gründen ist die Kontrolle über die eigenen Personendaten ausschlaggebend für die Benutzerakzeptanz von FIM. Bereits die Einführung zentraler Identity Repositories in I&AM-Systemen, in denen Personendaten aus mehr als einer Datenquelle aggregiert und korreliert werden, führt häufig zu massiven Datenschutz- und Sicherheitsbedenken: Die Kombination vormals getrennter Datenbestände ermöglicht nicht nur eventuell **neue Auswertungsverfahren**, sondern stellt auch ein besonders lukratives **Ziel für Ausspähungsangriffe** dar. Zusammen mit FIM entstehen deshalb neue Befürchtungen über die unkontrollierte, organisationsübergreifende Weitergabe dieser Daten.

Im Hinblick auf den Datenschutz und die damit verbundene Benutzerakzeptanz muss den frühen FIM-Ansätzen aus heutiger Sicht das Defizit attestiert werden, diese Thematik zu lange ignoriert zu haben. So hat einerseits die ausschließlich zentrale Speicherung der Personendaten zum Scheitern von Microsoft Passport beigetragen (vgl. [PIMWAY, Koch02]), andererseits sind in der SAML-Architektur keine Möglichkeiten zur Einschränkung der Datenübermittlung vorgesehen. Wie bereits in Kapitel 3 erläutert wurde, hat auch der erste Ansatz der Liberty Alliance, Benutzer interaktiv explizit jeder einzelnen Datenübertragung zustimmen zu lassen, die wohlgemeinte Intention verfehlt und stattdessen eher zur Verärgerung der Anwender beigetragen.

In Anbetracht der inzwischen engen Zusammenarbeit zwischen den Shibboleth-Entwicklern und der Liberty Alliance stellt die von Shibboleth ermöglichte Kontrolle über den Fluss einzelner Attribute den De-facto-Standard dar: Über Attribute Release Policies (ARPs), die in einer so genannten **Privacy Preferences Expression Language** (PPEL) formuliert werden, haben Benutzer direkten Einfluss darauf, welche Daten von ihrem Identity Provider an einen Service Provider übermittelt werden dürfen.

Shibboleth ARPs ermöglichen dabei die Steuerung der Datenflüsse in der Granularität einzelner Benutzerattribute und SPs. Formalrechtlich betrachtet stellen sie deshalb eine hinreichende Lösung für die FIM-Datenschutzproblematik dar. In der Praxis mangelt es den Shibboleth ARPs wie unten erläutert jedoch an Funktionalität, so dass sich der Umgang mit ihnen in komplexeren Szenarien als äußerst mühsam erweist. Dieses Defizit ist den Entwicklern von Shibboleth durchaus bewusst; da die Implementierung einer umfassenderen ARP-Sprache aufgrund des damit verbundenen Aufwands nicht priorisiert werden konnte, wurde stattdessen eine Schnittstelle geschaffen, über die eigene ARP-Implementierungen relativ einfach integriert werden können.

In Abschnitt 5.3.1 wird die Wahl von XACML als Policysprache für ARPs im Rahmen dieses Konzepts begründet. Hierzu werden zuerst die relevanten ARP-spezifischen Anforderungen erläutert; im Anschluss wird das Ergebnis einer Bewertung in Frage kommender existierender Policysprachen vorgestellt, das im Rahmen der Arbeit an eigenen Publikationen und einer vom Autor betreuten Diplomarbeit ermittelt und verfeinert wurde.

Da XACML eine sehr umfangreiche und flexible Policysprache ist, muss sie durch einen als Tailoring bezeichneten Prozess an die Verwendung für ARPs angepasst werden; ein wesentlicher Vorteil von XACML ist dabei, dass die Standardkonformität nicht verloren geht, wodurch beliebige XACML Policy Decision Points (PDPs) für die Auswertung von XACML-ARPs eingesetzt werden können, ohne modifiziert werden zu müssen. In Abschnitt 5.3.2 wird entsprechend nach einer knappen Übersicht über die relevanten XACML-Policysprachelemente auf deren genaue Syntax und Semantik für ARPs eingegangen.

Die Ermittlung der für eine Anfrage an das FIM Privacy Management System relevanten ARPs, ihr Kombinations- und Auswertungsprozess sowie die Interpretation des vom PDP ermittelten Ergebnisses durch den XACML Policy Enforcement Point (PEP) werden in Abschnitt 5.3.3 beschrieben. Der PEP bildet dabei auch die im Architekturkonzept beschriebene Schnittstelle zu den anderen FIM-Komponenten.

Abschließend werden in Abschnitt 5.3.4 einige einfache Anwendungsbeispiele vorgestellt und die für eine Migration benötigte automatisierte Konvertierung von Shibboleth ARPs in XACML demonstriert.

Abbildung 5.8 zeigt eine Zusammenfassung der Struktur dieses Abschnitts.

5.3.1. Selektion der verwendeten Policysprache

Wie im Architekturkonzept bereits verankert wurde, wird im Rahmen dieser Arbeit eine adäquate Kombination aus Benutzerinteraktion und Policyauswertung zur Kontrolle der Datenflüsse angestrebt; dies deckt sich mit der sich abzeichnenden Entwicklung der Liberty Alliance und dem Funktionsumfang aktueller UCIM-Implementierungen, wohingegen frühere Ansätze rein auf Interaktion (Liberty Phase One bzw. BBAE, vgl. Kapitel 3) *oder* auf Policies (Shibboleth) aufbauten. Da auf die nähere Untersuchung von Benutzeroberflächen in dieser Arbeit bewusst verzichtet wird, stellt die Wahl der für die Formulierung von Attribute Release Policies verwendeten Policysprache die nächste grundlegende Entscheidung dar.

Die grundlegenden **ARP-spezifischen Kriterien für die Bewertung von Policysprachen** wurden in einer früheren eigenen Veröffentlichung vorgestellt und im Rahmen einer Diplomarbeit anhand von einfachen Beispielszenarien verfeinert [Hom05a, Eber06]. Nach einem Überblick über relevante andere Arbeiten im nachfolgenden Abschnitt werden in den Abschnitten 5.3.1.2 und 5.3.1.3 deshalb lediglich die Anforderungen selbst, getrennt in die Betrachtung der Ausdrucksfähigkeit der Policysprache und übrige Kriterien, zusammenfassend vorgestellt. Details zu ihrer Herleitung können den beiden genannten Arbeiten entnommen werden, in denen diverse in Frage kommenden Policysprache auch bereits bewertet wurden; das Ergebnis und somit die Entscheidung für die Verwendung von XACML werden in Abschnitt 5.3.1.4 zusammengefasst.

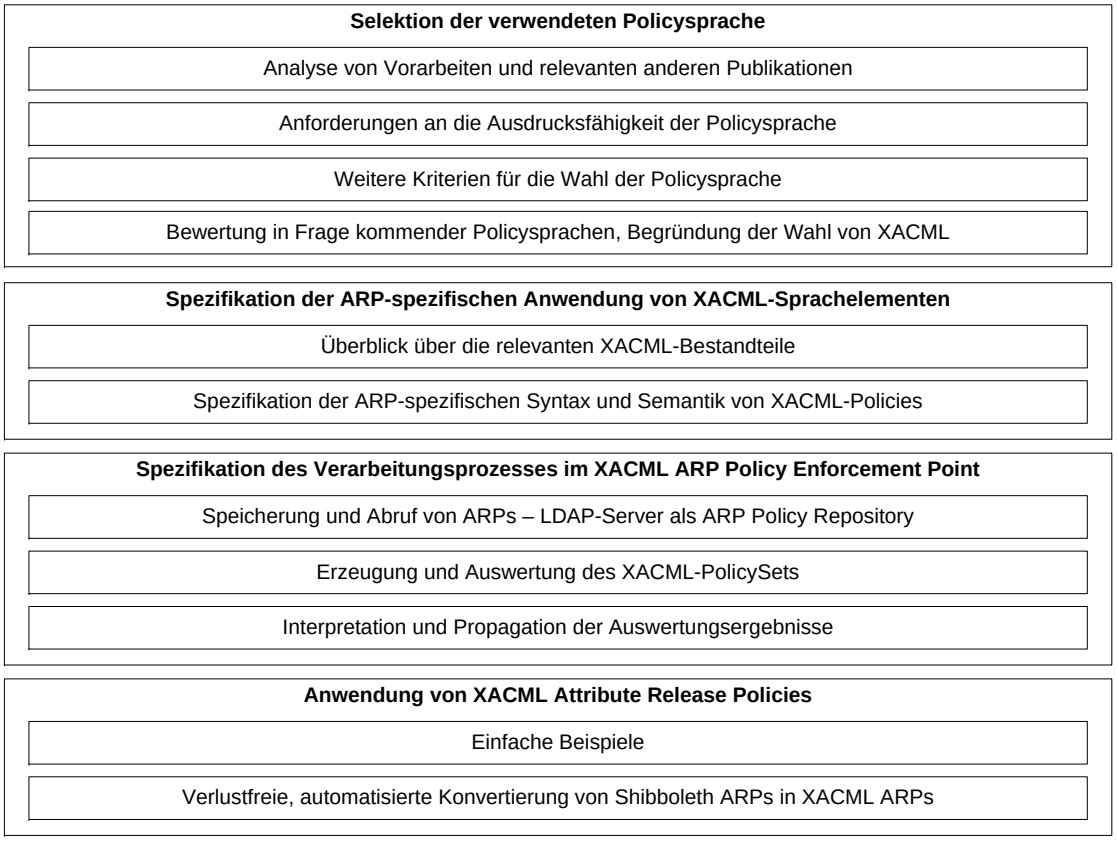


Abbildung 5.8.: Struktur der Beschreibung der XACML-basierten FIM Privacy Management Komponente

5.3.1.1. Relevante andere Arbeiten

Bei der Auswahl der Policysprache, der Gestaltung des Funktionsumfangs der XACML ARPs und den sukzessiven Verfeinerungen des hier vorgestellten Konzepts wurde eine Reihe anderer Publikationen berücksichtigt, die nachfolgend sehr knapp skizziert werden:

- Arbeiten im Umfeld des Privacy Managements:
  - [PRISER] stellt die Grundkomponenten einer organisationsinternen Privacy Architektur vor und kategorisiert die einzelnen Aufgaben im Umfeld des Privacy Managements.
  - [BPS03] definiert einen Privacy Policy Lebenszyklus und betont analog zu [BBKS04] die Notwendigkeit zur effizienten Auswertung mehrerer zusammenhängender Policies; Aspekte wie die Schnittmengenbildung von Privacy Policies werden in [BDS04] diskutiert.
  - [WBS+05] geht auf föderierte Umgebungen ein, zielt jedoch auf eine vollständig pseudonymisierte Dienstnutzung zum Schutz personenbezogener Daten ab. Im

Gegensatz dazu betrachtet [PIMWAY] die Datenschutzproblematik in föderierten Umgebungen aus der Perspektive des E-Governments.

- [PRIMET] versucht, „Privacy-Metriken“ zu definieren; die Ergebnisse zeigen jedoch, dass es derzeit noch kaum möglich ist, die Effektivität des Datenschutzes objektiv zu quantifizieren.
- [DN03] stellt eine Heuristik vor, die Aufschluss über den Grad der eigenen Anonymität in Abhängigkeit von den an verschiedene Service Provider bereits übermittelten Benutzerattributen geben soll.

- Arbeiten mit konkretem Bezug zu Policysprachen:
  - [BM05] demonstriert Defizite von APPEL und betont die Komplexität der Aufgabe, die korrekte technische Umsetzung in Prosa formulierter Datenschutzerklärungen zu erzwingen.
  - In [BMR04] werden analoge Probleme von EPAL Policies erläutert und Anforderungen zur Sicherstellung der Konsistenz von Policies hergeleitet.
  - [TK06] stellt eine Kategorisierung von Policysprachen vor und weist mehreren Policysprachen unklare Semantik nach, so dass entsprechend konstruierte Policies je nach Interpretationsart zu einem anderen Ergebnis führen. Ebenso werden typische Fallstricke demonstriert, die beim Design einer neuen Policysprache berücksichtigt werden müssen.

- Arbeiten, die eigene ARP-Sprachen definieren:
  - [PRIPOL] schlägt als grundlegende Bestandteile von Privacy Policies *Benutzer*, *Daten* und *Verwendungszwecke* vor und erläutert die Notwendigkeit von Bedingungen und Obligationen; es werden exemplarische Policies in der Logiksprache ASL vorgestellt.
  - [CYS+05] orientiert sich an organisationsinternen Identity Management Systemen und definiert eine einfache XML-basierte Sprache, die für ARPs mit Basisfunktionalität eingesetzt werden könnte.
  - [SSB05] untersucht Cachingverfahren für Authentifizierungs- und Autorisierungsdaten zur Effektivierung FIM-basierter Dienstnutzung; in diesem Kontext wird eine minimalistische, XML-basierte Sprache für die Spezifikation von Privacy Preferences vorgestellt.
  - [ADdVS05] erläutert die Schwierigkeiten bei der Definition von Namensräumen zur Adressierung von Entitäten und Ressourcen und stellt eine einfache, XML-basierte Policysprache vor, die Ontologien für die Subjekte, Aktionen und Objekte der Policies verwendet.
  - [PREP] geht konkret auf die Notwendigkeit von ARPs im FIM-Umfeld ein; die vorgeschlagene Policysprache PREP ist stark auf die Interaktion mit den Benutzern ausgelegt.

Es ist ferner zu beachten, dass im Rahmen der XACML-Spezifikation inzwischen ein als „Privacy Policy Profile“ bezeichnetes ergänzendes Dokument herausgegeben wurde (siehe [X2PRIV]); anders als der Name vermuten lässt, wird in dem netto weniger als 50 Zeilen

umfassenden Dokument jedoch lediglich ein neues XACML-Element namens `purpose` eingeführt, mit dem Verwendungszwecke in XACML-Policies angegeben werden können. Das in Abschnitt 5.3.2 vorgestellte Konzept geht darüber weit hinaus.

5.3.1.2. Anforderungen an die Ausdrucksfähigkeit der Policysprache

In Abschnitt 2.1.2.6 wurden die elementaren Aufgaben von ARPs bereits beschrieben. Sie lassen sich wie folgt zu Anforderungen an den Sprachumfang der verwendeten Policysprache konkretisieren:

1. Es müssen *Namensräume* unterstützt werden, die eine präzise Spezifikation von

   - Service Providern *mit verschiedenen Diensten*
   - *Benutzern mit mehreren Identitäten und mehreren Rollen* sowie hierzu gehörenden *Attributen*

   in einem *globalen, föderationsübergreifenden Kontext* unterstützen. Aus den bereits eingehend diskutierten Gründen muss die Policysprache dabei prinzipiell vom lokal oder föderationsweit gewählten *Datenmodell für Benutzerattribute unabhängig* sein.

2. Die Herausgabe von Attributen muss *zweckgebunden* erfolgen können; für Verwendungszwecke wie „Marketing“ und „Bestellungsabwicklung“ muss ebenfalls ein geeigneter Namensraum vorhanden sind.

   Hiervon klar zu unterscheiden ist die ebenfalls zu unterstützende *Differenzierung von Zugriffsarten*: Für das vorliegende Konzept muss mindestens zwischen einmalig lesendem, abonnierendem und schreibendem Zugriff unterschieden werden können. Da Verfeinerungen wie die Untergliederung schreibenden Zugriffs in das Neuanlegen, Modifizieren bzw. Löschen von Attributen denkbar sind, muss auch hier Erweiterbarkeit gefordert werden.

3. Die Entscheidung muss an möglichst flexibel formulierbare *Bedingungen* knüpfbar sein. Hierzu gehört beispielsweise, dass ein Attribut nur dann freigegeben werden soll, wenn die Herausgabe bestimmter anderer Attribute ebenfalls bereits genehmigt wurde (*Abhängigkeitsrelation*). Ferner sollen *Kontext- und Umgebungsinformationen* wie z. B. die aktuelle Uhrzeit mit einbezogen werden können.

4. Neben *Bedingungen* müssen auch *Obligationen* unterstützt werden. Dabei handelt es sich um Aktionen, die unmittelbar nach der Auswertung einer Policy angestoßen werden sollen. Ein typisches Beispiel ist die Benachrichtigung des Benutzers mittels E-Mail, wenn ein Service Provider bestimmte Attribute abgerufen hat; Obligationen in ARPs sind dabei unabhängig davon zur Verfügung zu stellen, ob die Herausgabe eines Attributs genehmigt oder verwehrt wurde.

   Obligationen können entweder für den lokalen IDP (bzw. AA) oder für den SP gelten. Als *Langzeit-Obligationen* werden Aktionen bezeichnet, die zwar unmittelbar angestoßen, aber erst deutlich später abgeschlossen werden, z. B. die SP-seitige Löschung aller personenbezogenen Daten 90 Tage nach der letzten Dienstnutzung.

5. Es muss möglich sein, die Policies *dezentral zu administrieren* und im Kontext einer Anfrage eine *Kombination mehrerer Policies* auszuwerten. Dieser Anforderung liegt die angestrebte Aufteilung in föderationsweite, IDP-spezifische sowie von den Benutzern selbst konfigurierte Policies zugrunde; insbesondere soll eine beliebige *hierarchische Anordnung von Policies* möglich sein:

   - Es ist szenarienspezifisch zu entscheiden, in welcher *Vorrangbeziehung* z. B. föderationsweite und benutzerspezifische Policies zueinander stehen.
   - Die Möglichkeit zur Pflege mehrerer Policies unterschiedlicher *Priorität* kann die Spezifikation komplexer Regelwerke vereinfachen; beispielsweise kann die Formulierung einer Ausnahme durch eine zusätzliche, höher priorisierte Policy leichter nachvollziehbar sein als die Hinzunahme weiterer Bedingungen in eine bereits bestehende Policy.

6. Die *Integrität der Policies* muss z. B. durch die Verwendung einer PKI und entsprechender kryptographischer Signaturen gewährleistet werden können; dies ist im Datenmodell der Policies oder in der Spezifikation des Policy Repository geeignet zu berücksichtigen.

7. Die gewählte Policysprache muss effizient für ARPs zu verwenden sein; auf Basis der in Kapitel 3 genannten Nachteile von Shibboleth-ARPs bedeutet dies insbesondere, dass *Benutzerattribute und Service Provider gruppiert* werden können sollen, so dass für m Attribute und n SPs nicht $m \cdot n$ einzelne Regeln spezifiziert und gepflegt werden müssen.

   Zu diesem Kriterium zählt jedoch auch der Anspruch, die gewählte Policysprache nicht zweckzuentfremden; insbesondere sollen Sprachelemente nicht entgegen ihrer ursprünglich definierten Semantik eingesetzt werden. Sofern Modifikationen der Sprache notwendig werden, ist auf vorgesehene Erweiterungsmechanismen zurückzugreifen.

Eine gesamtheitliche Betrachtung dieser Anforderungen zeigt dabei bereits starke Parallelen zwischen Attribute Release Policies und herkömmlichen Access Control Policies; diese Kategorie ist deshalb neben anderen Privacy Management Policysprachen in die Kandidatenmenge aufzunehmen.

5.3.1.3. Weitere Kriterien für die Wahl der Policysprache

Neben den oben genannten Anforderungen an den Sprachumfang der Policysprache werden im Hinblick auf eine praktische Realisierbarkeit auch die folgenden Aspekte berücksichtigt:

- Die gewählte Policysprache sollte bereits einen nennenswerten *Verbreitungsgrad* gefunden haben; hierdurch wird weitgehend gewährleistet, dass
  - die nicht selten beim Design einer neuen Policysprache auftretenden grundlegenden Fehler bereits bekannt und behoben worden sind. Insbesondere sollte nur dann eine neue ARP-Sprache geschaffen werden, wenn auf Basis der genannten Anforderungen keine geeignete Ausgangsbasis gefunden werden kann.
  - bereits vorhandene Werkzeuge wie graphische Policyeditoren sowie Wissen zur Anwendung der Policysprache genutzt werden können.

- Die *Kompatibilität* mit bisherigen Ansätzen ist anzustreben; beispielsweise müssen die schon weit verbreiteten Shibboleth-ARPs automatisch und verlustfrei übernommen bzw. konvertiert werden können.
- Im Hinblick auf eine Implementierung ist es von großem Vorteil, wenn für die Policysprache bereits ein *Policy Decision Point* vorhanden ist, der einfach in eigene Programme integriert werden kann, um den Aufwand für die Bereitstellung des Policyparsers und -interpreters zu minimieren.

Im Unterschied zu den Anforderungen an den Sprachumfang sind diese Kriterien für das Konzept jedoch nicht essentiell.

5.3.1.4. Bewertung in Frage kommender Policysprachen

Aufgrund der benötigten Sprachelemente wurden neben den in Kapitel 3 bereits vorgestellten Privacy Management Ansätzen auch Access Control Policysprachen untersucht. In der bereits erwähnten Diplomarbeit von Matthias Ebert wurde auch anhand von konkreten Beispielen analysiert, wie gut sich die einzelnen Ansätze für die Formulierung und Auswertung von ARPs eigenen; die folgende Übersicht fasst die Bewertung für die nicht ausreichend geeigneten Ansätze zusammen:

- Die Sprache EPAL geht wie in Abschnitt 3.5.2 beschrieben nicht auf die kombinierte Auswertung mehrerer Policies ein; zudem ist trotz ihrer konzeptionellen Reife noch keine frei zugängliche Implementierung verfügbar, die bei eigenen Entwicklungen genutzt werden könnte. Aufgrund der Ausrichtung auf organisationsinternen Einsatz müssten zudem mehrere FIM-spezifische Sprachanpassungen vorgenommen werden.
- E-P3P unterstützt im Gegensatz zu EPAL die Kombination mehrerer Policies; wie in Abschnitt 3.5.2 erläutert wurde, bestehen dabei jedoch noch Defizite hinsichtlich der Konflikterkennung und -lösung. Die beiden anderen bei EPAL genannten ARP-spezifischen Probleme treffen auch auf E-P3P zu.
- P3P und APPEL (vgl. Abschnitt 3.5.1) bieten nur sehr einfache Bedingungen und keine Obligationen; zudem werden durch P3P bereits ein e-commerce-spezifisches Datenmodell und ein zu stark limitiertes Namensraumkonzept vorgegeben.
- Ponder [PONDER] ist eine im akademischen Umfeld weit verbreitete Policysprache, die für Securitypolicies im Umfeld des Netz- und Systemmanagements konzipiert wurde. Sie unterstützt jedoch keine Differenzierung zwischen Zugriffsart und Zweckangabe; der vorgeschlagene Namensraum müsste um die Unterstützung von Identitäten und Rollen in globaler Ausprägung erweitert werden. Die vormals verfügbare Open Source Referenzimplementierung wird nicht mehr zum Download angeboten, da kein Support mehr geleistet werden kann. Im Hinblick auf die XSLT-basierte Konvertierung von Shibboleth-ARPs kommt erschwerend hinzu, dass Ponder als einzige der hier betrachteten eine nicht auf XML basierende Policysprache ist.
- Shibboleth-ARPs haben die bereits erwähnten Nachteile, weder zwischen Verwendungszwecken noch zwischen Zugriffsarten zu differenzieren, unterstützen keine Obligationen,

keine Gruppierungen und eine nur sehr eingeschränkte Bedingungssprache. Zudem werden nur zwei fest vorgegebene Policies pro Anfrage (Site ARP bzw. User ARP) unterstützt; die Sicherstellung der Policyintegrität durch elektronische Signaturen ist nicht möglich.

- Die im SPADE-Projekt implementierte Alternative zu Shibboleth-ARPs weist die bereits in Abschnitt 3.5.3 diskutierten Defizite auf; neben der Unterscheidung von Verwendungszwecken und Zugriffsarten fehlt die Unterstützung für dynamische Bedingungen und Obligationen, so dass der Sprachumgang nicht ausreicht.

Demgegenüber unterstützt die eXtensible Access Control Markup Language (XACML 2.0, [XACML]) alle benötigten Sprachelemente mit folgenden Randbedingungen:

- Für die Angabe des Verwendungszwecks existiert im Standardsprachumfang kein dediziertes Sprachelement; vielmehr muss eine in diesem Fall dreistufige Verfeinerung „Service Provider → Service → Zweck“ der Angabe des Datenabrufenden angewendet werden; alternativ kann ein XACML-PDP eingesetzt werden, der das oben erwähnte XACML Privacy Policy Profile unterstützt.
- XACML unterstützt im Standardumfang lediglich einige ausgewählte Policykombinationsalgorithmen wie *deny-overrides* und *first-applicable* (siehe auch Abschnitt 5.3.2). Ein prioritätsgesteuerter Auswertungsalgorithmus muss somit selbst implementiert werden; XACML bietet eine hierfür dedizierte Erweiterungsschnittstelle.
- Die Verwendung elektronischer Signaturen zur Integritätsgewährleistung wird in einem den Standard ergänzenden Dokument beschrieben [And04a].

XACML wird darüber hinaus bereits in mehreren anderen Projekten mit Bezug zum Identity Management bzw. den erläuterten hier relevanten Aspekten erfolgreich eingesetzt:

- Die Integration von XACML-Policies in SAML wird in [AL04] beschrieben und in [WP05] allgemein sowie in [GRIDSA, WALDEN] für das Grid-Umfeld demonstriert.
- Die Kombination der Authentifizierung auf Basis von Identity Management und der Autorisierung mittels XACML wird am Beispiel der WLAN-Nutzung in [LGMC05] erörtert.
- In [SRS+05] wird eine Variante der dezentralen, delegierten Administration von XACML-Policies erläutert.
- Der Einsatz von XACML zur dezentralen Autorisierung im Föderationskontext ist Gegenstand von [WEK05]; dabei spielt insbesondere die Umsetzung von Role-Based Access Control (RBAC) eine zentrale Rolle. Eine weitere Variante zur XACML-basierten Autorisierung beim Einsatz einer Trusted Third Party wird in [MCCP06] diskutiert.

Eine gute Übersicht über weitere XACML-Projekte wird in [XACMLD] gegeben; die Integration in den Web Services WS-* Protokollstack wird in [WSPL] erläutert. Das mögliche

Zusammenspiel mit P3P und die konzeptionellen Unterschiede zu EPAL werden in [And04d] und [And04b, And05] beschrieben.

Zudem ist eine Open Source Referenzimplementierung verfügbar, die nahtlos in eigene Programme integriert werden kann [SUNXAC]; die Konvertierung von Shibboleth-ARPs wird in Abschnitt 5.3.4.2 beschrieben.

5.3.2. Spezifikation der ARP-spezifischen Anwendung von XACML-Sprachelementen

Die Version 2.0 des Standards XACML wurde im Februar 2005 verabschiedet; seit Ende 2006 wird an ersten Entwürfen von XACML 3.0 gearbeitet, die hier noch nicht berücksichtigt werden, da keine unmittelbar relevanten Neuerungen zu erwarten sind.

Bereits XACML 2.0 bietet über 50 Sprachelemente, die eine sehr flexible Unterstützung verschiedenster Anwendungsszenarien ermöglichen sollen. Als Konsequenz ist nicht sofort im Detail offensichtlich, wie XACML zur Modellierung von Attribute Release Policies eingesetzt werden kann. Vielmehr ist eine Selektion der benötigten Sprachelemente vorzunehmen und deren semantische Bedeutung präzise zu verfeinern; dieser Vorgang wird als Tailoring bezeichnet.

Im folgenden Abschnitt 5.3.2.1 wird ein sehr knapper Überblick über die grundlegenden Bestandteile von XACML gegeben, der sich bereits auf die für ARPs relevanten Aspekte beschränkt; er ermöglicht ein Verständnis der in Abschnitt 5.3.2.2 erläuterten ARP-Spezifika, die im Rahmen dieses Konzepts erarbeitet wurden, ohne eine vorherige intensive Auseinandersetzung mit der XACML-Standardspezifikation notwendig zu machen.

5.3.2.1. Überblick über die relevanten XACML-Bestandteile

XACML ist, wie der Name bereits vermuten lässt, eine XML-basierte Sprache, deren Elemente auf Basis der nachfolgend angegebenen Regeln ineinander verschachtelt werden können:

- Jede XACML-`Policy` besteht aus mindestens einer `Rule`.
- Jede `Rule` hat einen `effect`, z. B. *permit* oder *deny*, und wird durch eine eindeutige `id` identifiziert.

  In jeder `Rule` kann ein `Target` angegeben werden, auf das sich die Regel bezieht. Ein `Target` besteht aus einem Tripel (`Subject`, `Action`, `Resource`), durch das spezifiziert wird, welche Operationen (Action) welcher Entitäten (Subject) auf welchen Objekten (Resource) durch die Regel überwacht werden. Wenn kein explizites `Target` angegeben wird, gilt die Regel für alle Anfragen.

  Optional kann eine `Rule` darüber hinaus eine `Condition` enthalten; zur Formulierung komplexer Bedingungen stehen boolesche Operatoren und eine Vielzahl von Funktionen bereit, mit denen beispielsweise die aktuelle Uhrzeit mit einem vorgegebenen Zeitintervall verglichen werden kann.

  Ebenfalls optional können pro Regel `Obligations` spezifiziert werden; das Ausführen jeder `Obligation` kann an den resultierenden `effect` der Regel gebunden werden, so dass

beispielsweise zwei unterschiedliche Obligationen angestoßen werden, wenn als Ergebnis *permit* bzw. *deny* geliefert wird.

- Für jede `Policy` muss ein `RuleCombiningAlgorithm` spezifiziert werden, der bestimmt, welchen `effect` die Policyauswertung liefert, falls mehr als eine `Rule` zur Anfrage passt. XACML gibt bereits einige dieser Algorithmen vor: Beispielsweise führt *deny-overrides* dazu, dass eine Policy, bei der mindestens eine zutreffende `Rule` als `effect` den Wert *deny* hat, als Gesamtresultat ebenfalls *deny* liefert; beim Algorithmus *first-applicable* wird die Auswertung der Policy nach der ersten passenden `Rule` beendet und deren `effect` als Ergebnis der Policy zurückgegeben.
- Die Vereinigungsmenge der Targets der Rules kann optional als `Target` der `Policy` angegeben werden; hierdurch kann effizienter entschieden werden, ob eine Policy überhaupt für eine Anfrage relevant ist.
- Mehrere `Policy`-Elemente können zu einem `PolicySet` zusammengefasst werden. Für die Steuerung der Auswertung der in einem `PolicySet` enthaltenen Policies muss analog zum `RuleCombiningAlgorithm` ein `PolicyCombiningAlgorithm` angegeben werden; hierfür stehen ebenfalls einige vorgefertigte Algorithmen zur Auswahl.

Diese Zusammenhänge werden als UML-Klassendiagramm in der Abbildung 5.9 visualisiert, die der Standardspezifikation [XACML] entnommen wurde.

Das folgende Beispiel skizziert eine einfache XACML-Policy:[5]

```
1  <Policy id="Beispiel1" RuleCombiningAlgorithm="first-applicable">
2    <Description> Einfaches Beispiel einer XACML-Policy </Description>
3    <Target />
4    <Rule id="BeispielRegel1" effect="permit">
5      <Description> Einfaches Beispiel einer XACML-Rule </Description>
6      <Target>
7        <Resource>
8          Auto
9        </Resource>
10       <Subject>
11         Anton
12       </Subject>
13       <Action>
14         benutzen
15       </Action>
16     </Target>
17     <Condition Function="time-in-range">
18       <Apply EnvironmentAttribute="current-time">
19       <value> 14:00:00 </value>
20       <value> 18:00:00 </value>
21     </Condition>
22   </Rule>
23   <Rule id="CatchAllFinalRule" effect="deny"/>
24 </Policy>
```

Die erste `Rule` gibt an, dass *Anton* das *Auto benutzen* darf (`effect` *permit*), sofern die aktuelle Uhrzeit im Intervall zwischen 14:00 und 18:00 Uhr liegt. In der zweiten `Rule` wurde kein `Target` angegeben; sie gilt somit für alle Anfragen und wird, da sie auch keine `Condition` enthält, als so genannte *catch-all* Regel bezeichnet. In Kombination mit dem `RuleCombiningAlgorithm` *first-applicable* ergibt sich daraus, dass alle nicht zur ersten Regel passenden Anfragen als Ergebnis *deny* liefern; für in sich geschlossene Policies wird diese

[5] Wie bei den anderen XML-Beispielen wird zur Verbesserung der Übersichtlichkeit auf den Abdruck der XML-Namespaces verzichtet; einige formal notwendige XACML-Elemente und -Attribute, die jedoch nicht zur Veranschaulichung beitragen, wurden in diesem einführenden Abschnitt ebenfalls weggelassen.

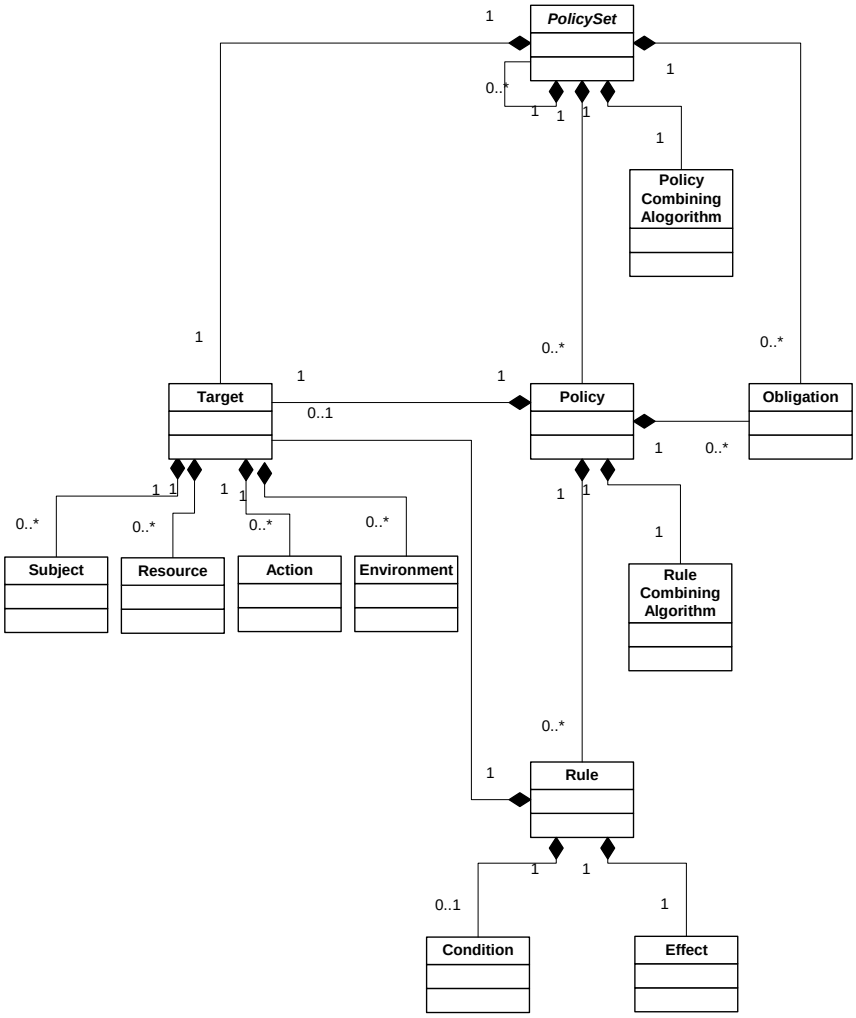


Abbildung 5.9.: UML-Klassendiagramm der XACML-Policystruktur (Bildquelle: [XACML])

zweite Regel benötigt, da der XACML Policy Decision Point (PDP) andernfalls das Ergebnis *not applicable* liefern würde, wenn keine passende `Policy` bzw. `Rule` gefunden wurde.

Anfragen an den XACML-PDP werden vom Policy Enforcement Point (PEP) gestellt; sie enthalten insbesondere das Tripel (`Subject`, `Action`, `Resource`) und können optional weitere Daten enthalten, die als *Resource Content* bzw. *Environment Context* bezeichnet werden; auf diese Weise können beispielsweise wie im nächsten Abschnitt erläutert die aktuellen Werte der Attribute der Benutzeridentitäten übergeben werden.

Das folgende Beispiel zeigt einen einfachen XACML-`Request`:

```
<Request>
  <Subject>
    Anton
  </Subject>
  <Resource>
    Auto
  </Resource>
```

```
8     <Action>
9       benutzen
10    </Action>
11  </Request>
```

Als Ergebnis wird vom XACML-PDP die folgende `Response` geliefert:

```
1  <Response>
2    <Result>
3      <Decision> Permit </Decision>
4      <Status> OK </Status>
5    </Result>
6  </Response>
```

Diese Antwort muss vom XACML-PEP geeignet interpretiert werden; insbesondere ist der PEP für die Ausführung der optional in der Antwort enthaltenen `Obligations` zuständig.

Die von XACML vorgegebenen Regel- und Policykombinationsalgorithmen sowie die möglichen Obligationen können mit minimalem Aufwand um eigene Varianten erweitert werden, da lediglich die Wertemengen der XML-Attribute wie `RuleCombiningAlgorithm` erweitert werden müssen.

5.3.2.2. ARP-spezifische Syntax und Semantik

Nachfolgend wird die exakte Verwendung der XACML-Sprachelemente bei der Verwendung für Attribute Release Policies spezifiziert; dies betrifft insbesondere die Semantik der Wertemengen von XML-Elementen, z. B. die Angabe von `Subject` und `Resource`. Das hier vorgestellte Konzept stellt eine Weiterentwicklung der beiden eigenen Publikationen [Hom05a] und [Hom05b] dar; in der bereits genannten Diplomarbeit [Eber06] wurde zur Begrenzung der Komplexität nur eine Teilmenge davon berücksichtigt.

Es sind die folgenden grundlegenden Aspekte zu berücksichtigen:

- Für eine Anfrage kann mehr als eine Policy relevant sein, beispielsweise wenn jeweils beliebig viele föderationsweite, IDP- sowie benutzerspezifische ARPs berücksichtigt werden sollen. Aus diesem Grund sind die oben erläuterten *catch-all* Regeln in einzelnen Policies zu vermeiden; vielmehr wird wie unten erläutert das Ergebnis *not applicable* vom XACML-PEP geeignet ausgewertet.

- Die verschiedenen Arten von ARPs sollen in eine beliebige zueinander hierarchische Relation gebracht werden können; dabei ist szenarienspezifisch zu entscheiden, ob beispielsweise Benutzer-ARPs Vorrang vor föderationsweiten ARPs haben sollen oder nicht. Aus diesem Grund wird jeder Policy eine Priorität zugeordnet; treffen auf eine Anfrage mehrere Policies zu, wird das Ergebnis der Auswertung der Policy mit der höchsten Priorität zurückgeliefert.

- Das Architekturkonzept sieht vor, dass neben *permit* und *deny* ein dritter Ergebnistyp zurückgeliefert wird, wenn der Benutzer interaktiv um seine Zustimmung gefragt werden soll; der hierfür neu eingeführte Wert für den `effect` ist *ask*.

Die einzelnen Sprachelemente von XACML sind wie folgt anzuwenden und werden im untenstehenden Beispiel gezeigt:

- Üblicherweise ist der `RuleCombiningAlgorithm` *first-applicable* zu wählen (siehe Zeile 1); wie in Abschnitt 5.3.3 beschrieben wird, kann dadurch die Auswertung der Policy mit der höchsten Priorität gewährleistet werden. Eine Ausnahme bilden von Shibboleth übernommene ARPs, für die *deny-overrides* zu wählen ist (vgl. Abschnitt 5.3.4.2).

- Die Priorität einer Policy wird als XACML-`CombinerParameter` mit dem Namen *ARPpriority* angegeben (siehe Zeilen 2–6)). Zur Vereinfachung des Policymanagements ist die Wertemenge auf alle positiven ganzen Zahlen beschränkt. Die zum Bearbeiten der ARPs eingesetzten Werkzeuge müssen sicherstellen, dass die Priorität in einem geeigneten Intervall liegt, d. h. dass Benutzer beispielsweise keine Prioritäten außerhalb von [50; 100] vergeben dürfen.

- Policies und Regeln können und sollen `Description`-Elemente enthalten, die z. B. den jeweiligen Zweck in Prosa beschreiben (siehe Zeilen 7 und 9).

- Die als `effect` von `Rule` zulässigen Werte sind wie oben beschrieben *permit*, *ask* und *deny* (siehe Zeile 8). Da bei Anfragen, auf die keine ARP zutrifft, implizit *ask* zurückzuliefern ist, was wiederum als *deny* interpretiert wird, falls der Benutzer keine Interaktionsmöglichkeit hat, reicht es prinzipiell aus, ARPs mit dem `effect` *permit* zu erstellen; die beiden anderen Varianten können für die Formulierung von Ausnahmefällen verwendet werden.

- Die einzelnen Bestandteile des `Target`-Elements werden wie folgt spezifiziert (vgl. Zeilen 10–41):

  - Die durch die ARP geschützten `Resources` sind die Benutzerattribute. Für sie wird ein URL-basierter Namensraum verwendet, dessen Segmente den zuständigen IDP, die digitale Identität und Rolle des Benutzers sowie den lokalen Attributsnamen widerspiegeln (siehe Zeile 15). Für IDPs, die nur eine Rolle pro Benutzer unterstützen, wird die Konstante `defaultrole` gewählt. Die Verwendung des XACML-Elements `ResourceMatch` dient der Unterstützung der unten erläuterten Gruppierung von Attributen (siehe Zeilen 13–18).
  - Als `Subject` wird das Tripel (Service Provider, Dienst, Verwendungszweck) angegeben; XACML bietet hierzu die sequentielle Verwendung dreier `SubjectMatch`-Elemente an (siehe Zeilen 21–33). Analog zur Verwendung von `ResourceMatch` werden Gruppierungen unterstützt; durch den Einsatz von regulären Ausdrücken bzw. Wildcards können Regeln definiert werden, die z. B. für alle Verwendungszwecke oder alle Dienste eines Service Providers gelten.

    Die Namensgebung der Service Provider und Dienste muss analog zu den Föderationsmetadaten erfolgen, da sie von der IDP-Software in dieser Form an das FIM Privacy Management System geliefert werden. Für die möglichen Verwendungszwecke muss – wie in Abschnitt 4.4.4 diskutiert – eine gemeinsame diskrete Wertemenge festgelegt werden, die szenarienspezifisch ist; als Ausgangsbasis können z. B. die von P3P standardisierten Werte verwendet werden.

– Die `Action` kann den im Architekturkonzept vorgesehenen Möglichkeiten folgend die Werte *read*, *subscribe* und *write* bzw. analog zu Attributsgruppierungen eine Kombination davon annehmen (siehe Zeilen 34–40).

Mehrere anzugebende Werte wie z. B. Namen von Attributen können über eine XACML-`VariableDefinition` gruppiert werden, indem sie als regulärer Ausdruck, z. B. „`PLZ|Wohnort`“, notiert und einer Variable zugeordnet werden; in den anderen XACML-Elementen können dann Referenzen auf diese Variablen verwendet werden (Element `VariableReference`). Somit ist es beispielsweise möglich, Gruppen von Attributen an Gruppen von Service Providern freizugeben.

- Bedingungen können wie oben erläutert mit Hilfe des XACML-Elements `Condition` ausgedrückt werden (siehe Zeilen 42–46); da die Benutzerattribute wie in Abschnitt 5.3.3 beschrieben als `ResourceContent` übergeben werden, kann die Herausgabe eines Attributs beispielsweise von den aktuellen Werten anderer Attribute abhängig gemacht werden. Ebenso bietet sich eine Auswertung der definierten Trust Levels an.

  Die über 200 verfügbaren Funktionen sind im Anhang der XACML-Spezifikation aufgeführt und werden hier nicht vertieft; die Ausdrucksmächtigkeit übersteigt jedoch z. B. diejenige der Shibboleth-ARPs bei Weitem.

- Analog dazu können XACML-`Obligations` wie in der Standardspezifikation beschrieben verwendet werden (siehe Zeilen 47–56). Da nur sehr wenige Obligationen standardisiert sind, ist häufig eine Erweiterung um eigene Varianten notwendig; insbesondere wenn die Obligationen zusammen mit den freigegebenen Attributen an den Service Provider übertragen werden sollen, da sie von diesem erfüllt werden müssen, muss eine föderationsweit einheitliche Benennung der Obligationsidentifikatoren geschaffen werden.

Im zugehörigen Beispiel wird die Kreditkartennummer des Benutzers für eine ausgewählte E-Commerce-Website zwischen 08:00 und 23:00 Uhr freigegeben, wobei beim erfolgreichen Abruf vom IDP des Benutzers eine E-Mail mit der Angabe des Service Providers und Verwendungszwecks geschickt wird:

```
1  <Policy id="xacmlUserARP_Anton_1" RuleCombiningAlgorithm="first-applicable">
2    <CombinerParameters>
3      <CombinerParameter ParameterName="ARPpriority">
4        100
5      </CombinerParameter>
6    </CombinerParameters>
7    <Description> ARP Nr. 1 von Benutzer Anton </Description>
8    <Rule id="Kreditkartennummer" effect="permit">
9      <Description> Kreditkartennummer an Online-Buchhandlung herausgeben </Description>
10     <Target>
11       <Resources>
12         <Resource>
13           <ResourceMatch MatchId="string-regexp-match">
14             <AttributeValue>
15               https://idp.example.com/Anton/defaultrole/creditCardNumber
16             </AttributeValue>
17             <ResourceAttributeDesignator AttributeId="userattribute-id"/>
18           </ResourceMatch>
19         </Resource>
20       </Resources>
21       <Subjects>
22         <Subject>
23           <SubjectMatch MatchId="string-regexp-match" AttributeValue="sp.example.com">
24             <SubjectAttributeDesignator AttributeId="service_provider-id"/>
25           </SubjectMatch>
26           <SubjectMatch MatchId="string-regexp-match" AttributeValue="Buchhandlung">
27             <SubjectAttributeDesignator AttributeId="service-id"/>
```

```
28            </SubjectMatch>
29            <SubjectMatch MatchId="string-regexp-match" AttributeValue="billing">
30              <SubjectAttributeDesignator AttributeId="purpose-id"/>
31            </SubjectMatch>
32          </Subject>
33        </Subjects>
34        <Actions>
35          <Action>
36            <ActionMatch MatchId="string-regexp-match" AttributeValue="read">
37              <ActionAttributeDesignator AttributeId="action-id"/>
38            </ActionMatch>
39          </Action>
40        </Actions>
41      </Target>
42      <Condition Function="time-in-range">
43        <Apply EnvironmentAttribute="current-time">
44        <value> 08:00:00 </value>
45        <value> 23:00:00 </value>
46      </Condition>
47      <Obligations>
48        <Obligation Id="Mail" FulfillOn="Permit">
49          <AttributeAssignment Id="text">
50            Ihre Kreditkartennummer wurde an den Dienstleister
51              <SubjectAttributeDesignator AttributeId="service_provider-id"/>
52            zu folgendem Zweck uebermittelt:
53              <SubjectAttributeDesignator AttributeId="purpose-id"/>
54          </AttributeAssignment>
55        </Obligation>
56      </Obligations>
57    </Rule>
58  </Policy>
```

Wie bereits erläutert kann jede Policy auf Basis der in [And04a] spezifizierten Methode elektronisch signiert und so gegen unbemerkte Manipulation geschützt werden.

Die Kombination der einzelnen ARPs zu einem `PolicySet` und die übrigen auswertungsspezifischen Abläufe werden im nächsten Abschnitt beschrieben.

5.3.3. Spezifikation des Verarbeitungsprozesses im XACML ARP-PEP

Nach der Beschreibung des grundlegenden Aufbaus der verwendeten Policies wird nun die **interne Architektur des FIM Privacy Management Systems** erläutert.

Die Auswertung der Attribute Release Policies wird wie in Abbildung 5.10 dargestellt vom XACML Policy Enforcement Point (PEP) koordiniert; er bietet den anderen FIM-Komponenten die im Architekturkonzept in Abschnitt 4.4.4 beschriebenen Schnittstellen an, über die er Anfragen entgegennimmt und für den XACML-PDP geeignet aufbereitet.

Die Entscheidungen des XACML-PDPs müssen interpretiert und für die Rückgabe an die aufrufende FIM-Komponente aufbereitet werden. Dieser Schritt umfasst insbesondere auch die Erfüllung der IDP-seitigen Obligationen, die vom XACML-PDP zusammen mit der Entscheidung geliefert werden – bei Langzeit-Obligationen ist hierzu die Kooperation mit dem Obligation Monitor des lokalen I&AM-Systems erforderlich.

Zur Verdeutlichung der Arbeitsschritte zur Policyermittlung und -kombination wird nachfolgend zuerst das Attribute Release Policy Repository beschrieben; in Abschnitt 5.3.3.2 wird anschließend der genaue Ablauf bei der Bearbeitung eingehender Anfragen spezifiziert. Die Auswertung der vom XACML-PDP gemeldeten Ergebnisse wird in Abschnitt 5.3.3.3 diskutiert.

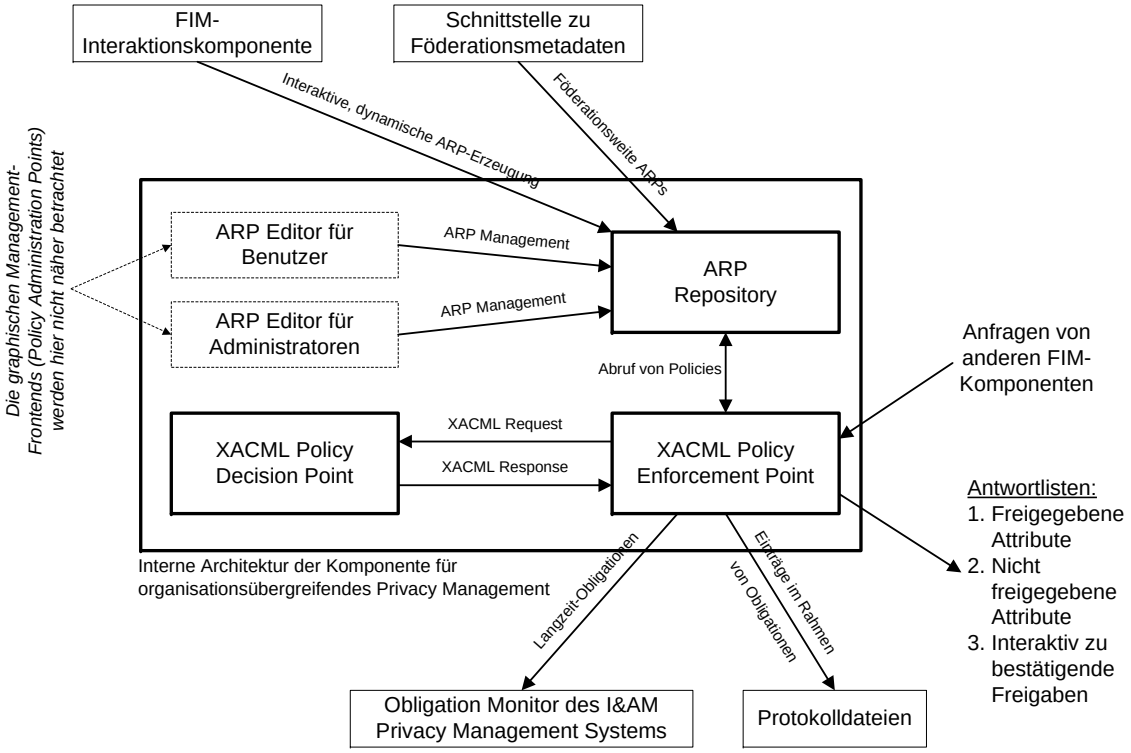


Abbildung 5.10.: Subkomponenten und Schnittstellen des XACML-basierten FIM Privacy Management Systems

5.3.3.1. Speicherung und Abruf von ARPs

Der Speicherort für die Attribute Release Policies wird als Policy Repository bzw. **ARP Repository** bezeichnet; während beispielsweise bei Shibboleth ein bestimmter Pfad im Dateisystem als ARP Repository fungiert, wird im Rahmen dieses Konzepts ein LDAP-Server eingesetzt.

Die Modellierung der LDAP-Attribute und des LDAP Directory Information Trees sind darauf ausgelegt, ein möglichst effizientes Auffinden der für eine Anfrage relevanten ARPs zu ermöglichen. Der ausschlaggebende Grund hierfür ist, dass aus Performanzgründen vermieden werden muss, die XACML `Target`- und `Condition`-Elemente *aller* Policies bzw. Rules bei jeder Anfrage erneut auswerten zu müssen, da z. B. von der beliebig großen Anzahl benutzerspezifischer ARPs in der Regel nur ein kleine Teilmenge pro Anfrage relevant ist.

Wie in Abbildung 5.11 dargestellt ist, wird aus diesem Grund zwischen drei Kategorien von ARPs unterschieden:

1. **Allgemeine ARPs**: Hierzu gehören z. B. föderations- und IDP-weite ARPs, die potentiell auf alle Benutzer zutreffen können.
2. **Individuelle ARPs**: In diesem Teilbaum des LDAP-Servers werden alle von Benutzern selbst spezifizierten ARPs abgelegt.

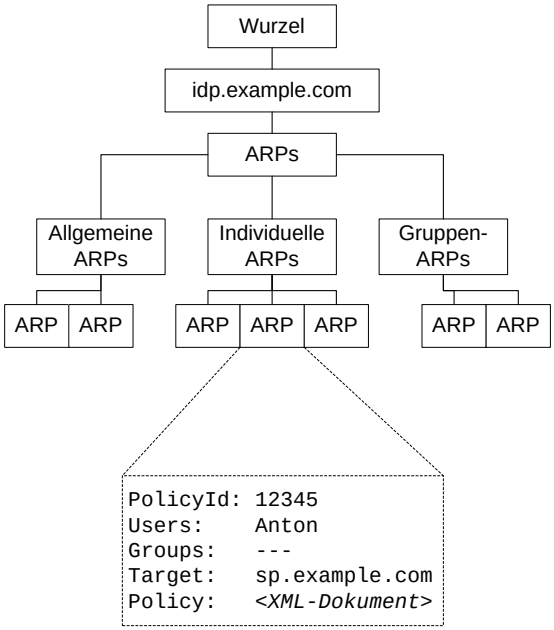


Abbildung 5.11.: Directory Information Tree und grundlegendes Schema des ARP Policy Repositories

3. **Gruppenspezifische ARPs**: Benutzer können Gruppen zugeordnet werden, für die wiederum ARPs definiert werden können, die alle Mitglieder einer Gruppe betreffen.

In jedem der drei LDAP-Teilbäume werden Objekte gespeichert, die folgende hier relevanten Attribute haben:

- `Policy`: In diesem single-value Attribut ist eine vollständige ARP, also ein XML-Dokument enthalten.
- `PolicyId`: Dieses single-value Attribut wird auf den Wert der auch in der Policy angegebenen `PolicyId` gesetzt; es dient lediglich zur eindeutigen Identifikation des Objekts im ARP Repository.
- `Users`: In dieses multi-value Attribut werden die Namen der Identitäten aller Benutzer eingetragen, für die diese ARP relevant ist; bei Verwendung des Wildcards `*` gilt die ARP für *alle* Benutzer.
- `Groups`: Analog zu `Users` kann eine Liste aller Gruppen angegeben werden, für die eine ARP relevant ist; dieses Attribut wird nur im LDAP-Teilbaum für gruppenspezifische ARPs benötigt.
- `Targets`: Ebenso können die Service Provider, für die eine ARP gilt, angegeben werden.

Die Menge der für eine Anfrage *potentiell* relevanten ARPs kann dann wie folgt ermittelt werden, wenn der anfragende Service Provider und die betroffene Identität bekannt sind:

1. In den LDAP-Teilbäumen mit allgemeinen bzw. individuellen ARPs werden die benötigten ARPs anhand des Attributs `Users` ermittelt.

2. Sofern der Benutzer Mitglied in Gruppen ist, werden aus dem LDAP-Teilbaum für gruppenspezifische ARPs alle für diese Gruppen relevanten ARPs ermittelt.

3. Die so gefundene Kandidatenmenge wird um diejenigen ARPs reduziert, die aufgrund der angegebenen `Targets` nicht zur Anfrage passen.

Diese drei Kriterien können zu einer einzigen LDAP-Suchanfrage zusammengefasst werden. In der verbleibenden Menge können jedoch nach wie vor für die konkrete Anfrage irrelevante ARPs enthalten sein, z. B. wenn

- sie einen anderen Dienst desselben Anbieters betreffen als die Anfrage, oder
- weitere Einschränkungen nicht im `Target`, sondern in einer beliebig komplexen `Condition` spezifiziert werden.

In diesem Fall würden nicht benötigte ARPs letztendlich vom XACML-PDP ignoriert werden; diese Vorgehensweise stellt deshalb einen effizienten Kompromiss zur Auswertung sämtlicher ARPs dar, bei dem mit geringem Aufwand mindestens alle benötigten und möglichst wenig darüber hinausgehende ARPs ermittelt werden.

Die weitere Verarbeitung der so gefundenen ARPs wird im folgenden Abschnitt spezifiziert.

5.3.3.2. Erzeugung und Auswertung des XACML-PolicySets

Wie bereits in den Abschnitten 4.4.3 und 4.4.4 beschrieben wurde, werden dem FIM Privacy Management System beim Aufruf über SOAP die folgenden Informationen übergeben:

- Der komplette Benutzerdatensatz, d. h. die aktuellen Werte *aller* Benutzerattribute.
- Angaben zur Anfrage, d. h. das Tripel (Service Provider, Service, Verwendungszweck).
- Details zum Zugriff, d. h. Art des Zugriffs, die Liste der betroffenen Attribute und bei Schreiboperationen deren neue Werte.

Die erste Aufgabe besteht in der Erzeugung eines vollständigen XACML `PolicySet`, das sämtliche vom XACML-PDP benötigten Daten enthält; dazu werden die folgenden Schritte durchgeführt:

1. Auf Basis der im Benutzerdatensatz enthaltenen Angaben über die Identität und Rolle des Benutzers sowie seine Gruppenzugehörigkeiten und des Namens des Service Providers werden wie im vorhergehenden Abschnitt erläutert alle potentiell relevanten ARPs ermittelt und aus dem Identity Repository abgerufen.

2. Die Policies werden anhand ihrer absteigenden Priorität sortiert, die jeweils dem XACML-Element `Combinerparameter` entnommen werden kann.

   Diesbezüglich ist zu beachten, dass jede Policy eine unterschiedliche Priorität haben sollte, um eine deterministische sortierte Reihenfolge zu erhalten; sind Policies mit gleicher Priorität nicht zu vermeiden, sollte zumindest sichergestellt werden, dass sie disjunkte `Target`-Angaben haben, da es ansonsten zu schwierig nachvollziehbaren Fehlersituationen kommen kann.

3. Die Policies werden ihrer Sortierreihenfolge gemäß in ein XACML `PolicySet` übertragen, d. h. die Policy mit der höchsten Priorität kommt zuerst. Als `PolicyCombiningAlgorithm` wird *first-applicable* verwendet; dadurch wird sichergestellt, dass von den zur Anfrage passenden nur genau die Policy mit der höchsten Priorität über das Ergebnis entscheiden wird.

Das somit konstruierte `PolicySet` kann von jedem XACML-konformen Policy Decision Point ausgewertet werden, ohne dass dieser an die hier spezifizierte ARP-Semantik angepasst werden müsste.

Da der XACML-PDP pro Anfrage nur *ein Gesamtergebnis* liefern kann, muss die Auswertung des `PolicySet` als zweite Aufgabe des hier beschriebenen PEPs separat für jedes einzelne der vom Lese- oder Schreibzugriff betroffenen Attribute durchgeführt werden. In einer Schleife wird deshalb für jedes dieser Attribute ein XACML-`Request` nach folgendem Schema erzeugt:

- Im `Subject` des `Request`-Elements werden die über den Anfragesteller verfügbaren Informationen auf die Attribute *service_provider-id*, *service-id* und *purpose-id* abgebildet.
- Die Zugriffsart wird als XACML-`Attribute` *action-id* im Element `Action` übergeben.
- Im Element `Resource` wird das im aktuellen Schleifendurchlauf bearbeitete Benutzerattribut als XACML-`Attribute` *userattribute-id* angegeben.
- Alle Attribute des zur Verfügung stehenden Benutzerdatensatzes werden in ein XACML `ResourceContent`-Element gekapselt innerhalb des `Resource`-Elements angehängt; sie sind dazu analog zum Identitätsdatenkonverter in XML zu verwandeln (siehe Abschnitt 5.2.2.1).
- Ebenso werden bei Schreibzugriffen auch die neuen Werte der zu modifizierenden Attribute als `ResourceContent` eingebracht; die Attributsnamen werden dabei durch den XML-Namespace `new` von den mit den aktuellen Werten belegten Attributen unterschieden.

Die beiden letzten Schritte sind an dieser Stelle notwendig, da ein XACML `PolicySet` aus syntaktischen Gründen keinen eigenen `ResourceContent` haben kann, wodurch eine strikte Trennung zwischen den Daten und die sie betreffenden Policies erreicht wird; die Benutzerattribute können somit nicht in das erzeugte `PolicySet` integriert werden und sind stattdessen bei jedem `Request` an den PDP zu übergeben.

Ein zur oben angegebenen Policy passender XACML-`Request` würde beispielsweise wie folgt aussehen:

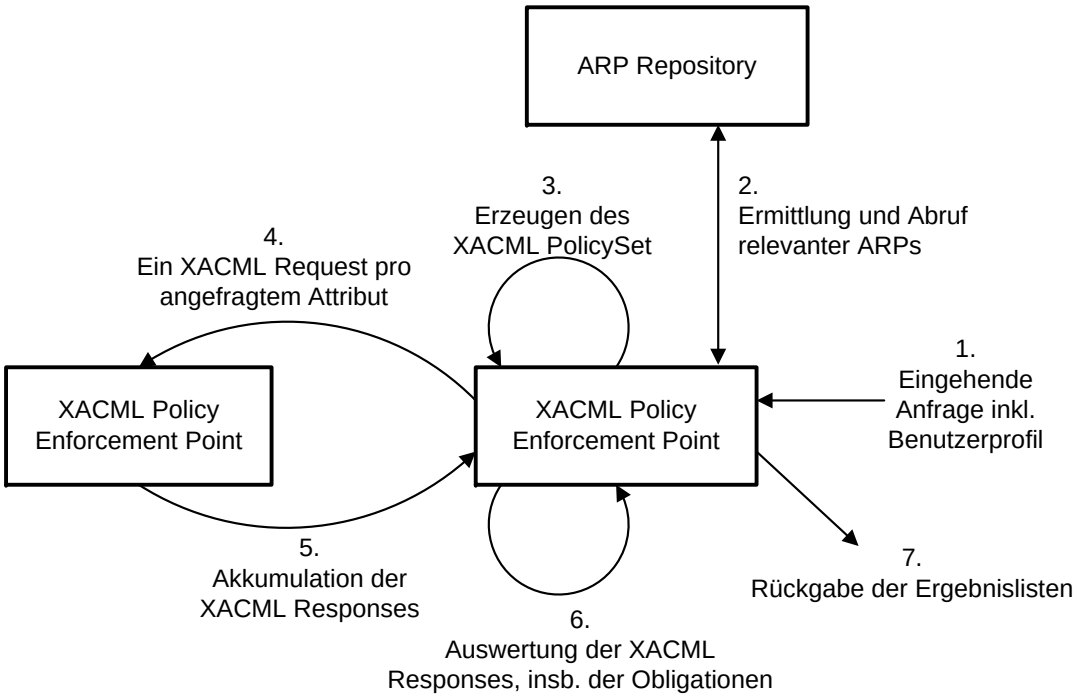


Abbildung 5.12.: Workflow bei der Anfragebearbeitung durch das FIM Privacy Management System

```
<Request>
  <Subject>
    <Attribute Id="service_provider-id">
      sp.example.com
    </Attribute>
    <Attribute Id="service-id">
      Buchhandlung
    </Attribute>
    <Attribute Id="purpose-id">
      billing
    </Attribute>
  </Subject>
  <Action>
    <Attribute Id="action-id">
      read
    </Attribute>
  </Action>
  <Resource>
    <Attribute Id="userattribute-id">
      https://idp.example.com/Anton/defaultrole/creditCardNumber
    </Attribute>
    <ResourceContent>
      <!-- Hier folgen die Benutzerattribute -->
    </ResourceContent>
  </Resource>
</Request>
```

Jeder `Request` wird dem XACML-PDP zusammen mit dem `PolicySet` als Eingabe übergeben. Die von ihm übermittelten Ergebnisse werden akkumuliert und anschließend wie im nächsten Abschnitt beschrieben ausgewertet.

Abbildung 5.12 zeigt eine Zusammenfassung dieser Arbeitsschritte.

5.3.3.3. Interpretation und Propagation der Auswertungsergebnisse

Pro von der Anfrage betroffenem Attribut muss eine XACML `Response` ausgewertet werden; die enthält eine `Status`-Angabe, die über eventuell PDP-intern aufgetretene Fehler informiert, sowie die eigentliche Entscheidung über die Freigabe des Attributs (XACML-Element `Decision`) und gegebenenfalls die zu erfüllenden Obligationen:

```
<Response>
  <Result ResourceId="https://idp.example.com/Anton/defaultrole/creditCardNumber">
    <Decision> Permit </Decision>
    <Status> OK </Status>
    <Obligations>
      <Obligation Id="Mail" FulfillOn="Permit">
        <AttributeAssignment Id="text">
          Ihre Kreditkartennummer wurde an den Dienstleister
            <SubjectAttributeDesignator AttributeId="service_provider-id"/>
          zu folgendem Zweck uebermittelt:
            <SubjectAttributeDesignator AttributeId="purpose-id"/>
        </AttributeAssignment>
      </Obligation>
    </Obligations>
  </Result>
</Response>
```

Wie in Abschnitt 4.4.4 bereits erläutert wurde, müssen die betroffenen Attribute in drei Gruppen zusammengefasst werden:

1. Attribute, bei denen die gewünschte Zugriffsart auf Grundlage der Policyauswertung zugelassen werden soll. Hierzu gehören alle Attribute, bei denen die XACML-`Response` den `Status` *OK* hat und die `Decision` *Permit* ist.

2. Attribute, deren Herausgabe bzw. Modifikation nicht erlaubt wird. Neben der `Decision` *Deny* gehören hierzu auch alle Attribute, bei denen der `Status` auf einen Fehler hinweist. Im Fehlerfall sollten auch Protokollmeldungen für die Administratoren generiert werden, da die diesbezüglichen Eingriffsmöglichkeiten für Benutzer sehr beschränkt sind, sofern das von Benutzern zum Editieren ihrer ARPs verwendete Frontend bereits das Einspielen syntaktisch fehlerhafter ARPs verhindert.

3. Attribute, bei denen der Benutzer interaktiv um Zustimmung gefragt werden soll; in Verbindung mit dem `Status` *OK* ist neben der `Decision` *Ask* auch die `Decision` *not applicable* zu berücksichtigen, die eintritt, wenn keines der XACML `Target`-Elemente auf die Anfrage zutrifft.

Der XACML-Standard sieht vor, dass der Policy Enforcement Point für die sofortige Umsetzung aller in einer `Response` enthaltenen Obligationen verantwortlich ist; insbesondere sind Entscheidungen, deren Obligationen nicht erfüllt werden können, wie *Deny* zu behandeln. Im Hinblick auf Langzeit-Obligationen und SP- statt IDP-seitig zu erfüllende Obligationen ist jedoch zwischen den folgenden Fällen zu unterscheiden:

1. **Vom XACML-PEP sofort zu erfüllende Obligationen**: Zu dieser Kategorie gehören insbesondere die beiden von XACML standardisierten Obligationen:

   - Generieren von Protokolleinträgen: Der in der Obligation enthaltene Text wird nach der Substitution der darin enthaltenen Variablen durch ihre aktuellen Werte in eine dem Benutzer zugeordnete Datenbasis eingetragen, die dieser wie in Abschnitt 4.4.5 beschrieben bei Bedarf einsehen kann.

- Versenden einer E-Mail: Analog zu den Protokolleinträgen kann der Text auch direkt per E-Mail an den Benutzer versendet werden; es bietet sich dabei an, alle zu einer Anfrage gehörenden Obligationen dieser Art zu einer einzigen E-Mail zusammenzufassen.

Darüber hinaus können für den ARP-spezifischen Einsatz noch die folgenden neuen Obligationen vorgesehen werden:

- Einmaliger E-Mail-Versand: Um den Benutzer bei ständiger Nutzung eines Dienstes nicht mit E-Mails zu überhäufen, wird bei dieser Obligation nur dann eine E-Mail verschickt, wenn das betroffene Attribut zum ersten Mal vom entsprechenden Service Provider abgerufen wird. Die Verwendung dieser Obligation setzt das Einverständnis des Benutzers zur Speicherung der Tupel (Service Provider, Attribut) voraus, die zur Entscheidung, ob eine E-Mail verschickt werden soll, notwendig sind.
- Anonymisierung von Datensätzen: Um die in Kapitel 2 definierte Anforderung [DSA-Anonymisierung] zu erfüllen, könnte durch eine Obligation die Anonymisierung der herauszugebenden Attribute angestoßen werden. Zu diesem Zweck können die Attribute beispielsweise analog zum Identitätsdatenkonverter von einem XSLT-Stylesheet verarbeitet werden, das z. B. Bestandteile von Attributen entfernt oder irreversibel modifiziert.

2. **IDP-seitige Langzeit-Obligationen**: Hierzu gehören alle Obligationen, die nicht sofort nach der Policyauswertung erfüllt werden können. Sie werden wie in den Abschnitten 4.3.6.1 und 4.4.4 erläutert an das organisationsinterne Privacy Management System übergeben.

3. **SP-seitige Obligationen**: Eine stark zunehmende Bedeutung hat die Übermittlung von Obligationen an die Service Provider, von denen die Attribute abgerufen werden (vgl. [STICKY, ROLPOL]). Somit können beispielsweise Daten mit der Auflage, nur eine bestimmte Maximaldauer gespeichert werden zu dürfen, übertragen werden; ein hierbei wesentliches und noch ungelöstes Problem ist die derzeit nicht vorhandene Möglichkeit, die SP-seitige Einhaltung dieser Auflagen überprüfen und nachvollziehen zu können. Wie in Abschnitt 4.7.1 diskutiert wurde, erscheint derzeit der Einsatz zertifizierter Software in Kombination mit gegen unbemerkte Manipulationen schützender Hardware als bislang einzige praktikable Lösung (vgl. [CMP05]).

   Bislang unterstützt keiner der in Kapitel 3 beschriebenen FIM-Ansätze die Übermittlung von Obligationen an SPs. Bis die Standardisierung auf diesem Sektor voranschreitet, muss deshalb beispielsweise von den Erweiterungsmöglichkeiten für SAML Assertions Gebrauch gemacht werden (vgl. [S2CORE, Kap. 7]). Diese provisorische Lösung bedingt jedoch entsprechende syntaktische Vereinbarungen zwischen den Föderationsteilnehmern, so dass die Interoperabilität im Allgemeinen nicht gewährleistet wäre.

Die hier neu eingeführte Integration von Obligationen in Attribute Release Policies sollte entsprechend bei Weiterentwicklungen der FIM-Standards vertieft werden.

Nach Abschluss der Behandlung von Obligationen werden die nach *permit*, *ask* und *deny* gruppierten Attribute als Ergebnis an die aufrufende FIM-Komponente zurückgegeben.

5.3.4. Anwendung von XACML-ARPs

Zur Veranschaulichung der ARP-spezifischen Verwendung von XACML werden im nachfolgenden Abschnitt zwei weitere einfache Beispiele gegeben; in Abschnitt 5.3.4.2 wird abschließend demonstriert, wie bereits vorhandene Shibboleth-ARPs automatisch und verlustfrei in XACML-ARPs konvertiert werden können, um eine ggf. notwendige Migration zu erleichtern.

5.3.4.1. Einfache Beispiele für XACML-ARPs

Die folgende Attribute Release Policy ist minimal, aber praxisrelevant; sie gibt lediglich das Attribut `eduPersonScopedAffiliation`, das die Art der Zugehörigkeit eines Benutzers zu seinem IDP angibt, an alle Service Provider für lesende Zugriffe frei. In der deutschen Shibboleth-basierten Föderation DFN-AAI ist die Bereitstellung dieses Attributs verpflichtend, so dass Service Provider z. B. *Studenten* von *Mitarbeitern* einer an der DFN-AAI beteiligten Hochschule unterscheiden können. Es handelt sich somit um eine typische föderationsweite ARP:[6]

```
<Policy id="DFN-AAI-ePSA" RuleCombiningAlgorithm="first-applicable">
  <CombinerParameters>
    <CombinerParameter ParameterName="ARPpriority">
      1000
    </CombinerParameter>
  </CombinerParameters>
  <Description> Freigabe von eduPersonScopedAffiliation an alle SPs </Description>
  <Rule id="DFN-AAI-ePSA-1" effect="permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="string-regexp-match">
            <AttributeValue>
              https://.*/.*/.*/eduPersonScopedAffiliation
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="userattribute-id"/>
          </ResourceMatch>
        </Resource>
      </Resources>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="string-regexp-match" AttributeValue=".*">
            <SubjectAttributeDesignator AttributeId="service_provider-id"/>
          </SubjectMatch>
        </Subject>
      </Subjects>
      <Actions>
        <Action>
          <ActionMatch MatchId="string-regexp-match" AttributeValue="read">
            <ActionAttributeDesignator AttributeId="action-id"/>
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
  </Rule>
</Policy>
```

Das folgende zweite Beispiel zeigt die Gruppierung von Benutzerattributen und deren Freigabe für beide Varianten von Lesezugriffen an zwei ausgewählte Service Provider; eine SP-seitig zu erfüllende Obligation ist das Löschen der Daten nach spätestens 90 Tagen:

```
<Policy id="Anschrift_fuer_SP1_und_SP2" RuleCombiningAlgorithm="first-applicable">
  <CombinerParameters>
    <CombinerParameter ParameterName="ARPpriority">
      100
    </CombinerParameter>
  </CombinerParameters>
```

[6] Anmerkung: Im Rahmen der DFN-AAI werden derzeit Shibboleth-ARPs, nicht XACML-ARPs, eingesetzt; somit müssen „föderationsweite“ ARPs von jedem IDP lokal implementiert werden.

```
7   <Rule id="rule1" effect="permit">
8     <Target>
9       <Resources>
10        <Resource>
11          <ResourceMatch MatchId="string-regexp-match">
12            <AttributeValue>
13              <VariableReference VariableId="Anschrift"/>
14              <!-- Siehe Variablendefinition unten -->
15            </AttributeValue>
16            <ResourceAttributeDesignator AttributeId="userattribute-id"/>
17          </ResourceMatch>
18        </Resource>
19      </Resources>
20      <Subjects>
21        <Subject>
22          <SubjectMatch MatchId="string-regexp-match"
23                        AttributeValue="sp1.example.com|sp2.example.com">
24            <SubjectAttributeDesignator AttributeId="service_provider-id"/>
25          </SubjectMatch>
26        </Subject>
27      </Subjects>
28      <Actions>
29        <Action>
30          <ActionMatch MatchId="string-regexp-match" AttributeValue="read|subscribe">
31            <ActionAttributeDesignator AttributeId="action-id"/>
32          </ActionMatch>
33        </Action>
34      </Actions>
35    </Target>
36    <Obligations>
37      <Obligation Id="SP:retention-limit:90days" FulfillOn="Permit"/>
38    </Obligations>
39    <VariableDefinition VariableId="Anschrift">
40        https://idp.example.com/Anton/defaultrole/(Vorname|Nachname|Strasse|PLZ|Ort|Land)
41    </VariableDefinition>
42  </Rule>
43 </Policy>
```

Die Verwendung von XACML-Variablendefinitionen zur Gruppierung von Attributen ist insbesondere dann effektiv, wenn die Variablenreferenzen in mehreren Policies verwendet werden.

5.3.4.2. Verlustfreie Konvertierung von Shibboleth ARPs

Ein für die Praxis nicht unwesentlicher Aspekt ist die Möglichkeit, Shibboleth-ARPs ohne Informationsverlust in XACML-ARPs konvertieren zu können; dies ermöglicht beispielsweise eine Umstellung auf XACML-ARPs im laufenden Betrieb, ohne dass jeder Benutzer seine Dateifreigaben neu konfigurieren muss.

Das nachfolgende XSLT-Stylesheet konvertiert Shibboleth-ARPs mit beliebig vielen Regeln in das oben spezifizierte XACML-basierte ARP-Format. Es dient ferner als Beispiel für die Transformation ganzer Policies, die wie in Abschnitt 4.4.11 erläutert beispielsweise zur Anpassung föderationsweiter ARPs an das lokale Datenmodell erforderlich ist.

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
3    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4    xmlns:shibarp="urn:mace:shibboleth:arp:1.0"
5    xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy">
6  <xsl:output method="xml" indent="yes" encoding="UTF-8"/>
7
8  <!-- Variable arpid holds the XACML policy id -->
9  <xsl:variable name="arpid" select="'Converted_ARP'"/>
10 <!-- Variable idp_user holds the XACML resource attributevalue prefix -->
11 <xsl:variable name="idp_user" select="'https://idp.example.com/identity/defaultrole/'"/>
12
13 <!-- XSLT processing starts here -->
14 <xsl:template match="/">
15   <xsl:comment> ARP converted from Shibboleth to XACML format </xsl:comment>
16   <xsl:apply-templates select="shibarp:AttributeReleasePolicy"/>
17 </xsl:template>
18
19 <!-- Build the structure of the XACML Policy -->
20 <xsl:template match="shibarp:AttributeReleasePolicy">
```

```
21    <Policy RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
22      <xsl:attribute name="PolicyId"> <xsl:value-of select="$arpid"/> </xsl:attribute>
23      <xsl:apply-templates select="shibarp:Description"/>
24      <xsl:apply-templates select="shibarp:Rule"/>
25    </Policy>
26  </xsl:template>
27
28  <!-- Copy the ARP description -->
29  <xsl:template match="shibarp:Description">
30    <Description> <xsl:apply-templates/> </Description>
31  </xsl:template>
32
33  <!-- Convert each Shibboleth rule -->
34  <xsl:template match="shibarp:Rule">
35    <!-- Create a XACML rule for each Shibboleth ARP Attribute element -->
36    <xsl:apply-templates select="shibarp:Attribute"/>
37  </xsl:template>
38
39  <!-- Convert each Shibboleth ARP Attribute element -->
40  <xsl:template match="shibarp:Attribute">
41    <Rule>
42      <Target>
43        <!-- Each XACML rule must have a unique id -->
44        <xsl:attribute name="id"> <xsl:value-of select="generate-id(.)"/> </xsl:attribute>
45        <!-- Decide whether the rule's effect should be permit or deny, based
46             on the "release" attribute of ShibARPs Value/AnyValue elements. -->
47        <xsl:attribute name="effect">
48          <xsl:choose>
49            <xsl:when test="shibarp:Value/@release='permit'">
50              <xsl:value-of select="'permit'"/>
51            </xsl:when>
52            <xsl:when test="shibarp:AnyValue/@release='permit'">
53              <xsl:value-of select="'permit'"/>
54            </xsl:when>
55            <xsl:otherwise>
56              <xsl:value-of select="'deny'"/>
57            </xsl:otherwise>
58          </xsl:choose>
59        </xsl:attribute>
60
61        <!-- Add the Action element, which is always "read" -->
62        <xsl:call-template name="addAction"/>
63
64        <!-- Add the Subject element, which is based on the ShibARP rule's Target element. -->
65        <xsl:call-template name="addTarget"/>
66
67        <!-- The attribute "name" holds the resource; unless there is an
68             AnyValue child, there also has to be a XACML condition. -->
69        <Resources>
70          <Resource>
71            <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
72              <AttributeValue>
73                <xsl:choose>
74                  <!-- If the ShibARP rule is flagged as 'default', apply it to anybody.
75                       Otherwise, restrict it to the user whom this ARP belongs to. -->
76                  <xsl:when test="../@default='true'">
77                    <xsl:value-of select="concat('*/',
78                          substring-after(@name, 'urn:mace:eduPerson:1.0:'))"/>
79                  </xsl:when>
80                  <xsl:otherwise>
81                    <xsl:value-of select="concat($idp_user, substring-after(@name,
82                       'urn:mace:eduPerson:1.0:'))"/>
83                  </xsl:otherwise>
84                </xsl:choose>
85              </AttributeValue>
86              <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
87                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:userattribute-id"/>
88            </ResourceMatch>
89          </Resource>
90        </Resources>
91      </Target>
92
93      <!-- Optional XACML condition -->
94      <xsl:if test="not(shibarp:AnyValue)">
95        <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
96          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
97            <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#string">
98              <xsl:attribute name="RequestContextPath">
99                <xsl:value-of select="concat('//xacml:user/xacml:attributes/xacml:',
100                          substring-after(@name, 'urn:mace:eduPerson:1.0:'))"/>
101             </xsl:attribute>
102           </AttributeSelector>
103         </Apply>
104         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
105           <xsl:value-of select="./shibarp:Value"/>
106         </Apply>
107       </Condition>
108     </xsl:if>
109   </Rule>
110 </xsl:template>
```

```
111
112 <!-- Convert Shibboleth ARP Targets into XACML subjects -->
113 <xsl:template name="addTarget">
114   <xsl:param name="targ" select="../shibarp:Target"/>
115   <!-- The Shibboleth target is either <AnyTarget> or <Requester> -->
116   <Subjects>
117     <xsl:choose>
118       <xsl:when test="../shibarp:Target/shibarp:AnyTarget">
119         <!-- It's <AnyTarget> -->
120         <SubjectMatch MatchId="string-regexp-match" AttributeValue=".*">
121           <SubjectAttributeDesignator AttributeId="service_provider-id"/>
122         </SubjectMatch>
123       </xsl:when>
124     <xsl:otherwise>
125         <!-- It's <Requester> -->
126         <Subject>
127           <!-- We assume that the Requester value has the format
128                https://service.provider.com/path/to/service/ -->
129           <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
130             <xsl:attribute name="AttributeValue">
131               <xsl:value-of select="substring-before(substring-after($targ, 'https://'), '/')"/>
132             </xsl:attribute>
133             <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
134               AttributeId="service_provider-id"/>
135           </SubjectMatch>
136           <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
137             <xsl:attribute name="AttributeValue">
138               <!-- The following selection retrieves the /path/to/service/ part of the Requester
139                    value, removes the leading / and also removes the optional trailing / by
140                    converting all slashes to spaces, normalizing the string and then converting
141                    all spaces back to slashes. The inner normalize-space call removes any optional
142                    whitespaces in the Requester value first. The result is "path/to/service". -->
143               <xsl:value-of select="translate(normalize-space(translate(normalize-space(
144                    substring-after($targ, concat(substring-before(substring-after($targ,
145                    'https://'), '/'), '/'))), '/', ' ')), ' ', '/')"/>
146             </xsl:attribute>
147             <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
148                 AttributeId="service-id"/>
149           </SubjectMatch>
150         </Subject>
151       </xsl:otherwise>
152     </xsl:choose>
153   </Subjects>
154 </xsl:template>
155
156 <xsl:template name="addAction">
157   <Actions>
158     <Action>
159       <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"
160         AttributeValue="read">
161         <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
162             AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
163       </ActionMatch>
164     </Action>
165   </Actions>
166 </xsl:template>
167
168 </xsl:stylesheet>
```

Wie anhand von Zeile 21 ersichtlich ist, wird die Konvertierung erheblich dadurch vereinfacht, dass XACML auch den von Shibboleth verwendeten Regelkombinationsalgorithmus *deny-overrides* unterstützt. Bei einer Modifikation der so konvertierten Shibboleth-ARPs muss allerdings berücksichtigt werden, dass *deny-overrides* und *first-applicable* nicht miteinander kombiniert werden können, da die prioritätsbasierte Policyauswertung eine stark abweichende Semantik hat.

Eine mögliche Lösung dieses Problems besteht darin, konvertierten Shibboleth User ARPs eine höhere Priorität zuzuweisen als der konvertierten Shibboleth Site ARP; dies ist jedoch nur für Szenarien geeignet, in denen der Vorrang benutzerspezifischer ARPs vor IDP- und föderationsweiten ARPs gewünscht oder toleriert wird.

Das XSLT-Stylesheet kann von einem beliebigen XSLT-Prozessor verarbeitet werden; als Eingabe kann z. B. die folgende, dem ersten Beispiel aus Abschnitt 5.3.4.1 nachempfundene Shibboleth-ARP dienen:

```
<?xml version="1.0" encoding="UTF-8" ?>
<arp:AttributeReleasePolicy xmlns:arp="urn:mace:shibboleth:arp:1.0"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:mace:shibboleth:arp:1.0 shib-arp-1.0.xsd">
   <arp:Description>
      Freigabe der eduPersonScopedAffiliation an alle Service Provider
   </arp:Description>
   <arp:Rule>
      <arp:Target><arp:AnyTarget/></arp:Target>
      <arp:Attribute
         name="urn:mace:eduPerson:1.0:eduPersonScopedAffiliation">
         <arp:AnyValue release="permit"/>
      </arp:Attribute>
   </arp:Rule>
</arp:AttributeReleasePolicy>
```

Die Ausgabe entspricht dem bereits als XACML-ARP angegebenen Beispiel mit der genannten Abweichung bzgl. `RuleCombiningAlgorithm`:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- ARP converted from Shibboleth to XACML format -->
<Policy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:shibarp="urn:mace:shibboleth:arp:1.0"
        xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides"
        PolicyId="Converted_ARP">
   <Description>
      Freigabe der eduPersonScopedAffiliation an alle Service Provider
   </Description>
   <Rule>
      <Target id="id44712" effect="permit">
         <Actions>
            <Action>
               <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"
                  AttributeValue="read">
                  <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                    AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
               </ActionMatch>
            </Action>
         </Actions>
         <Subjects>
            <SubjectMatch MatchId="string-regexp-match" AttributeValue=".*">
               <SubjectAttributeDesignator AttributeId="service_provider-id"/>
            </SubjectMatch>
         </Subjects>
         <Resources>
            <Resource>
               <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
                  <AttributeValue>
                     https://idp.example.com/identity/defaultrole/eduPersonScopedAffiliation
                  </AttributeValue>
                  <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:userattribute-id"/>
               </ResourceMatch>
            </Resource>
         </Resources>
      </Target>
   </Rule>
</Policy>
```

Beim praktischen Einsatz könnten als weitere Verfeinerung die Namen der Identitäten, deren Shibboleth User ARP bearbeitet wird, an den XSLT-Prozessor übergeben werden, so dass ein komplettes ARP Repository konvertiert werden kann, ohne dass eine manuelle Nachbearbeitung notwendig wird.

5.4. Attribute Acceptance Policies auf XACML-Basis

Attribute Acceptance Policies (AAPs) stellen bei Service Providern das Pendant zu den Attribute Release Policies bei Identity Providern dar. Wie in Abschnitt 4.4.8 bereits diskutiert wurde, dienen die AAPs primär der Sicherstellung der SP-seitig geforderten Datenqualität,

zu der in diesem Fall insbesondere auch die Vollständigkeit des übermittelten Benutzerprofils gehört; nachfolgend wird somit das Innenleben der FIM-Komponente zur Auswertung der Attribute Acceptance Policies spezifiziert.

Zuerst werden hierzu die konzeptionell bei AAPs verfolgten Ziele in Abschnitt 5.4.1 erläutert. Die Motivation, wie für ARPs auch für AAPs die Policysprache XACML einzusetzen, wird in Abschnitt 5.4.2 diskutiert. Abschließend werden in Abschnitt 5.4.3 die Syntax und die Semantik von XACML-basierten ARPs spezifiziert; die Darstellung ist dabei aufgrund der Analogien zu den XACML-ARPs bewusst knapp gehalten.

5.4.1. Ziele des AAP-Konzepts

Um die Ausprägung des AAP-Konzepts zu erläutern, wird zuerst eine grobe Kategorisierung der SP-seitig erfassten und verarbeiteten Daten vorgestellt; daran anschließend werden die grundlegenden Anforderungen an AAPs diskutiert.

5.4.1.1. Kategorisierung der SP-seitig erfassten Daten

Die im Architekturkonzept beschriebene Integration der SP-Software in das I&AM-System des Service Providers zielt wie erläutert auf die uneingeschränkte Nutzung aller über FIM akquirierten Benutzerdatensätze durch die dort eingesetzten Dienste und prozessunterstützenden Werkzeuge ab. Diesbezüglich können personenbezogene Daten grob in die folgenden drei nicht zwangsweise disjunkten Kategorien eingeteilt werden:

1. Daten, die **zur Erbringung des Dienstes unbedingt erforderlich** sind; hierzu gehören unter anderem auch Angaben für das Rechnungswesen, ohne die eine Nutzung des Dienstes nicht aus technischen, sondern aus organisatorischen Gründen ausgeschlossen ist.
2. Profilinformationen, die eine **Personalisierung** eines angebotenen Dienstes ermöglicht; die Übermittlung dieser optionalen Daten an den SP ist somit mit Vorteilen für den Benutzer verknüpft.
3. Profilinformationen, die beispielsweise auf demographischen Informationen beruhen und SP-seitig z. B. mit **Data Mining** Verfahren ausgewertet werden, um die eigenen Angebote zu verbessern.

Beispielsweise könnten auf Basis der in Rechnungsanschriften enthaltenen Postleitzahlen Statistiken über die geographische Herkunft der Benutzer erstellt werden, um in Ballungszentren gezieltes Marketing betreiben zu können; die Nutzung der Daten für diesen Zweck muss deshalb offensichtlich Datenschutzregelungen unterliegen.

Darüber hinaus ist zu differenzieren, wie ein Service Provider an Profilinformationen gelangt:

1. Die Daten werden **mittels FIM von einem IDP** oder einer AA eingeholt.
2. Die Daten werden **vom Benutzer während der Dienstnutzung** explizit eingegeben, wobei dieser den damit verbundenen Verwendungszwecken zustimmt.

3. Der SP analysiert das **Dienstnutzungsverhalten**, indem er z. B. auswertet, für welche Funktionen des Dienstes sich ein Benutzer besonders häufig interessiert; dies wird im Umfeld von Webapplikationen auch als Clickstream-Analyse bezeichnet und bei E-Commerce-Webseiten häufig für gezielte Kaufempfehlungen eingesetzt (vgl. [KM05]).

Die hier beschriebenen Attribute Acceptance Policies greifen für prinzipiell alle Arten von Daten, sofern diese FIM-basiert übertragen werden; die beiden anderen Formen der Datenakquisition sind nicht FIM-spezifisch und können in der Regel unverändert beibehalten werden.

5.4.1.2. Prinzipielle Anforderungen an Attribute Acceptance Policies

Wie aus ihrem Namen bereits hervorgeht, entscheiden Attribute Acceptance Policies darüber, ob die in allgemeinen Attributsauskünften enthaltenen Attribute und deren Werte an das SP-seitige I&AM-System weitergegeben oder verworfen werden sollen; somit ergeben sich an die Funktionalität folgende Anforderungen:

- Die Vollständigkeit der übermittelten Identitätsdaten im Hinblick auf die lokal zwangsweise erforderlichen Attribute muss sichergestellt werden können.
- Die Werte der Attribute müssen überprüft werden können; bezugnehmend auf das in Abschnitt 5.3.4.1 gegebene Beispiel kann es erforderlich sein, den Zugang zu Diensten anhand des Attributs `eduPersonScopedAffiliation` auf Angehörige des Typs *Mitarbeiter* ausgewählter Hochschulen einzuschränken.
- Attribute, die nach einer einmaligen Auswertung in den AAPs nicht mehr benötigt werden, sollen aus Datenschutzgründen verworfen und nicht in das SP-seitige I&AM-System eingetragen werden.

In den ersten beiden Fällen würde folglich das komplette Benutzerprofil verworfen und die Dienstnutzung nicht gestattet werden. Der dritte Anwendungsfall zum Filtern einzelner Attribute ist darüber hinaus praxisrelevant, da Implementierungen wie Shibboleth derzeit immer sämtliche durch ARPs freigegebene Attribute an SPs zurückliefern und nicht nur einzelne angeforderte; durch das Verwerfen ausgewählter Attribute können somit von korrekt konfigurierten SPs nicht ausreichend restriktive ARPs kompensiert werden.

Für AAPs gelten analog zu ARPs die folgenden Anforderungen hinsichtlich ihres verteilten Managements:

- Wie in Abschnitt 4.4.11 erläutert sollen föderationsweite AAPs unterstützt werden.
- Service Provider definieren in der Regel ein Minimum an benötigten Attributen und daran gestellte Qualitätsanforderungen; diese sollen in Form SP-weiter AAPs umgesetzt werden.
- Darüber hinaus kann es spezielle Anforderungen je nach Dienst geben, die abgebildet werden müssen. Insbesondere kann derselbe Dienst auch in verschiedenen Varianten angeboten werden, die ggf. zusätzliche Benutzerattribute benötigen.

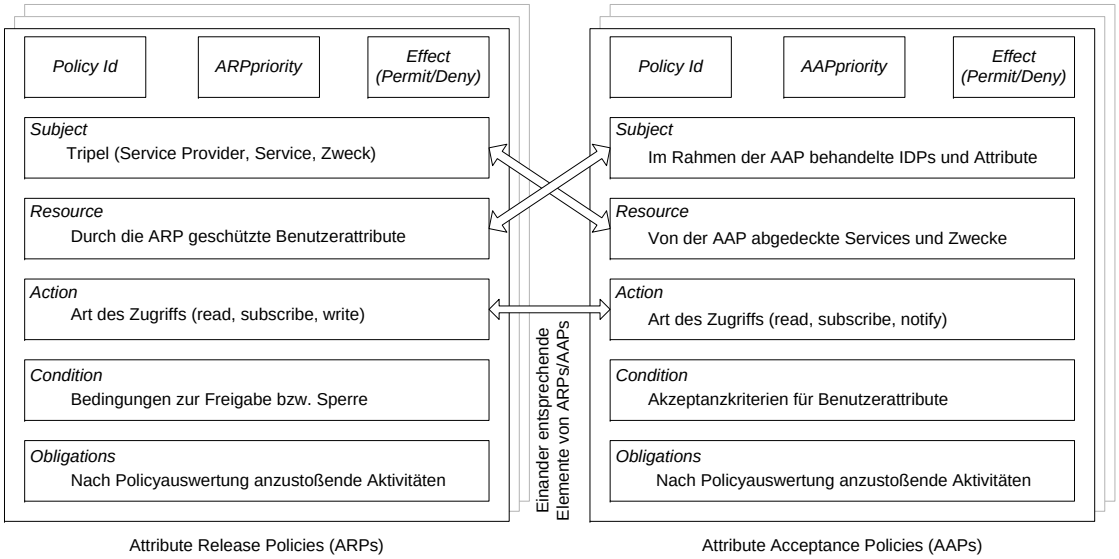


Abbildung 5.13.: Analoge Struktur von ARPs und AAPs und ihre komplementären Elemente

Bereits hinsichtlich dieser äußerlichen Betrachtung ergeben sich starke Gemeinsamkeiten zwischen ARPs und AAPs, die eine im nächsten Abschnitt beschriebene Untersuchung weiterer Ähnlichkeiten motiviert haben.

5.4.2. Motivation für den Einsatz von XACML für ARPs und AAPs

Im Unterschied zu ARPs, deren Notwendigkeit wie erläutert inzwischen auch insbesondere von der Liberty Alliance betont wird, ohne sie zu konkretisieren, werden AAPs in den aktuellen Industriestandards derzeit noch überhaupt nicht erwähnt; dies ist sicherlich zum Teil darauf zurückzuführen, dass bei diesen bisherigen Ansätzen jeder Dienst selbst FIM-fähig sein muss und für die Verarbeitung der bezogenen Daten eigenverantwortlich ist. Lediglich Shibboleth bietet eine AAP-Implementierung, die analog zu den Shibboleth-ARPs durch die beschränkte Ausdrucksfähigkeit der dafür verwendeten proprietären, XML-basierten Sprache geprägt ist.

In der eigenen Publikation [Hom06a] wurde aus den oben genannten Anforderungen eine interne Struktur für AAPs abgeleitet und einer früheren Version des in Abschnitt 5.3 vorgestellten ARP-Konzepts gegenüber gestellt. Die aus dem aktuellen Konzept resultierenden Ergebnisse werden nachfolgend knapp zusammengefasst und sind in Abbildung 5.13 dargestellt:

- In AAPs muss angegeben werden können, auf welche Dienste sie sich beziehen; dies folgt aus der Anforderung, dass es mehrere verschiedene, für einen konkreten Fall relevante AAPs geben kann und unterscheidet sich vom Shibboleth AAP-Konzept, in dem genau eine AAP für genau einen Dienst zuständig ist.

  Wie oben erläutert können sich AAPs in Abhängigkeit von der Dienstausprägung unterscheiden; zudem muss auch SP-seitig zwischen verschiedenen Datenverarbeitungszwecken unterschieden werden. Es bietet sich deshalb an, den bei XACML-ARPs für die

`Subject`-Angaben verwendeten Namensraum auf die `Resource`-Angaben in AAPs zu übertragen.

- Ebenso müssen die Attribute, auf die sich die AAP bezieht, deklariert werden können; hierfür ist eine Unterscheidung je nach IDP wünschenswert, da an die von verschiedenen IDPs gelieferten Daten prinzipiell auch unterschiedliche Qualitätsanforderungen gestellt werden können. Somit liegt es nahe, den bei XACML-ARPs für `Resource`-Angaben verwendeten Namensraum für die `Subjects` von AAPs zu verwenden.
- Die Zugriffsart sollte in AAPs ebenfalls wie in ARPs spezifiziert werden können, wobei funktionsbedingt lediglich die beiden Werte *read* und *subscribe* für vom SP initiierte Anfragen sowie *notify* bei eingehenden Aktualisierungsnachrichten in Frage kommen (siehe auch Abschnitt 5.5.2).
- Ebenfalls analog zu ARPs sollen beliebige Bedingungen verwendet werden können, um über die Weiterverwendung von Attributen beispielsweise auf Basis von Trust Levels entscheiden zu können, und Obligationen unterstützt werden, die beispielsweise zurückgewiesene Datensätze für weitere Analysen in Protokolldateien aufbewahren.

Durch die komplementären Anforderungen an ARPs und AAPs und ihre strukturelle Ähnlichkeit sowie die gemeinsame Verwendung von Namensräumen für die Identifikation von Diensten und Attributen liegt es nahe, XACML auch für AAPs einzusetzen, so dass Synergien durch vorhandene XACML-Kenntnisse und -Werkzeuge genutzt werden können. Darüber hinaus ist zu beachten, dass es für AAPs mit Ausnahme des Shibboleth-Ansatzes noch keine dedizierten Policysprachen und -implementierungen existierten, so dass eine Entscheidung für XACML auch unabhängig von bereits existierenden XACML-ARPs analog zum in Abschnitt 5.3.1 beschriebenen Selektionsprozess getroffen werden kann.

Bei der Verwendung einer gemeinsamen Policysprache für ARPs und AAPs ergibt sich darüber hinaus der Vorteil, dass u. U. eine effiziente Policyschnittmengenbildung ermöglicht wird, anhand derer über Freigabe und Akzeptanz von Attributen entschieden werden kann, ohne dass deren Werte zur Prüfung an den Service Provider übermittelt werden müssen. Voraussetzung hierfür ist jedoch die Erfüllung bestimmter algebraischer Eigenschaften (vgl. [BDS04, BPS03]), die bislang nur für eine als Web Services Policy Language bezeichnete echte Teilmenge von XACML erfüllt wird (siehe [WSPL] und [And04c]); diesbezüglich sind insbesondere die Neuerung durch XACML 3.0 abzuwarten.

5.4.3. Spezifikation von AAPs in XACML

In diesem Abschnitt wird die exakte Verwendung von XACML zur Spezifikation von AAPs erläutert, wie sie von der in Abschnitt 4.4.8 diskutierten FIM-Komponente ausgewertet werden; die angegebenen Zeilennummern beziehen sich auf die untenstehende Beispiel-AAP:

- Als `PolicyCombiningAlgorithm` wird wiederum *first-applicable* gewählt, um die Auswertung der Policy mit der höchsten Priorität, die als `PolicyCombinerParameter` *AAP-priority* angegeben wird, sicherzustellen (vgl. Zeilen 1–6).
- Der `effect` von Regeln kann *permit* oder *deny* sein (siehe Zeile 8).

- Die Subkomponenten des `Target`-Elements werden wie folgt eingesetzt (vgl. Zeilen 10–39):
  - Die den Diensten und Anwendungszwecken entsprechenden `Resources` werden gemäß dem bei ARPs definierten Namensraum verwendet (siehe Zeilen 11-23). Zur Gruppierung mehrerer Dienste oder Anwendungszwecke können wiederum Wildcards und `VariableDefinition`-Elemente eingesetzt werden.
  - Als `Subject` können Mengen von Benutzerattributen angegeben werden; durch die Verwendung des bereits bei ARPs eingeführten Namensraums kann insbesondere zwischen den von verschiedenen IDPs bzw. AAs gelieferten Attributen differenziert werden, so dass unterschiedliche Anforderungen an die Benutzerprofile unterschiedlicher Herkunft gestellt werden können (siehe Zeilen 24–31).
  - Als `Action` wird *read*, *subscribe* oder *notify* verwendet; bei vom SP ausgehenden schreibenden Zugriffen (`Action` *write* in ARPs) spielen AAPs keine Rolle (siehe Zeilen 32–38). Die Werte *read* und *subscribe* werden in der Regel gleich behandelt; der Wert *notify* kommt zum Einsatz, wenn das Attribut in Form einer Aktualisierungsbenachrichtigung eingegangen ist (vgl. Abschnitte 4.4.1.1 und 5.5).
- Für Bedingungen können XACML `Condition`-Elemente im selben Umfang wie bei ARPs eingesetzt werden (siehe Zeilen 40–44).
- Über die zum Einsatz kommenden XACML-`Obligations` können neben den standardisierten Protokoll- und Mailversandmöglichkeiten auch die unten beschriebenen Steuerungsmöglichkeiten zur Kommunikation mit der Datenquelle der überprüften Attribute genutzt werden (siehe Zeilen 45–52).

Das zugehörende Beispiel akzeptiert die Kreditkartennummer eines Benutzers nicht, wenn ihr Gültigkeitsdatum bereits überschritten wurde:

```
1  <Policy id="xacml_AAP_1" RuleCombiningAlgorithm="first-applicable">
2    <CombinerParameters>
3      <CombinerParameter ParameterName="AAPpriority">
4        20
5      </CombinerParameter>
6    </CombinerParameters>
7    <Description> Attribute Acceptance Policy der Online-Buchhandlung </Description>
8    <Rule id="Kreditkartengueltigkeit" effect="deny">
9      <Description> Gueltigkeitsdatum der Kreditkarte pruefen </Description>
10     <Target>
11       <Resources>
12         <Resource>
13           <ResourceMatch MatchId="string-regexp-match" AttributeValue="sp.example.com">
14             <ResourceAttributeDesignator AttributeId="service_provider-id"/>
15           </ResourceMatch>
16           <ResourceMatch MatchId="string-regexp-match" AttributeValue="Buchhandlung">
17             <ResourceAttributeDesignator AttributeId="service-id"/>
18           </ResourceMatch>
19           <ResourceMatch MatchId="string-regexp-match" AttributeValue="billing">
20             <ResourceAttributeDesignator AttributeId="purpose-id"/>
21           </ResourceMatch>
22         </Resource>
23       </Resources>
24       <Subjects>
25         <Subject>
26           <SubjectMatch MatchId="string-regexp-match"
27                 AttributeValue="https://idp.*/.*/.*/creditCardNumber">
28             <SubjectAttributeDesignator AttributeId="userattribute-id"/>
29           </SubjectMatch>
30         </Subject>
31       </Subjects>
32       <Actions>
33         <Action>
34           <ActionMatch MatchId="string-regexp-match" AttributeValue="read|subscribe|notify">
```

```
35              <ActionAttributeDesignator AttributeId="action-id"/>
36            </ActionMatch>
37          </Action>
38        </Actions>
39      </Target>
40      <Condition Function="time-greater">
41            <!-- Effect deny, wenn das aktuelle Datum hinter dem Ablaufdatum liegt -->
42        <Apply EnvironmentAttribute="current-time"/>
43        <AttributeSelector Path="//ResourceContent/creditCardExpiryDate"/>
44      </Condition>
45      <Obligations>
46        <Obligation Id="Log" FulfillOn="Deny">
47          <AttributeAssignment Id="text">
48            Abgelaufene Kreditkarte von folgendem Benutzer nicht akzeptiert:
49            <AttributeSelector Path="//ResourceContent/username"/>
50          </AttributeAssignment>
51        </Obligation>
52      </Obligations>
53    </Rule>
54  </Policy>
```

Die Speicherung, Ermittlung und Zusammenführung der im Rahmen einer Anfrage relevanten AAPs erfolgt analog zu ARPs über einen XACML-PEP, dessen Schnittstellen nach außen in Abschnitt 4.4.8 beschrieben wurden.

Ebenfalls analog zu ARPs wird der XACML-PDP für jedes Attribut einzeln angestoßen. Sofern auf die Vollständigkeit des gelieferten Benutzerprofils geachtet werden muss, sollte eine geeignet hochpriorisierte Policy anhand des XACML-`ResourceContent` überprüfen, ob alle benötigten Attribute vorhanden sind. Um fehlende Attribute an den XACML-PEP zu kommunizieren, kann die Obligation *Missing-Attributes* verwendet werden, die eine Liste der zusätzlich benötigten und somit vom SP noch anzufordernden Attribute enthält.

An die aufrufende FIM-Komponente werden entsprechend drei Listen der akzeptierten, zurückgewiesenen und noch einzuholenden Attribute als Ergebnis zurückgeliefert (vgl. Abschnitt 4.4.7).

Bereits existierende Shibboleth-AAPs können ebenso wie Shibboleth-ARPs mit Hilfe eines XSLT-Stylesheets in XACML konvertiert werden (vgl. Abschnitt 5.3.4.2).

5.5. Föderierte Datensynchronisation mittels Notifications-Konnektors

In organisationsinternen Identity & Access Management Systemen ist die *zeitnahe* Synchronisation der Identitätsdatenbestände eine explizite und inzwischen selbstverständliche Aufgabe, die Fehler durch Inkonsistenzen verhindert. Mit der Einführung der ersten FIM-Ansätze wurde dieses Ziel für den organisationsübergreifenden Fall jedoch aufgegeben, da ein Abruf der Identitätsdaten durch den Service Provider jeweils nur während der Nutzung des Dienstes möglich war.

Hommel und Reiser haben dieses Defizit in [HoRe05b] erläutert und die Untersuchung der aus dem Umfeld verteilter Datenbanken bekannten Methoden zu Cache-Invalidierung bzw. -Updates angekündigt. Im Rahmen von ID-WSF 2.0 wurde von der Liberty Alliance im Jahr 2006 mit der *Subscriptions & Notifications* Spezifikation [LASUBS] der Grundstein für ein Push-Verfahren gelegt, mit dem beispielsweise Identity Provider als *Notifications* bezeichnete Nachrichten an Service Provider übermitteln können, um diesen die neuen Werte von Benutzerattributen mitteilen zu können. Da dies genau dem angestrebten Verfahren für Cache-

Updates entspricht, wurde im hier vorgestellten Architekturkonzept bereits Gebrauch von dieser Spezifikation der Liberty Alliance gemacht (siehe Abschnitte 4.4.1.1 und 4.4.7).

Da die Liberty Alliance jedoch wie bereits in Kapitel 3 dargelegt nicht auf das Zusammenspiel mit dem I&AM-System des Identity Providers eingeht und Aspekte wie Attribute Release Policies unberücksichtigt bleiben, werden nachfolgend der in Abschnitt 4.4.6 skizzierte Notifications-Konnektor und die durch ihn angestoßenen Datenflüsse genauer spezifiziert. Durch die Verteilung der einzelnen Verarbeitungsschritte auf mehrere Komponenten, die entsprechende Funktionalität bereits aufweisen, und die Integration der Liberty Subscriptions & Notifications wird dabei ein kompakter und klar strukturierter Workflow erreicht.

Im folgenden Abschnitt 5.5.1 wird die interne Funktionsweise des Notifications-Konnektors näher erläutert. Die für Notifications spezifischen Aufgaben der IDP- und SP-Software werden anschließend in Abschnitt 5.5.2 spezifiziert.

5.5.1. Interne Funktionsweise des Notifications-Konnektors

Wie im Architekturkonzept erläutert verbindet die als Notifications-Konnektor bezeichnete FIM-Komponente das lokale Identity Repository eines Identity Providers bzw. einer Attribute Authority mit der IDP-Software. Entsprechend der in Abschnitt 2.1.1.3 erläuterten Kategorisierung handelt es sich dabei um einen eventorientierten, unidirektionalen Push-Konnektor.

Der Notifications-Konnektor wird dabei wie die anderen Konnektoren des lokalen I&AM-Systems über die folgenden Arten von Änderungen im Identity Repository informiert:

- **Add-Event**: Anlegen neuer Identitätsobjekte im Repository.
- **Modify-Event**: An bestehenden Identitätsobjekten werden Attribute hinzugefügt, verändert oder gelöscht.
- **Delete-Event**: Ein Identitätsobjekt wird aus dem Repository gelöscht.
- **Rename-Event**: Ein Identitätsobjekt wird im Directory Information Tree des LDAP-Servers an eine andere Stelle verschoben.

Für den Notifications-Konnektor sind Add-Events irrelevant, da für lokal neu eingetragene Identitäten noch keine Subscriptions von SPs vorliegen können; ebenso können Rename-Events ignoriert werden, da über FIM generell nur die Attribute der Identitätsobjekte, aber nicht deren quellsystemseitige Objektidentifikatoren übertragen werden.

Der wichtigste zu bearbeitende Eventtyp ist somit der Modify-Event; ein Delete-Event kann vom Notifications-Konnektor analog zu einem Modify-Event, bei dem sämtliche Attribute inklusive des Benutzernamens gelöscht werden, bearbeitet werden.

Die einzige und triviale Aufgabe des Notifications-Konnektors ist es, aus dem von der Änderung betroffenen Objekt den Benutzernamen zu extrahieren und zusammen mit einer Liste der betroffenen Attribute an die IDP-Software zu übermitteln, die hierzu einen entfernten Methodenaufruf auf Basis von Web Services anbietet (siehe Abschnitt 4.4.1.3).

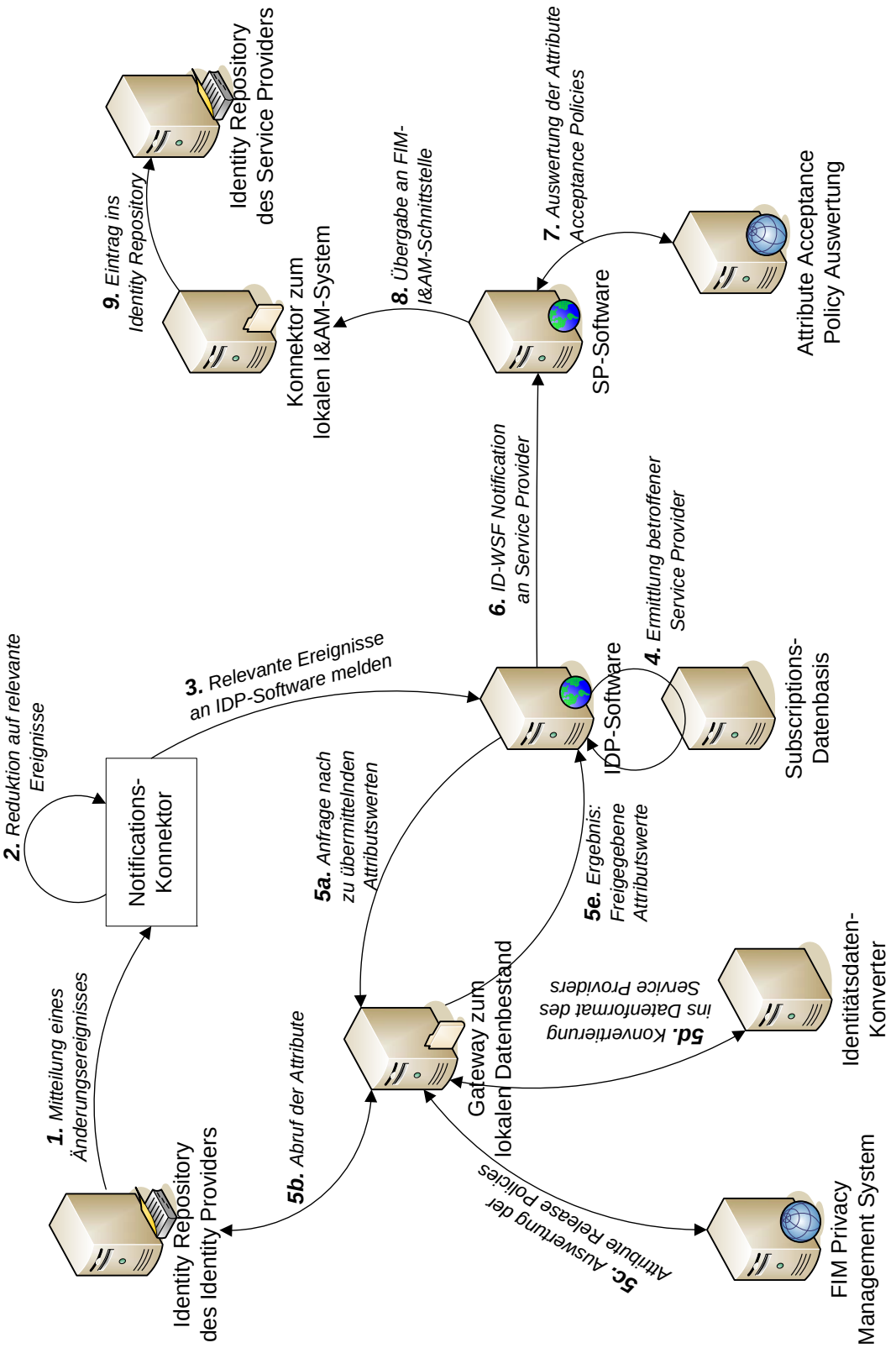


Abbildung 5.14.: Exemplarischer Workflow beim Einsatz des Notifications-Konnektors

5.5.2. Notifications-Workflow in der IDP- und SP-Software

Wie in Abschnitt 4.4.1.1 erläutert wurde, pflegt die IDP-Software alle ihr bekannten *Subscriptions* in einer Datenbasis, in der jeweils das Tripel (Service Provider, Benutzer, Attribut) festgehalten wird. Anhand der vom Notifications-Konnektor übergebenen Attributliste kann somit die Menge der zu benachrichtigenden Service Provider sehr einfach ermittelt werden.

Für jeden Service Provider werden anschließend die aktuellen Werte für die relevanten Attribute analog zu über FIM eingehenden Anfragen nach Attributsauskünften über den Gateway zum IDP-lokalen Datenbestand eingeholt. Dieser Schritt ist gegenüber der Alternative, dass der Notifications-Konnektor die aktuellen Attributswerte mitliefert, vorzuziehen, da die Gatewaykomponente wie in Abschnitt 4.4.3 beschrieben den Identitätsdatenkonverter und die Auswertung der Attribute Release Policies berücksichtigt, so dass diese beiden Bestandteile nicht redundant im Notifications-Konnektor realisiert werden müssen. Es ist insbesondere zu berücksichtigen, dass sich die Attribute Release Policies seit dem Eingang der Subscription verändert haben können, so dass ein früher freigegebenes Attribut eventuell inzwischen nicht mehr an den Service Provider übermittelt werden darf.

Für jedes freigegebene Attribut ist anschließend eine `Notification` gemäß [LASUBS, Kap. 5] zu erstellen; im folgenden Beispiel wird die Änderung der Kreditkartennummer des Benutzers Anton kommuniziert:

```
<Notify>
  <Notification subscriptionID="idp.example.com-subscr-123456">
    <ItemData>
      <User id="Anton">
        <Attribute id="creditCardNumber">
          1234567887654321
        </Attribute>
      </User>
    </ItemData>
  </Notification>
</Notify>
```

Bei gelöschten Attributen sieht die Spezifikation vor, dass im `Notification`-Element die Attribute `expires` mit einem aktuellen Zeitstempel sowie `endReason` mit dem Wert `urn:liberty:subs:endreason:resourcedeleted` übergeben werden müssen.

Analog zur Übermittlung von Attributsauskünften im Push-Verfahren wird die Nachricht anschließend auf Basis der in den Föderationsmetadaten enthaltenen Informationen an den zuständigen Service Provider geschickt (vgl. Abschnitt 4.4.1.1); sofern dieser temporär unerreichbar ist, werden regelmäßig erneute Zustellversuche unternommen, bis die Notification erfolgreich versendet werden kann oder der SP aus den Föderationsmetadaten entfernt wurde.

Das Eingehen von Notifications stellt SP-seitig eine der Standardoperationen der SP-Software dar (siehe Abschnitt 4.4.7). Die neuen Attributswerte durchlaufen den Identitätsdatenkonverter, der nur aktiv wird, falls die Daten nicht bereits vom IDP ins lokal benötigte Format konvertiert wurden. Anschließend wird eine Überprüfung auf Basis der der Attribute Acceptance Policies durchgeführt, wobei als Zugriffsart *notify* verwendet wird (siehe Abschnitt 5.4.3). Schließlich wird neue Wert des Attributs über den Konnektor zum SP-seitigen I&AM-System ins Identity Repository eingetragen bzw. dort analog zum Identity Provider gelöscht.

Abbildung 5.14 zeigt eine Zusammenfassung des gesamten Workflows für den Fall, dass die Konvertierung der Identitätsdaten bereits IDP-seitig erfolgt.

5.6. Bewertung auf Basis des Kriterienkatalogs

Dieses Kapitel abschließend wird nachfolgend zusammengefasst, wie die hier spezifizierten FIM-Komponenten zur Erfüllung der in Kapitel 2 erörterten Anforderungen beitragen.

Die *essentielle* Anforderung [DSA-ARPs] zielt auf eine policybasierte Steuerung der Flüsse personenbezogener Daten zwischen Identity Providern bzw. Attribute Authorities und Service Providern ab. In Kapitel 3 wurde sie für die Liberty Alliance und Shibboleth als jeweils partiell erfüllt gewertet, da in diesen beiden FIM-Lösungen konzeptionelle Ansätze bzw. eine grundlegende Implementierung enthalten sind.

Das in dieser Arbeit vorgestellte FIM Privacy Management System geht aufgrund seiner Konkretisierung und nahtlosen Integration in die Gesamtarchitektur klar erheblich über den aktuellen Stand der Liberty Alliance Spezifikationen hinaus; sowohl der Sprachumfang der XACML-Policies als auch die Flexibilität im Zusammenspiel mit den anderen FIM-Komponenten stellen darüber hinaus eine deutliche Differenzierung gegenüber dem aktuellen Stand von Shibboleth dar.

Die Anforderungen an die Ausdrucksfähigkeit von ARPs und ihre Modellierung in XACML wurden im Rahmen dieser Arbeit in mehrfachen Iterationen verfeinert, um aktuelle andere Arbeiten aus dem Umfeld des Privacy Managements und Anmerkungen zu eigenen Publikationen zu dieser Thematik zu berücksichtigen. Durch die Unterstützung von Obligationen und die Integration der Spezifikation von Verwendungszwecken in Anfragen wird ein Funktionsumfang definiert, der von den aktuellen FIM-Standards noch nicht erfüllt wird; aufgrund der erläuterten Notwendigkeit dieser Sprachelemente und ihrer Verbreitung im organisationsinternen Privacy Management ist mit Erweiterungen der FIM-Protokolle zu rechnen, die vom hier vorgestellten ARP-Konzept bereits berücksichtigt werden. Die Anforderung [DSA-ARPs] kann somit im Hinblick auf die heute in der Forschung bekannten Anforderungen als vollständig erfüllt betrachtet werden. Durch die Möglichkeit zur Zusammenstellung einer beliebigen Hierarchie aus benutzerspezifischen und z. B. föderations- und IDP-weiten ARPs wird auch die Anforderung [DSA-DefaultARPs] erfüllt; hierbei wurde auch erläutert, wie Policytransformationen zur Konvertierung des föderationsweiten in das lokale Datenschema genutzt werden können. Da die Policies auch zur Kontrolle von schreibenden Zugriffen verwendet werden können, wird zudem die Anforderung [DSA-Schreibzugriff] erfüllt, ohne dass hierfür weitere Komponenten notwendig werden.

Die *wichtige* Anforderung [FA-Schema] untermauert die Notwendigkeit, die für FIM verwendeten Identitätsdaten auf Absender- und Empfängerseite im jeweils benötigten Format bereitzustellen und dabei z. B. auf Mindestanforderungen bzgl. notwendiger Attribute pro Datensatz zu achten. Diese Teilanforderungen werden durch eine Kombination des Identitätsdatenkonverters mit den Attribute Acceptance Policies vollständig erfüllt: Der Identitätsdatenkonverter stellt ein flexibles Rahmenwerk für die aus Elementaroperationen zusammengesetzten Datenkonvertierungsregelsätze bereit; über die Attribute Acceptance Policies können darüber hinaus Qualitätsanforderungen an einzelne Attribute sowie die Vollständigkeit des Benutzerdatensatzes umgesetzt werden. Das Konzept des Federation Schema Correlation Services geht über die prinzipiellen technischen Aspekte der Schemakonvertierung dadurch hinaus, dass die Wiederverwendbarkeit von Konvertierungsregeln und deren Spezifikation durch Dritte unterstützt wird. Die Anforderung [FA-Schema] wird somit ebenfalls voll erfüllt.

Mit [FA-Updates] wird die zeitnahe Aktualisierung der SP-seitig gespeicherten Daten bei

IDP-seitig durchgeführten Änderungen verlangt. Der vom Notifications-Konnektor angestoßene Workflow zielt genau auf diese Anforderung ab, wobei wichtige Teilschritte wie die Identitätsdatenkonvertierung und die Berücksichtigung von Attribute Release und Acceptance Policies redundanzfrei integriert wurden; um eine möglichst große Interoperabilität mit den FIM-Standards und ihren erwarteten Erweiterungen zu erzielen, wird zur eigentlichen Datenübertragung auf die Formatspezifikation der Liberty Alliance – ID-WSF Subscriptions & Notifications – zurückgegriffen. Insbesondere wird auch das IDP-seitige Löschen von Benutzern an Service Provider kommuniziert, wodurch die Basis für das Erfüllen der Anforderung [SEC-Deprovisioning] geschaffen wird.

Die in diesem Kapitel vorgestellten FIM-Komponenten tragen darüber hinaus zur Erfüllung der folgenden *empfehlenswerten* Anforderungen bei:

- Das Konzept für die Attribute Release Policies unterstützt mehrere Identitäten und Rollen pro Benutzer (vgl. [FA-Identitätswahl]).
- Alle Komponenten unterstützen den Fall, dass der Benutzer den Dienst gerade nicht benutzt (vgl. [FA-UserOffline] und die in Kapitel 3 diskutierten Defizite bisheriger FIM-Ansätze).
- Durch geeignete Konfiguration der IDP-weiten Attribute Release Policies können die szenarienspezifischen Ausprägungen der Anforderungen [SEC-ARPs], [SEC-Benutzerkreis], [SEC-Trust] und [ORG-Trust] abgebildet werden.
- Die Anforderung [DSA-Obligationen] wird offensichtlich erfüllt; die in Attribute Release Policies zur Verfügung stehende Obligation zur Erzeugung von Protokolldateien trägt zum Erfüllen der Anforderung [DSA-Selbstbestimmung] bei.

Als Schnittstellen zu anderen Forschungsfragestellungen sind schließlich die in Abschnitt 5.3.3.3 skizzierten anonymisierenden Datentransformationen und die Möglichkeit, durch Obligationen in Attribute Acceptance Policies Genehmigungsprozesse anzustoßen, zu nennen (vgl. die noch nicht erfüllten Anforderungen [SEC-Genehmigung] und [DSA-Anonymisierung]).

Kapitel 6.

Prototypische Implementierung ausgewählter neuer FIM-Komponenten

Inhalt dieses Kapitels

In diesem Kapitel werden die prototypischen Implementierungen des Identitätsdatenkonverters und des XACML-basierten FIM Privacy Management Systems vorgestellt. Beide Komponenten haben die Eigenschaften, einerseits das in dieser Arbeit vorgestellte Architekturkonzept maßgeblich zu prägen und andererseits über bereits vorhandene Schnittstellen in die Open Source FIM-Software Shibboleth integriert werden zu können, ohne dass Anpassungen bei den anderen Föderationsteilnehmern notwendig werden.

Im nachfolgenden Abschnitt 6.1 wird die Motivation für die Wahl von Shibboleth als Implementierungsbasis skizziert; anschließend werden in Abschnitt 6.2 die Gründe erläutert, von den in den Architektur- und Werkzeugkonzepten vorgestellten Komponenten im Rahmen dieser Arbeit nur genau den Identitätsdatenkonverter und das FIM Privacy Management System implementiert zu haben.

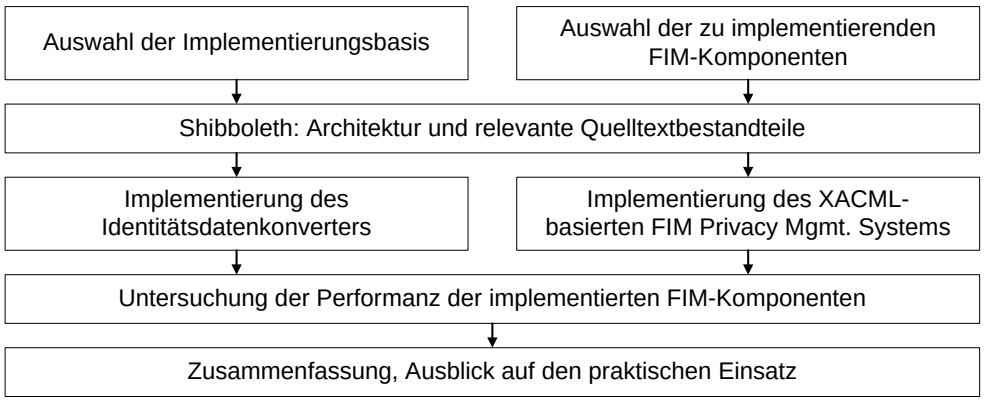


Abbildung 6.1.: Vorgehensmodell für dieses Kapitel

In Abschnitt 6.3 wird die Architektur von Shibboleth zusammengefasst, um eine Einordnung der implementierten Werkzeuge zu ermöglichen. Die Umsetzung dieser beiden neuen FIM-Komponenten wird in den Abschnitten 6.4 und 6.5 vorgestellt, wobei das XACML-basierte FIM Privacy Management System im Rahmen der Diplomarbeit von Matthias Ebert [Eber06] implementiert wurde, so dass hier lediglich die Ergebnisse vorgestellt werden.

Für beide Komponenten wurde eine rudimentäre Instrumentierung vorgenommen, um ihre Performanz beurteilen zu können, die für die praktische Nutzbarkeit mit entscheidend ist; die Ergebnisse exemplarischer Untersuchungen werden in Abschnitt 6.6 erläutert. Eine zusammenfassende Bewertung in Abschnitt 6.7 schließt das Kapitel ab, dessen Struktur in Abbildung 6.1 zusammengefasst ist.

6.1. Selektion der Implementierungsbasis

Bereits der Umfang der Spezifikationen von SAML, der Liberty Alliance und von WS-Federation sowie die in Kapitel 3 erwähnte Gegebenheit, dass selbst offiziell „standardkonforme“ Implementierungen verschiedener Hersteller längere Zeit nicht interoperabel waren, verdeutlichen, dass eigene Implementierungen nicht effizient von Grund auf neu erfolgen können, sondern auf bereits vorhandenen Programmen und Funktionsbibliotheken aufbauen sollten.

Aufgrund der zum Teil tiefgehenden Eingriffe in die Architektur SAML-basierter FIM-Lösungen (vgl. Abschnitt 4.2) ist es zudem offensichtlich, dass bestehende FIM-Komponenten modifiziert werden müssen, um von den neu eingeführten Werkzeugen Gebrauch machen zu können. Um darüber hinaus die Ergebnisse der Implementierung auch anderen zur Verfügung stellen zu können, wurde die Auswahl einer möglichen Implementierungsbasis von vornherein auf **Open Source Produkte** eingeschränkt, deren Lizenzbedingungen die notwendigen Modifikationen und deren Veröffentlichung zulassen.

In Abschnitt 3.4.1 wurden mit OpenSAML, den Ping Identity Toolkits und Lasso drei somit in Frage kommende Funktionsbibliotheken vorgestellt. Die Entscheidung, das auf OpenSAML basierende Shibboleth als Ausgangsbasis für eigene Implementierungen zu verwenden, wurde aus den folgenden Gründen getroffen:

- OpenSAML war bereits vor den beiden anderen Funktionsbibliotheken verfügbar. Hieraus lassen sich zwar keine Aussagen über Reife und Stabilität ableiten; dennoch ist der **Verbreitungsgrad von OpenSAML** höher und auch im Umfeld dieser Arbeit wurde entsprechendes Wissen frühzeitig aufgebaut.
- Im Unterschied zu den Ping Identity Toolkits werden mit OpenSAML/Shibboleth und Lasso/Authentic auch Open Source Implementierungen der auf den Funktionsbibliotheken aufbauende IDP-Softwarepakete angeboten, die einen einfacheren und realistischeren Test eigener Implementierungen in einem vollständigen Föderationskontext ermöglichen.
- Shibboleth stellt wie in Kapitel 3 erläutert den internationalen De-facto-Standard im Hochschulumfeld dar; dies zeigt sich auch darin, dass für die deutschlandweite Föderation, die derzeit vom DFN-Verein eingeführt wird (DFN-AAI), ebenfalls Shibboleth gewählt wurde. Eine Realisierung auf Basis von Shibboleth ermöglicht somit einen konkreten **praktischen Einsatz am Leibniz-Rechenzentrum**; darüber hinaus bietet es sich an, die erstellten Werkzeugprototypen in diesem Rahmen später weiterzuentwickeln. Die bisher am LRZ mit Shibboleth gesammelten Erfahrungen werden in Abschnitt 6.3.3 zusammengefasst.
- **Shibboleth** ist, obwohl die Identity Provider Software eine monolithische Web Applikation ist, quelltextseitig den Prinzipien objektorientierter Softwareentwicklung gemäß **stark modular aufgebaut**, so dass klar definierte Schnittstellen zur Verfügung stehen bzw. einzelne Module durch eigene Implementierungen ersetzt werden können, ohne andere Bestandteile modifizieren zu müssen.
- Über die Shibboleth-Supportinfrastruktur wird derzeit ein unkomplizierter und direkter Kontakt mit den Entwicklern der Software ermöglicht, durch den bei aufgetretenen Fragen und Problemen immer sehr rasch kompetente Lösungen gefunden werden konnten.

Während eine Implementierung somit prinzipiell auch für kommerzielle und andere frei verfügbare FIM-Softwarekomponenten möglich wäre, konzentrieren sich die nachfolgenden Ausführungen auf Shibboleth.

Darüber hinaus wurde bei den unten beschriebenen Implementierungen auch darauf geachtet, sie alleinstehend, d. h. **unabhängig von Shibboleth, lauffähig** zu halten; sie können somit auch z. B. als kommandozeilenbasierte Programme genutzt oder ggf. in andere FIM-Lösungen integriert werden. Die Motivation hierfür ist die Notwendigkeit, die Funktionalität der neuen FIM-Komponenten beispielsweise auch mit webbasierten Managementfrontends zu nutzen, um die korrekte Funktion von Konvertierungsregeln und Attribute Release Policies vor deren produktivem Einsatz überprüfen zu können.

6.2. Selektion der zu implementierenden FIM-Komponenten

Wie in Abbildung 4.4 auf Seite 170 dargestellt wurde, greift das in dieser Arbeit vorgestellte Architekturkonzept an vielen Stellen in die existierenden FIM-Lösungen ein, um die sich aus dem Anforderungskatalog ergebenden Fragestellungen zu lösen, ohne die existierenden und standardisierten Komponenten gänzlich zu verwerfen.

Eine vollständige Umsetzung aller vorgeschlagenen Änderungen war im Rahmen dieser Arbeit aufgrund des damit verbundenen Implementierungsaufwands nicht möglich und wäre auch nur sinnvoll, wenn das Ergebnis eine produktionsreife Lösung wäre, die auch von anderen genutzt und deren Nachhaltigkeit durch geeignete Supportmaßnahmen gewährleistet werden könnte.

Als Konsequenz wurde eine Priorisierung unter folgenden Aspekten vorgenommen:

- Die Implementierungen sollen als **Tragfähigkeitsnachweis** der hier vorgestellten Architektur- und Werkzeugkonzepte dienen und sich somit auf die in dieser Arbeit eingeführten **wesentlichen Neuerungen** konzentrieren.
- Änderungen, die auf eine Modifikation der Kernfunktionalität von IDP- und SP-Software abzielen, sollten vermieden werden, um eine **Inkompatibilität mit den offiziellen Versionen der Software zu vermeiden**.
- Die implementierten Komponenten sollen sinnvoll und **praktisch eingesetzt** werden können, **ohne** dass für ihre Nutzung ein **föderationsweites Deployment** erforderlich ist.

Von den fünf in Kapitel 5 spezifizierten FIM-Komponenten wurde deshalb der Notifications-Konnektor nicht umgesetzt, da SAML bzw. Shibboleth noch nicht auf Datenaktualisierungsnachrichten ausgelegt sind und somit ein Eingriff in IDP- und SP-Software notwendig wäre, der auch nur bei organisationsübergreifendem Deployment praktisch genutzt werden könnte.

Auch die Komponente zur Auswertung von Attribute Acceptance Policies wurde nicht implementiert, da sie wie in Abschnitt 5.4.2 beschrieben analog zum FIM Privacy Management System aufgebaut ist, das anhand des Kriterienkatalogs beurteilt eine wichtigere Komponente darstellt.

Neben dem **FIM Privacy Management System** wurde der **XSLT-basierte Identitätsdatenkonverter** implementiert, da seine Funktionalität essentiell für die im Architekturkonzept vorgesehene Schnittstelle zwischen FIM- und I&AM-Komponenten ist; er kann darüber hinaus sowohl IDP- als auch SP-seitig eingesetzt werden, wobei sich die realisierte Integration in Shibboleth auf den Identity Provider beschränkt.

Die Affinität zu IDP-seitigen Komponenten wurde auch dadurch motiviert, dass das Leibniz-Rechenzentrum vorerst primär die Rolle eines Identity Providers in der DFN-AAI Föderation wahrnehmen wird.

6.3. Die Architektur von Shibboleth und ihre Umsetzung

Shibboleth ist eine auf OpenSAML basierende, umfassende FIM-Lösung, die sowohl die IDP- als auch SP-seitigen Komponenten sowie einen als *Where Are You From?* (WAYF) bezeichneten IDP Discovery Service zur Verfügung stellt. Die nachfolgenden Ausführungen beziehen sich auf Shibboleth 1.3; der Termin für die Fertigstellung und Freigabe von Version 2.0 wurde bereits mehrfach verschoben und wird nicht vor Herbst 2007 erwartet. Die grundlegende Architektur wird zwar beibehalten werden, hinsichtlich des Quelltextes ist jedoch von größeren Änderungen auszugehen.

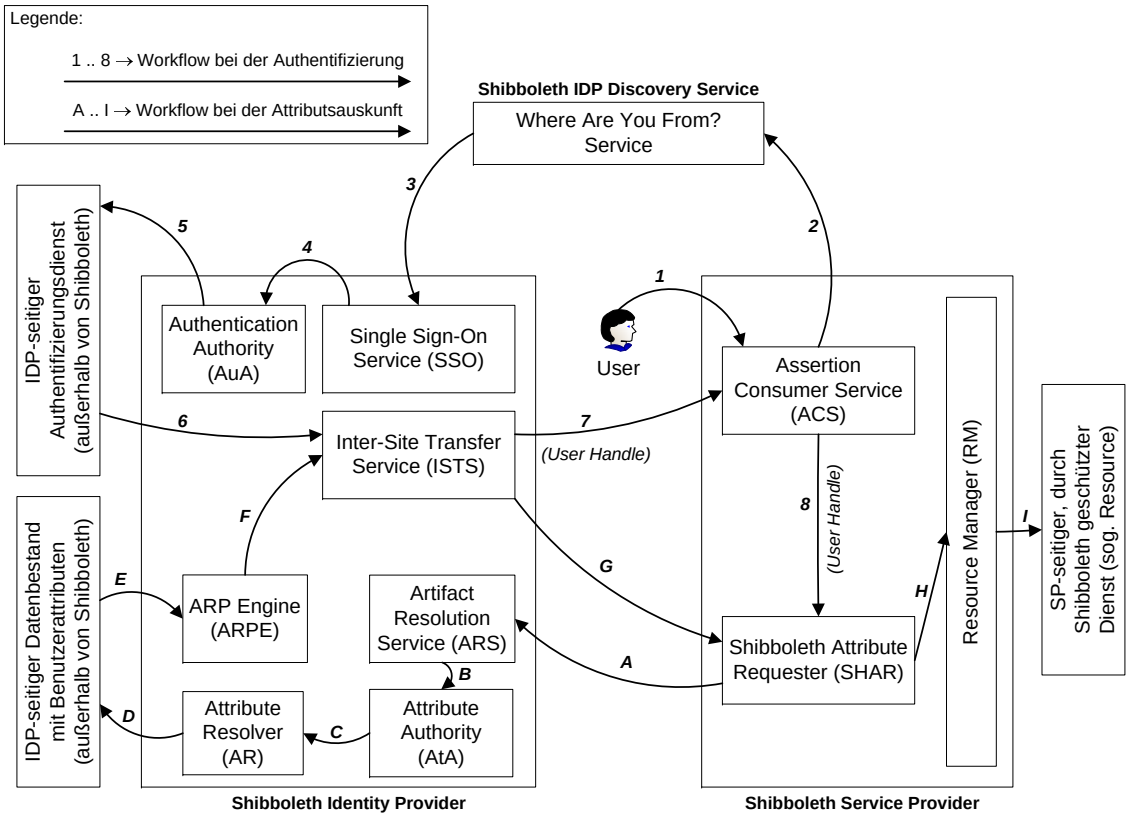


Abbildung 6.2.: Architektur und Workflows von Shibboleth 1.3

Im nachfolgenden Abschnitt 6.3.1 wird ein knapper Überblick über die Bestandteile einer Shibboleth-Infrastruktur gegeben, um eine grundlegende Einordnung der im Rahmen dieser Arbeit implementierten Komponenten zu ermöglichen, da sich die Architektur von Shibboleth aus offensichtlichen Gründen nicht mit der in Kapitel 4 beschriebenen deckt. In Abschnitt 6.3.2 werden die hier relevanten Bestandteile des Shibboleth-Quelltextes vorgestellt. Schließlich werden in Abschnitt 6.3.3 die am LRZ verfügbaren Shibboleth-Installationen, die als Entwicklungs- und Testumgebung genutzt wurden, skizziert.

6.3.1. Komponenten einer Shibboleth-Infrastruktur

Der **Shibboleth Identity Provider**, der in früheren Versionen als Shibboleth Origin bezeichnet wurde, ist eine in Java implementierte Webapplikation, die in einem so genannten Servlet-Container wie Apache Tomcat ausgeführt werden muss. Der Shibboleth IDP bietet im Wesentlichen die folgenden Schnittstellen zur Kommunikation mit den anderen Föderationsteilnehmern und den Benutzern an, die auch in Abbildung 6.2 dargestellt sind:

1. Der **Single Sign-On Service** (SSO) wird angestoßen, wenn ein Benutzer von einem Service Provider oder dem IDP Discovery Service an seinen Identity Provider umgeleitet wird. Die eigentliche Authentifizierung des Benutzers muss in Shibboleth 1.3 von

einer externen Softwarekomponente durchgeführt werden; in Shibboleth 2.0 wird eine dedizierte Authentifizierungsbenutzeroberfläche integriert sein. Aus historischen Gründen wird dieser Dienst oft auch als Handle Service bezeichnet, da er implizit für die Ermittlung des als *User Handle* bezeichneten Benutzeridentifikators zuständig ist.

2. Der **Inter-Site Transfer Service** (ISTS) dient bei der über den Benutzerclient mittelbaren Kommunikation zur Erzeugung von SAML Assertions und der HTTP-Redirect-basierten Weiterleitung des Benutzers an den entsprechenden Service Provider. Im Vergleich mit dem Architekturkonzept dieser Arbeit kombiniert er somit Teile der IDP-Software mit der Schnittstelle zu den Föderationsmetadaten.

3. Authentifizierungsbestätigungen bzw. Attributsauskünfte werden von den als **Authentication Authority** (AuA) bzw. **Attribute Authority** (AtA) bezeichneten Shibboleth-Komponenten erteilt. Während der Single Sign-On Service die Schnittstelle zur Authentication Authority darstellt, wird die Schnittstelle zur Attribute Authority als **Artifact Resolution Service** (ARS) bezeichnet. Beide Aufgaben decken sich mit der in dieser Arbeit der IDP-Software zugeordneten Funktionalität.

   Hinsichtlich dieser Nomenklatur ist zu berücksichtigen, dass Shibboleth nur die FIM-Rollen Identity Provider und Service Provider kennt, wohingegen noch keine eigenständigen Attribute Authorities unterstützt werden. Zur Vermeidung des Namenskonfliktes wird die Shibboleth Attribute Authority zukünftig als Attribute Query Protocol Handler bezeichnet werden.

Im Rahmen der Implementierung der neuen FIM-Komponenten ist primär die Shibboleth Attribute Authority relevant; sie koordiniert insbesondere die Abläufe in beiden folgenden weiteren IDP-Komponenten:

- Der so genannte **Attribute Resolver** (AR) dient der Ermittlung der Werte von Benutzerattributen aus externen Datenquellen. Shibboleth 1.3 bietet hierfür Möglichkeiten zum Zugriff auf Textdateien, relationale Datenbanken und LDAP-Server an. Zur Laufzeit können dynamisch neue Attribute angelegt werden, die mit konstanten Werten oder mit einem Wert eines anderen Attributs belegt werden können; diese Vorgehensweise wird beispielsweise benötigt, um ein Attribut durch Umkopieren seines Wertes in ein anderes Attribut umzubenennen (Attribute Mapping, vgl. Basisfunktionalitäten des Identitätsdatenkonverters in Abschnitt 5.2.1.2).

- Die vom Attribute Resolver ermittelten Attributswerte werden an die **ARP Engine** (ARPE) übergeben, von der die bereits in den Kapiteln 3 und 5 diskutierten Shibboleth Attribute Release Policies ausgewertet werden.

Der **Shibboleth Service Provider**, der früher als Shibboleth Target bezeichnet wurde, ist in Version 1.3 in der Programmiersprache C implementiert und soll mit Shibboleth 2.0 durch eine Java-Implementierung abgelöst werden. Es handelt sich um einen Hintergrundprozess (so genannter *Dämon* unter UNIX/Linux bzw. *Dienst* unter Windows), der Anfragen von Shibboleth-fähigen Webapplikationen entgegennimmt; für die weit verbreiteten Webserver-Softwarepakete Apache und Microsoft IIS wurden Plug-ins erstellt, mit denen herkömmliche Webanwendungen mit minimalem Aufwand Shibboleth-fähig gemacht werden können.

Der Shibboleth SP besteht aus den folgenden Komponenten:

Abbildung 6.3.: WAYF-Service der AAR-Testföderation (siehe auch Abschnitt 6.3.3)

1. Der **Assertion Consumer Service** (ACS) wird aufgerufen, wenn der Dienst den Shibboleth-SP mit der Authentifizierung des Benutzers beauftragt; er leitet den Benutzer zu diesem Zweck an den WAYF-Service bzw. bei einem bilateralen Deployment an einen fest vorkonfigurierten Identity Provider weiter und nimmt dessen Ergebnis in Form des *User Handles* entgegen. Aus historischen Gründen wird diese Komponente auch als SHIRE (Shibboleth Indexical Reference Establisher) bezeichnet.

2. Der **Shibboleth Attribute Requester** (SHAR) stellt Anfragen nach Benutzerattributen an den Identity Provider und wertet diese anhand der bereits erwähnten Shibboleth Attribute Acceptance Policies aus. Die zugelassenen Attribute werden anschließend dem **Resource Manager** übergeben, der sie dem als *Resource* bezeichneten Dienst zur Verfügung stellt.

Der als **Where Are You From?** (WAYF) Service bezeichnete IDP Discovery Service ist wie der Shibboleth IDP eine in Java implementierte Webapplikation, die mit Hilfe eines Servlet-Containers ausgeführt wird. Er dient wie in Abbildung 6.3 dargestellt der interaktiven Auswahl des für ihn zuständigen IDPs durch den Benutzer; über ein Cookie kann die Wahl optional clientseitig gespeichert werden, so dass die manuelle Interaktion bei zukünftigen Anfragen entfällt.

Die Vielzahl der zu konfigurierenden Komponenten, in denen zum Teil noch deren erwähnte historische Namen verwendet werden müssen, führt dazu, dass derzeit bereits die Inbetriebnahme von Shibboleth eine nicht triviale Aufgabe ist; Shibboleth 2.0 wird sich deshalb stärker an der Terminologie von SAML 2.0 und der Liberty Alliance orientieren und die Umbenennungen auch im Quelltext konsequent vollziehen.

6.3.2. Relevante Bestandteile des Shibboleth-Quelltextes

Da die in diesem Kapitel vorgestellten Neuentwicklungen nur Identity Provider, aber nicht Service Provider betreffen, wird im Folgenden lediglich auf den in Java implementierten Shibboleth IDP in Version 1.3 eingegangen.

Der Shibboleth IDP greift auf eine Reihe externer Funktionsbibliotheken, beispielsweise für kryptographische Operationen, Protokollierung und XML-Verarbeitung, zurück, die hier nicht betrachtet werden müssen. Der Shibboleth IDP selbst besteht aus rund 200 Java-Quelldateien mit mehr als 30.000 Lines of Code und überwiegend nur spärlichen Codeannotationen. Die Orientierung im Quelltext wird jedoch durch die Gruppierung von Quelltextdateien in Java-Packages und die Verwendung aussagekräftiger Klassen-, Methoden- und Variablennamen deutlich erleichtert. Die folgende Aufzählung gibt einen Überblick über ausgewählte Bestandteile der Java-Package-Struktur, die sich als für die in den Abschnitten 6.4 und 6.5 beschriebenen neuen Komponenten relevant erwiesen haben:[1]

- Das Package `shibboleth.idp` bildet den Kern der Software, dessen Java-Klassen vom Einlesen und Auswerten der Konfigurationsdateien über die Instanziierung der verwendeten ARP Engine bis hin zur Beantwortung eingehender Anfragen zuständig sind. Die Bearbeitung der SAML-basierten Authentifizierungs- und Attributsanfragen findet dabei im Package `shibboleth.idp.provider` statt.
- Die Bereitstellung der Föderationsmetadaten wird vom Package `shibboleth.metadata` übernommen, in dem lediglich Java-Interfaces und somit nicht instanziierbare abstrakte Klassen definiert werden, die das interne Föderationsmetadatenmodell repräsentieren. Im Package `shibboleth.metadata.provider` wird ein darauf aufbauender Parser für die von Shibboleth verwendeten, XML-dateibasierten Föderationsmetadaten implementiert (siehe Abschnitt 3.3.1).
- In den Packages `shibboleth.common`, `shibboleth.utils` und `shibboleth.xml` werden unter anderem Shibboleth-spezifische Hilfsmittel für den Umgang mit XML-Daten und das Schlüsselmanagement für kryptographische Operationen bereitgestellt; als zentrale Schnittstelle zur Ausgabe von Protokolldateieinträgen fungiert das Package `shibboleth.log`.
- Im Package `shibboleth.aa` wird das interne Datenmodell für angefragte Benutzerattribute definiert. Das Package `shibboleth.aa.attrresolv` umfasst Schnittstellendefinitionen zu den Shibboleth Attribute Resolvern, die im Package `shibboleth.aa.attrresolv.provider` wie erläutert z. B. für relationale Datenbanken und LDAP-Server implementiert sind.

  Das Package `shibboleth.aa.arp` beinhaltet analog dazu die interne Repräsentation von Attribute Release Policies; der von den Shibboleth ARPs zur Verfügung gestellte Sprachumfang wird im Package `shiboleth.aa.arp.provider` realisiert.

Für die Umsetzung des Identitätsdatenkonverters und der XACML-basierten ARPs sind insbesondere die Packages `shibboleth.aa.*` relevant; die von den anderen Packages bereitge-

[1] Der Name jedes Java-Packages trägt das Präfix `edu.internet2.middleware`, auf dessen wiederholte Nennung zur Verbesserung der Übersichtlichkeit verzichtet wurde.

stellte Funktionalität ermöglicht eine nahtlose Integration, z. B. hinsichtlich der Verwendung von Shibboleth-Konfigurations- und Protokolldateien für eigene Erweiterungen.

6.3.3. Shibboleth-Installationen am Leibniz-Rechenzentrum

Am LRZ wurde seit 2004 eine Reihe von Shibboleth-Testumgebungen aufgebaut, die für verschiedene studentische Arbeiten, für den Aufbau entsprechenden Fachwissens für den späteren Betrieb einer Shibboleth-Infrastruktur und im Rahmen dieser Arbeit als Entwicklungsumgebungen genutzt wurden:

- In einem Informatik-Fortgeschrittenenpraktikum wurde Shibboleth für eine **prototypische Single Sign-On Lösung für das Münchner Wissenschaftsnetz** (MWN) eingesetzt (siehe [EbZu05]). Dabei wurden die beiden Münchner Universitäten als Identity Provider sowie LMU, LRZ und TUM als Service Provider modelliert und einfache Dienste wie der hochschulübergreifende Zugriff durch Studenten auf Lehrmaterialien mit Einschränkungen nach Heimathochschule und Studiengang realisiert. Das LRZ fungiert in diesem Szenario auch als Föderationsverwaltung und betreibt den IDP Discovery Service.

- Im Rahmen einer Diplomarbeit, auf die in Abschnitt 6.5 noch näher eingegangen wird, wurde 2006 ein **bilaterales Shibboleth-Deployment** mit jeweils einem IDP und SP aufgebaut (vgl. Architekturmuster 5 in Abschnitt 4.9), um beim umfassenden Testen eigener Entwicklungen insbesondere die Latenzzeiten durch Einsatz eines IDP Discovery Services zu vermeiden.

- Internet2 bietet eine Shibboleth-Testföderation namens **InQueue** an, um neue Shibboleth-Nutzer bei der Installation und Konfiguration der Software zu unterstützen; beispielsweise können Organisationen, die lediglich als Identity Provider fungieren, das Zusammenspiel mit vorgegebenen Service Providern überprüfen. Das LRZ ist daran seit 2005 mit je einem Identity Provider und Service Provider, die mit Testdatensätzen und -diensten konfiguriert wurden, beteiligt.

- Das vom BMBF im Rahmen von *vascoda* geförderte und von der Universitätsbibliothek Freiburg geleitete Projekt **AAR**[2] stellt mit über 50 Teilnehmern die erste großflächige Shibboleth-Installation in Deutschland dar und fokussiert auf Hochschulbibliotheken. Da die DFN-AAI Föderation maßgeblich von diesem Projekt angeregt wurde, hat das LRZ die AAR-Testumgebung ebenfalls mit jeweils einem Identity Provider und Service Provider mitgenutzt.

- Seit Ende 2006 konkretisieren sich die Pläne für die vom Deutschen Forschungsnetz betriebene Föderation **DFN-AAI**; am LRZ wird an einem Identity Provider für die TUM gearbeitet, der nach Klärung der organisatorischen Aspekte mit dem DFN-Verein zügig produktiv eingesetzt werden soll.

Die nachfolgend erläuterten Implementierungsarbeiten wurden größtenteils in den ersten beiden Testumgebungen durchgeführt, um eine Unabhängigkeit von anderen Föderationsteil-

[2] AAR = Authentifizierung, Autorisierung und Rechteverwaltung; siehe `http://aar.vascoda.de/`.

nehmern zu erreichen und dennoch realistische Tests mit IDPs und SPs aus verschiedenen Domänen durchführen zu können.

6.4. XSLT-basierter Identitätsdatenkonverter für Shibboleth

Nachfolgend wird die prototypische Implementierung des Identitätsdatenkonverters für den Shibboleth-IDP erläutert. Hierzu werden zuerst die bei der Realisierung gegenüber dem in Kapitel 5 spezifizierten Werkzeugkonzept in Kauf genommenen Einschränkungen erläutert; anschließend werden in Abschnitt 6.4.2 die wesentlichen Elemente der Java-basierten Implementierung und in Abschnitt 6.4.3 die Integration in den Shibboleth-IDP beschrieben.

6.4.1. Konzeptionelle Anpassungen an das Shibboleth-Umfeld

Um bei der Implementierung des in Abschnitt 5.2 spezifizierten Identitätsdatenkonverters das Fehlen des Federation Schema Correlation Services zu kompensieren, wurde zur Veranschaulichung des Konzeptes ein zweistufiges Vorgehen bei der Realisierung des Repository für die Konvertierungsregelsätze gewählt:

- Beim Identity Provider wird ein OpenLDAP-basierter Verzeichnisdienst zur Speicherung aller Regelsätze verwendet, der gemäß Abbildung 5.5 auf Seite 300 aufgebaut ist. Aufgrund der IDP-lokalen Speicherung des Datenbestands wird diese Form der Datenspeicherung im Vergleich zum FSCS zudem dadurch vereinfacht, dass auf eine Rechteverwaltung in Form von LDAP Access Control Lists verzichtet werden kann.
- Der Identitätsdatenkonverter liest diese Regelsätze bei seiner Instanziierung aus dem LDAP-Server aus und speichert sie analog zur Beschreibung des FSCS intern in einer Matrix (zweidimensionales Array of Arrays, vgl. Abschnitt 5.2.2.1).

Es ist ferner zu beachten, dass Shibboleth die Verwendung eines föderationsweiten Datenmodells erzwingt, da jedes potentiell zu übertragende Attribut in der statischen Shibboleth-Konfiguration definiert werden muss. Diese Einschränkung ist tief in der Shibboleth IDP-Implementierung verankert und würde ein umfassendes Redesign erforderlich machen. Für den Einsatz des Identitätsdatenkonverters ergeben sich somit folgende Einschränkungen:

- Seine Funktionalität kann in der Praxis lediglich für die Konvertierung zwischen dem lokalen und dem föderationsweiten Schema eingesetzt werden. Aufgrund der Verwendung von XSLT für Konvertierungsregeln führt dies zwar zu einer deutlich verbesserten Flexibilität gegenüber den bislang von Shibboleth gebotenen Möglichkeiten; es entfällt jedoch zwangsweise der Vorteil, dass sich nicht alle Föderationsteilnehmer auf ein gemeinsames Schema verständigen müssen.
- Die darüber hinausgehende Konvertierung von Attributswerten in SP-spezifische Schemata kann nur IDP-intern durch Ausgabe der Resultate in Protokolldateien, aber nicht im Zusammenspiel mit real vorhandenen Service Providern getestet und überprüft werden.

Zur Vereinfachung dieses Vorgangs und für umfassendere, von Shibboleth unabhängige Tests steht der Identitätsdatenkonverter parallel ferner als kommandozeilenorientiertes Programm zur Verfügung, das auch für die Performanzmessungen in Abschnitt 6.6 verwendet wurde.

6.4.2. Implementierung des Identitätsdatenkonverters in Java

Zur Implementierung wurde die Programmiersprache Java verwendet, da dies eine Voraussetzung für die nahtlose lokale Integration in Shibboleth ist. Analog zum Aufruf über die Kommandozeile könnte die Implementierung mit geringem Aufwand auch um das im Architekturkonzept vorgesehene Web Services Interface erweitert werden; im Kontext von Shibboleth besteht hierfür jedoch keine Notwendigkeit, so dass lediglich die zwangsweise performantere Variante mit lokalen Methodenaufrufen umgesetzt wurde.

Als XSLT-Prozessor wurde Xalan-Java 2.7.0 [XALAN] verwendet, der auf der XML-Parserimplementierung Xerces basiert; das Deployment wird insbesondere dadurch erleichtert, dass diese beiden Java-Funktionsbibliotheken bereits zusammen mit dem Shibboleth-IDP ausgeliefert werden, weil XSLT zur Konvertierung von Konfigurationsdateien bei neuen Shibboleth-Softwareversionen verwendet wird. Da Java mit JAXP (Java API for XML Processing) eine einheitliche Schnittstelle für die XML-Verarbeitung anbietet, können prinzipiell auch beliebige andere XSLT-Prozessoren eingesetzt werden.

Im Folgenden wird die interne Arbeitsweise der Implementierung des Identitätsdatenkonverters in Ergänzung zum in Abschnitt 5.2 spezifizierten Workflow skizziert.

Bei der Initialisierung wird zunächst der gesamte Bestand an Konvertierungsregelsätzen aus dem OpenLDAP-Server abgerufen, dessen Directory Information Tree (DIT) in Abbildung 6.4 dargestellt ist; hierfür wird die Java JNDI-API (Java Naming and Directory Interface) genutzt:

```
1  [...]
2
3  import java.util.Hashtable;
4  import javax.naming.*;
5  import javax.naming.directory.*;
6
7  [...]
8
9      Hashtable env = new Hashtable(11);
10     env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.LdapCtxFactory");
11     env.put(Context.PROVIDER_URL, "ldap://localhost:389/dc=com,dc=example,ou=FSCS");
12
13     DirContext ctx = new InitialDirContext(env);
14
15     // Alle Objekte der Klasse FSCSregelsatz aus Teilbaum ou=Regelsaetze
16     // auslesen; gesamten Teilbaum danach durchsuchen (Scope = Subtree):
17     NamingEnumeration ldapErgebnis = ctx.search("ou=Regelsaetze",
18                                                 "objectclass=FSCSregelsatz",
19                                                 SearchControls.SUBTREE_SCOPE);
20
21     while (ldapErgebnis.hasMoreElements()) {
22         String regelsatzID = ldapErgebnis.getName(); // Liefert DN des LDAP-Objekts
23         Attributes alle_attribute = ldapErgebnis.getAttributes();
24
25         Attribute attr_AnfrageK = alle_attribute.get("anfragekonvertierung");
26         Attribute attr_AntwortK = alle_attribute.get("antwortkonvertierung");
27         Attribute attr_version  = alle_attribute.get("metadata_version");
28         Attribute attr_expiry   = alle_attribute.get("metadata_expiry");
29
30         // Methode zum Anlegen der intern verwendeten Matrix aufrufen:
31         this.erzeugeCacheEintrag(regelsatzID, attr_AnfrageK.get().toString(),
32             attr_AntwortK.get().toString(), attr_version.get().toString(),
33             attr_expiry.get().toString());
34     }
35
36     ctx.close();
37
38 [...]
```

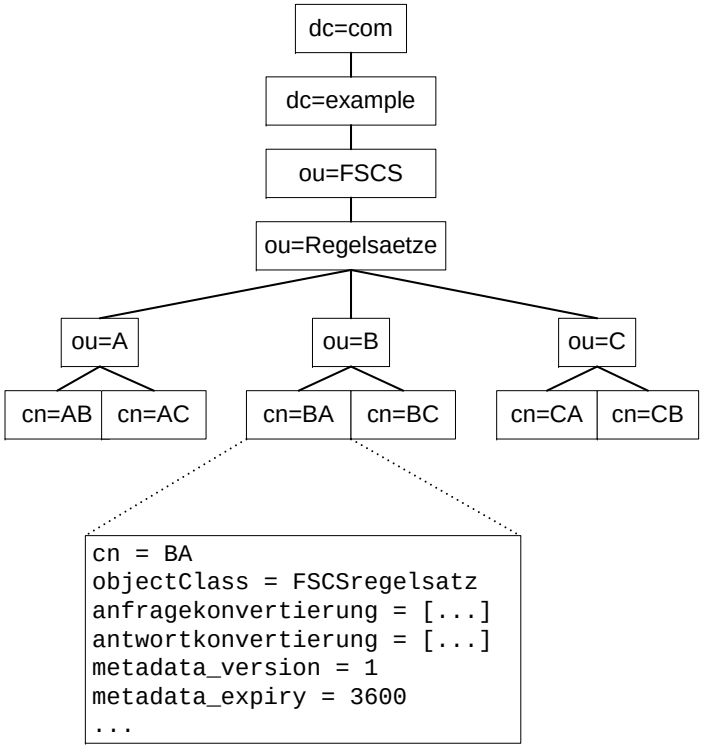


Abbildung 6.4.: LDAP-DIT bei der Implementierung des Identitätsdatenkonverters

Die einzelnen XSLT Stylesheets zur Anfrage- und Antwortkonvertierung liegen somit intern wie vom LDAP-Server geliefert als Zeichenketten vor, die dem XSLT-Prozessor wie folgt übergeben werden:

```
1  [...]
2  import java.io.*;
3  import java.xml.transform.*;
4  import java.xml.transform.stream.*;
5  [...]
6
7  public String xsltAnwendung(String stylesheet, String eingabe) {
8      String ausgabe;
9
10     // Umwandeln der Strings in StreamSources:
11     Source xsltEingabe = new StreamSource(new StringReader(stylesheet));
12     Source xmlEingabe  = new StreamSource(new StringReader(eingabe));
13
14     // Erzeugen einer XSLT-Prozessorinstanz fuer dieses Stylesheet:
15     TransformerFactory tf = TransformerFactory.newInstance();
16     Transformer        t  = tf.newTransformer(xsltEingabe);
17
18     // Vorbereiten des internen Ergebnisformats des XSLT-Prozessors
19     StringWriter sw           = new StringWriter();
20     StreamResult xslt_ergebnis = new StreamResult(sw);
21
22     // Durchfuehren der Konvertierung
23     t.transform(xmlEingabe, xslt_ergebnis);
24
25     // Uebernehmen des Ergebnisses als Ausgabe:
26     ausgabe = sw.toString();
27     sw.close(); // StringWriter abschliessen
28
29     // Ergebnis zurueckliefern
30     return ausgabe;
31 }
```

In dieser prototypischen Implementierung wurde auf die in Abschnitt 5.2.3 vorgeschlagene Optimierung, mit präkompilierten XSLT-Stylesheets zu arbeiten, verzichtet; Ausgangspunkt hierfür wäre die Verwendung von Xalan-Templates nach folgendem Muster (vgl. Zeilen 14–16 oben):[3]

```
1 [...]
2     // Erzeugen eines XSLT-Templates fuer dieses Stylesheet:
3     TransformerFactory tf  = TransformerFactory.newInstance();
4     Templates          tpl = tf.newTemplates(xsltEingabe);
5
6     // Erzeugen einer XSLT-Prozessorinstanz aus dem Template:
7     Transformer        t   = tpl.newTransformer();
8 [...]
```

Der Aufwand zur Verwaltung der Templates, insbesondere das Ermitteln und Zerstören nicht mehr benötigter Objekte vor dem Hintergrund des Speicherbedarfs im Dauerbetrieb, und deren Integration in den Shibboleth-IDP wäre deutlich höher und könnte beispielsweise Bestandteil einer produktionsreifen Implementierung werden.

6.4.3. Integration in den Shibboleth-IDP

Die Integration in Shibboleth erfolgt an zwei Stellen, um einerseits die Namen von Attributen eingehender Anfragen und andererseits die Werte an den Service Provider zu übermittelnder Attribute konvertieren zu können.

Um die Namen der Attribute, die Shibboleth aus einem LDAP-Server abruft, zu konvertieren, wurde die Methode `resolve` der Klasse `JNDIDirectoryDataConnector` im Package `shibboleth.aa.attrresolv.provider` so modifiziert, dass das vom Identitätsdatenkonverter gelieferte Ergebnis die für die LDAP-Anfrage verwendeten `ReturningAttributes` in den JNDI `SearchControls` ersetzt (siehe Zeilen 8–19 und 24):

```
1  public Attributes resolve(Principal principal, String requester, String responder,
2      Dependencies depends) throws ResolutionPlugInException
3  {
4      InitialDirContext context = null;
5      NamingEnumeration nEnumeration = null;
6      String populatedSearch = searchFilter.replaceAll("%PRINCIPAL%", principal.getName());
7
8      SearchControls idkonv_controls = new SearchControls();
9      idkonv_controls = controls;     // Bestehendes SearchControls-Objekt als Ausgangsbasis
10
11     int max = idkonverter.getAnzahlAttribute();
12     String[] idkonv_returningAttributes = new String[max];
13
14     // Service Provider Id, Identity Provider Id und
15     // Name des angefraten Attributs an Konverter uebergeben
16     idkonv_returningAttributes = idkonverter.konvertiereAnfrage(
17                                  requester, responder, this.getName());
18
19     idkonv_controls.setReturningAttributes(idkonv_returningAttributes);
20
21     try {
22         try {
23             context = initConnection();
24             nEnumeration = context.search("", populatedSearch, idkonv_controls);
25     [...]
26 }
```

[3] Siehe auch `http://xml.apache.org/xalan-j/usagepatterns.html#multithreading`.

Zur Konvertierung der an den Service Provider zurückzuliefernden Attributswerte wurde die Methode `filterAttributes` der Klasse `ArpEngine` im Package `shibboleth.aa.arp` modifiziert; sie stellt die Schnittstelle dar, um von allen aus dem lokalen Datenbestand ermittelten Attributen und deren Werten genau die zurückzugebenden Werte zur ArrayList-Variable `releaseValues` hinzuzufügen. Das folgende Codefragment zeigt, wie dies mit dem Aufruf des Identitätsdatenkonverters verknüpft wurde (siehe Zeilen 10–13):

```
1  public void filterAttributes(ArpAttributeSet attributes, Principal principal,
2      String requester, URL resource) throws ArpProcessingException
3  {
4  [...]
5
6      ArrayList releaseValues = new ArrayList();
7      for (Iterator valueIterator = arpAttribute.getValues(); valueIterator.hasNext();) {
8          Object value = valueIterator.next();
9          if (attribute.isValuePermitted(value)) {
10             String idkonv_value = new String;
11             idkonv_value = idkonverter.konvertiereAntwort(
12                                 requester, responder, arpAttribute.getName(), value);
13             releaseValues.add(idkonv_value);
14         }
15     }
16
17 [...]
18 }
```

Durch das Einschleifen des neuen Codes an dieser Stelle wird auch ein reibungsloses Zusammenspiel mit der nachfolgend beschriebenen Implementierung der XACML-ARPs ermöglicht.

6.5. XACML-basierte Attribute Release Policies für Shibboleth

Das in Abschnitt 5.3 vorgestellte Konzept zur Verwendung von XACML als Policysprache für ARPs wurde im Rahmen der Diplomarbeit [Eber06] für Shibboleth 1.3 implementiert; in diesem Abschnitt werden die Ergebnisse der Diplomarbeit aus der Perspektive des in dieser Arbeit vorgestellten Architekturkonzepts zusammengefasst.

Zur nahtlosen Integration in Shibboleth und zur Anpassung der Komplexität an den Rahmen einer Diplomarbeit wurden die folgenden Vereinfachungen durchgeführt:

- Der Sprachumfang der Policies wurde wie folgt eingeschränkt:
  - Das Ergebnis einer Policyauswertung ist entweder *Permit* oder *Deny*; auf die Ergebnisart *Ask* wurde verzichtet, da Shibboleth derzeit keine Möglichkeit zur interaktiven Nachfrage bei Benutzern vorsieht, so dass ein unverhältnismäßig tiefgehender Eingriff in die Shibboleth-Architektur und die Implementierung entsprechender graphischer Benutzeroberflächen erforderlich gewesen wäre.
  - Der bei der Policyauswertung berücksichtigte Verwendungszweck einer Anfrage wird bei der Kommunikation zwischen Shibboleth SPs und IDPs nicht übermittelt und deshalb durch einen in einer Konfigurationsdatei vorgegebenen Wert eingespeist.
  - Als Zugriffsart auf Attribute wird nur *read* berücksichtigt, da die Operationen *subscribe* und *write* von Shibboleth nicht unterstützt werden.

- *Gruppenspezifische* ARPs werden nicht in einem eigenen Teilbaum des LDAP-basierten Policy Repository gespeichert (vgl. Abschnitt 5.3.3.1); die Unterscheidung zwischen *individuellen* und *allgemeinen* ARPs, die über LDAP-Attribute auf Teilmengen von Benutzern eingeschränkt werden können, reichte für die in der Diplomarbeit behandelten Szenarien aus.

- Es wurden lediglich IDP-seitige Obligationen realisiert, da Shibboleth die Integration von Obligationen in die an SPs zurückgelieferten Nachrichten nicht unterstützt, ohne dass durch eigene Anpassungen die Interoperabilität mit herkömmlichen Shibboleth-Instanzen gefährdet werden würde.

Zur Implementierung des ARP Repository wurde ein OpenLDAP-Server verwendet; als XACML Policy Decision Point kommt die Open Source Referenzimplementierung von Sun in Version 1.2 zum Einsatz (siehe [SUNXAC]). Der Shibboleth-interne Workflow verändert sich somit wie folgt:

- Ausgangspunkt für die XACML-ARP-Implementierung ist die Java-Methode `getReleaseAttributes` der Klasse `IDPProtocolSupport` im Package `shibboleth.idp`; ihr werden der Name des lokalen Benutzers, des Service Providers und des Dienstes übergeben. Die Aufgabe dieser Methode ist die Rückgabe aller Attribute des Benutzers und deren aktuelle Werte, die an den Service Provider ausgeliefert werden sollen; hierzu bedient sich der nachfolgend erläuterten Methoden.

- Über die Methode `listPossibleAttributes` der Klasse `ArpEngine` im Package `shibboleth.aa.arp` wird eine Liste aller über den Benutzer verfügbaren Attribute erstellt; die XACML-ARP-Implementierung orientiert sich dazu an der lokalen Schemadefinition des Identity Repository und nicht wie ursprünglich an der Liste der Attribute, für die herkömmliche Shibboleth-ARPs definiert worden sind.

  Die Werte aller so ermittelten Attribute werden über die bereits vorhandene Methode `resolveAttributes` der Klasse `AttributeResolver` im Package `shibboleth.aa.attrresolv` aus den entsprechend konfigurierten Datenquellen abgerufen.

- Kern der XACML-ARP-Implementierung ist die Neuentwicklung der Methode `filterAttributes` in der Klasse `ArpEngine` im Package `shibboleth.aa.arp`. Sie ersetzt die Shibboleth-interne ARP Engine durch eine Implementierung des in Abschnitt 5.3.3.2 beschriebenen XACML-PEPs, der die für die Anfrage relevanten XACML-ARPs aus dem Policy Repository abruft, sie anhand ihrer Priorität zu einem XACML `PolicySet` zusammenstellt und an eine Instanz des XACML-PDPs zur Entscheidung über die Freigabe jedes einzelnen Attributs übergibt.

  Als Ergebnis wird lediglich die von Shibboleth benötigte Liste der freigegebenen Attribute zurückgegeben, d. h. die im Werkzeugkonzept in Abschnitt 5.3.3.3 vorgesehene Gruppierung von Rückgabewerten entfällt.

In [Eber06] werden die Einzelschritte bei der Implementierung und der Integration des XACML-PDPs von Sun genauer beschrieben und Beispiel-ARPs für verschiedene Shibboleth-

spezifische Szenarien erläutert; die Implementierung wurde zudem in Form eines Quelltext-Patches veröffentlicht.[4]

Zum Testen der Implementierung und eigener ARPs kann das von Shibboleth bereits mitgelieferte kommandozeilenorientierte Werkzeug *resolvertest* verwendet werden: Es wird üblicherweise zur Überprüfung der korrekten Konfiguration der Anbindung an LDAP-Server bzw. relationale Datenbanken eingesetzt; optional bietet es jedoch die Möglichkeit, eine Anfrage durch einen frei wählbaren Service Provider zu simulieren, bei deren Auswertung auch die Shibboleth ARP Engine berücksichtigt wird.

Im Hinblick auf einen praktischen Einsatz stellt das Fehlen eines graphischen, intuitiv bedienbaren XACML-ARP Editors ein klares Defizit dar; es ist offensichtlich, dass das manuelle Erstellen von XACML Policies und deren direktes Einspielen in den LDAP-Server fehleranfällig, nicht effizient und insbesondere den Benutzern nicht zumutbar ist. Bei einer Weiterentwicklung muss deshalb auch die Schaffung graphischer Benutzeroberflächen im Vordergrund stehen.

6.6. Untersuchung der Performanz

In Kapitel 2 wurde die für die Akzeptanz von FIM durch Benutzer *wichtige* Anforderung [NFA-Performanz] diskutiert; dadurch, dass in den Datenfluss einer FIM-Transaktion zusätzlich der Identitätsdatenkonverter und das FIM Privacy Management System eingeschleust wurden, erhöht sich IDP-seitig zwangsweise die interne Verarbeitungszeit bei der Beantwortung von FIM-Anfragen.

Insbesondere bei der über den Benutzerclient mittelbaren FIM-Kommunikation ist deshalb zu untersuchen, ob sich durch die neuen FIM-Komponenten spürbare Verzögerungen ergeben, die gegen einen praktischen Einsatz sprechen würden. Im nachfolgenden Abschnitt 6.6.1 werden die auf die Verarbeitungszeit Einfluss nehmenden Randbedingungen erläutert. In Abschnitt 6.6.2 wird anschließend das Szenario vorgestellt, das zur Durchführung der Performanzmessungen herangezogen wurde; die Ergebnisse der Messreihen werden in Abschnitt 6.6.3 diskutiert.

6.6.1. Einflüsse auf die Verarbeitungszeit in den neuen FIM-Komponenten

Für die Benutzerakzeptanz ist insbesondere die **absolute Verarbeitungszeit** ausschlaggebend, da zu lange systembedingte Verzögerungen zwischen den Interaktionsschritten die subjektive Nutzbarkeit von Diensten stark beeinträchtigen. Die sich durch die Verarbeitungszeit in den beiden neuen FIM-Komponenten ergebende Verzögerung ist von einer Vielzahl von Faktoren abhängig, zu denen insbesondere die folgenden gehören:

- Die Leistungsfähigkeit und Dimensionierung der eingesetzten Hardware hat insbesondere im Hinblick auf CPUs bzw. **Prozessorkerne** und **Arbeitsspeicher** einen großen und direkten Einfluss auf die Verarbeitungsgeschwindigkeit und Skalierbarkeit.

[4] Siehe `https://spaces.internet2.edu/display/SHIB/ShibXACML`.

- Die Anzahl der vom Identity Provider verwalteten **Benutzer** beeinflusst die Dauer von Lesezugriffen auf das Identity Repository; durch den Einsatz von Indizes kann jedoch sowohl bei relationalen Datenbanken als auch bei LDAP-Servern eine sehr gute Skalierbarkeit erzielt werden.
- Die **Anzahl der parallel eingehenden Anfragen** wirkt sich auf die Auslastung des Systems aus, insbesondere wenn sie die Anzahl der verfügbaren Prozessorkerne deutlich übersteigt. Hierbei ist zu berücksichtigen, dass
  - die beiden zu beurteilenden FIM-Komponenten aufgrund der Policy- und XML-Verarbeitung primär Prozessor- und Speicherressourcen beanspruchen, so dass der Hintergrundspeicher- und Netzwerk-I/O-Durchsatz vernachlässigt werden kann.
  - Aspekte wie das Scheduling durch das eingesetzte Betriebssystem sowie die Java Virtual Machines und die Multi-Threading-Fähigkeit der eingesetzten Funktionsbibliotheken aufgrund der Komplexität ihres Zusammenwirkens nicht näher analysiert wurden.
- Die **Anzahl** und die **Komplexität** der für eine Anfrage relevanten **Konvertierungsregeln** bzw. **Attribute Release Policies** haben ebenfalls direkte Auswirkungen auf die Verarbeitungszeit.

Aufgrund der somit vorliegenden Freiheitsgrade und fehlenden Metriken, beispielsweise für die Komplexität von XSLT-Stylesheets, wäre eine theoretische Komplexitätsanalyse im Rahmen dieser Arbeit nicht zielführend; vielmehr wurde eine rudimentäre **Instrumentierung** der neuen FIM-Komponenten vorgenommen, die eine **Messung ihrer Verarbeitungszeiten** im nachfolgend beschriebenen Szenario ermöglicht.

6.6.2. Szenario und Vorgehensweise für die Performanzmessungen

Zur Beurteilung der Performanz des Identitätsdatenkonverters und des FIM Privacy Management Systems wurde das folgende realitätsnahe Szenario herangezogen:

- Der Identity Provider verwaltet **50.000 Identitäten**; im Hinblick auf den Einsatz von Shibboleth im Rahmen der Föderation DFN-AAI soll dies als Beispiel für die Anzahl von Studenten und Mitarbeitern an größeren deutschen Hochschulen dienen.
- Alle simulierten Testanfragen umfassten den Abruf derselben **fünf Benutzerattribute** `displayName`, `telephoneNumber`, `mail`, `eduPersonScopedAffiliation` und `eduPersonEntitlement`, die im DFN-AAI-Schema vorgesehen sind. Dabei gelten die folgenden Randbedingungen:
  - Für die Konvertierung der Attributswerte werden bei jeder Anfrage dieselben **drei XSLT-Stylesheets** eingesetzt:
    - XSLT-Stylesheet A erzeugt das Attribut `displayName` durch Konkatenation aus den beiden lokalen Attributen `Vorname` und `Nachname`.
    - XSLT-Stylesheet B konvertiert die Telefonnummer des Benutzers aus dem lokalen Format *089/35831-7821* in das benötigte Format *+49 89 358317821*.

    - XSLT-Stylesheet C verwendet eine Abbildungstabelle für die zulässige Wertemenge und ergänzt den so genannten Scope im Attribut `eduPersonScopedAffiliation`, indem beispielsweise der Wert *Mitarbeiter* in *staff@example.com* konvertiert wird.

  Alle XSLT-Stylesheets liegen dabei bereits im Hauptspeicher des Identitätsdatenkonverters vor und müssen nicht erst aus dem LDAP-Server abgerufen werden (vgl. Abschnitt 6.4.1).

- Für die Anfragen sind jeweils drei von zehn *allgemeinen* und zwei von 1.000 *individuellen* Attribute Release Policies relevant. Die Anzahl der benutzerindividuellen ARPs wurde auf Basis von Erhebungen der Shibboleth-Entwickler gewählt, die gezeigt haben, dass bislang nur ein geringer Prozentsatz der Benutzer eigene ARPs definiert hat.[5] Diese **fünf ARPs** werden mittels einer einzigen LDAP-Anfrage aus dem Policy Repository abgerufen.

- Die beiden untersuchten FIM-Komponenten werden auf einer Servermaschine des LRZ vom Typ Sun Fire X4100 mit zwei Dual-Core AMD Opteron 285 Prozessoren und 8 Gigabyte Hauptspeicher betrieben. Als Betriebssystem ist SuSE Linux Enterprise (SLES) in Version 10 im Einsatz; als Java-Laufzeitumgebung steht das Sun JDK in Version 1.4.2 zur Verfügung.

- Das Identity Repository und das ARP Repository werden auf einer Maschine desselben Typs mit nur einem Dual-Core AMD Opteron 285 Prozessor und 2 Gigabyte Hauptspeicher ebenfalls unter SLES 10 betrieben. Als LDAP-Server wird OpenLDAP in Version 2.3.19 eingesetzt. Die Round Trip Time für IP-Pakete zwischen den beiden Maschinen beträgt 0,2 Millisekunden und wird nachfolgend nicht explizit berücksichtigt.

In diesem Szenario wurden zur Messung der Verarbeitungszeit und zur grundlegenden Beurteilung der Skalierbarkeit der implementierten FIM-Komponenten die folgenden drei Testreihen durchgeführt:

1. **Eine Anfrage** über einen Benutzer.
2. **Zehn parallele Anfragen** über zehn verschiedene Benutzer.
3. **50 parallele Anfragen** über 50 verschiedene Benutzer.

Diese Werte wurden ebenfalls auf Basis von Erfahrungsberichten anderer Shibboleth-Benutzer in produktiven Föderationen gewählt, bei denen schon derzeit Spitzenwerte mit bis zu 2.000 FIM-Transaktionen pro Minute auftreten.[6]

Jede Testreihe wurde 100 Mal wiederholt, um Störeinflüsse wie parallel auf den Servermaschinen laufende Softwareupdate- und Backupprozesse mittels Durchschnittsbildung berücksichtigen zu können; zwischen jeweils zwei Testläufen wurde dabei 30 Sekunden pausiert, um z. B.

[5] Dieses Phänomen ist einerseits auf das Fehlen entsprechender graphischer Benutzeroberflächen zur Konfiguration *individueller* ARPs und andererseits auf den in den aktuellen Shibboleth-Szenarien ausbleibenden Bedarf bei brauchbaren Voreinstellungen durch *allgemeine* ARPs zurückzuführen.

[6] Hierbei ist zu berücksichtigen, dass dieser Wert von einer US-amerikanischen Hochschule berichtet wurde, die Shibboleth auch für organisationsinternes Single Sign-On einsetzt.

der Speicherverwaltung ausreichend Zeit zu gewähren, so dass für jede Messung vergleichbare Ausgangszustände geschaffen werden konnten.

Die eigentlichen Messungen wurden zur Vereinfachung des Versuchsaufbaus durch einen sequentiellen Aufruf beider neuer FIM-Komponenten außerhalb des Shibboleth-Kontextes durchgeführt, indem entsprechende Aufrufparameter generiert wurden.

6.6.3. Ergebnisse der Performanzmessungen

Die **erste Messreihe** mit lediglich einer FIM-Anfrage resultiert in den bestmöglichen Antwortzeiten:

- Wie Abbildung 6.5 entnommen werden kann, variiert die Dauer für das Abrufen aller Benutzerattribute aus dem LDAP-basierten Identity Repository zwischen 16 und 20 Millisekunden; der Durchschnitt beträgt 16,56ms.
- Abbildung 6.6 zeigt die Dauer für die Durchführung der drei XSLT-basierten Konvertierungen; der Durchschnitt der 100 Messungen liegt bei 13ms.
- Die Dauer für die Bearbeitung der XACML Attribute Release Policies liegt wie in Abbildung 6.7 dargestellt zwischen 201 und 208 Millisekunden; der Durchschnitt beträgt 203,60ms.

Somit ergibt sich wie in Abbildung 6.8 dargestellt eine durchschnittliche Gesamtbearbeitungszeit von 233,16ms durch die beiden neuen FIM-Komponenten, an der die ARP-Verarbeitung mit rund 87% den größten Anteil hat. Die somit verursachte Verzögerung der FIM-Transaktion um rund 0,23 Sekunden fällt in der Praxis kaum ins Gewicht, da ihre Gesamtdauer in den vorhandenen Testumgebungen durch den Einsatz von HTTP-Redirect-basierter, über den Benutzerclient mittelbarer Kommunikation bei Shibboleth typischerweise rund zwei Sekunden beträgt.

In der **zweiten Messreihe** mit zehn parallelen Anfragen ergeben sich die folgenden Werte:

- Die Dauer für den Abruf eines Benutzerprofils aus dem Identity Repository beträgt durchschnittlich 51,866ms. Wie Abbildung 6.9 entnommen werden kann, können mehr als zwei Drittel der LDAP-Anfragen innerhalb von 25–60 Millisekunden beantwortet werden; nur sehr selten dauert der LDAP-Zugriff länger als 120ms.
- Die Verarbeitungsdauer für die XSLT-basierten Konvertierungen beträgt im Durchschnitt 42,950ms; Abbildung 6.10 zeigt, dass die Verarbeitungszeit in mehr als zwei Drittel aller Fälle weniger als 55 Millisekunden beträgt.
- Die in Abbildung 6.11 dargestellte Dauer für die Auswertung der XACML-ARPs beträgt durchschnittlich 318,965ms; mehr als zwei Drittel der Anfragen werden dabei in weniger als 400 Millisekunden beantwortet.

Wie in Abbildung 6.12 dargestellt ist, ergibt sich somit eine durchschnittliche Verzögerung von rund 414 Millisekunden; der Anteil der XACML-Verarbeitung beträgt dabei rund 77%.

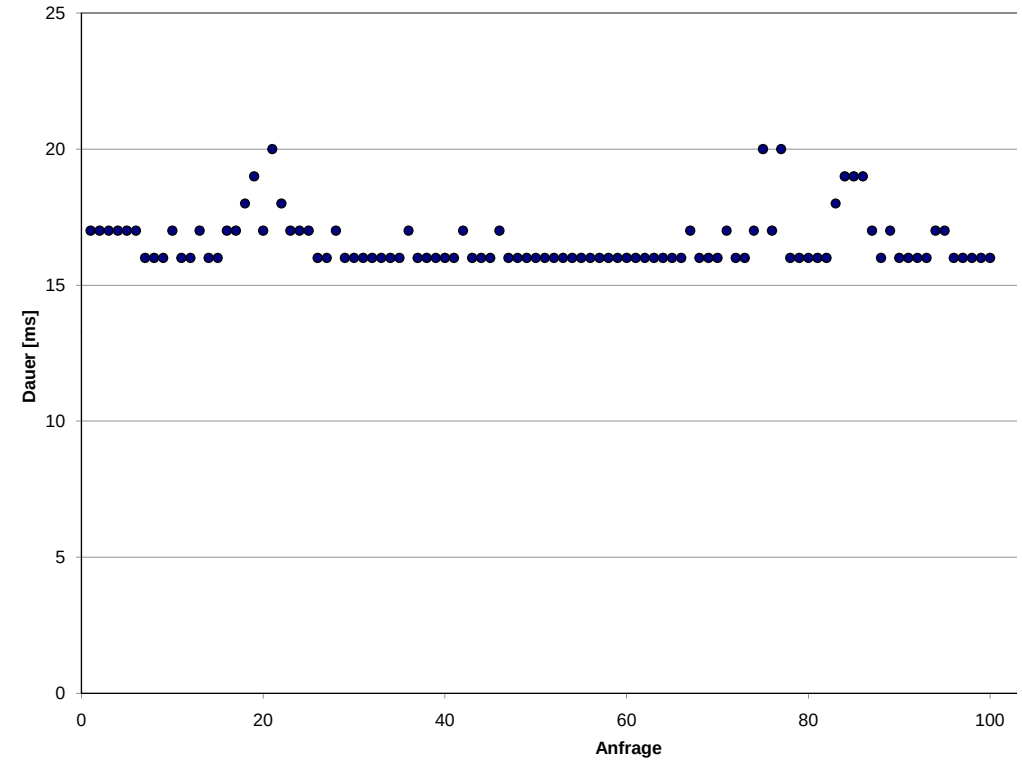


Abbildung 6.5.: Messreihe 1a: Dauer des Benutzerprofilabrufs bei *einer* Anfrage

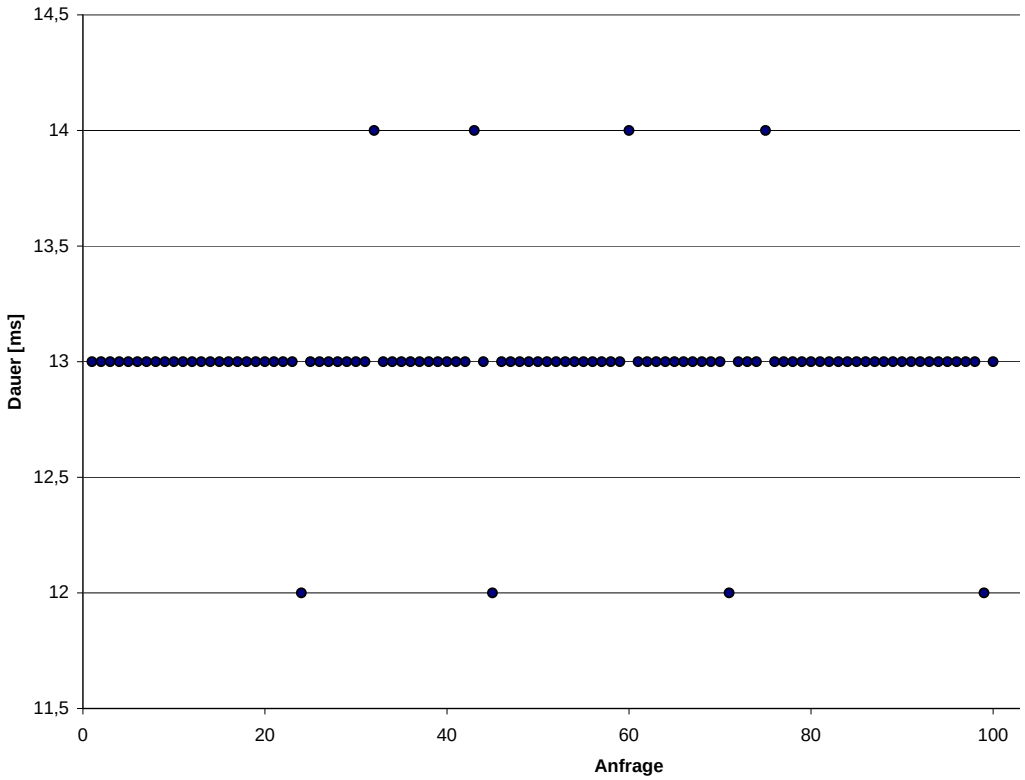


Abbildung 6.6.: Messreihe 1b: Dauer der XSLT-basierten Konvertierung bei *einer* Anfrage

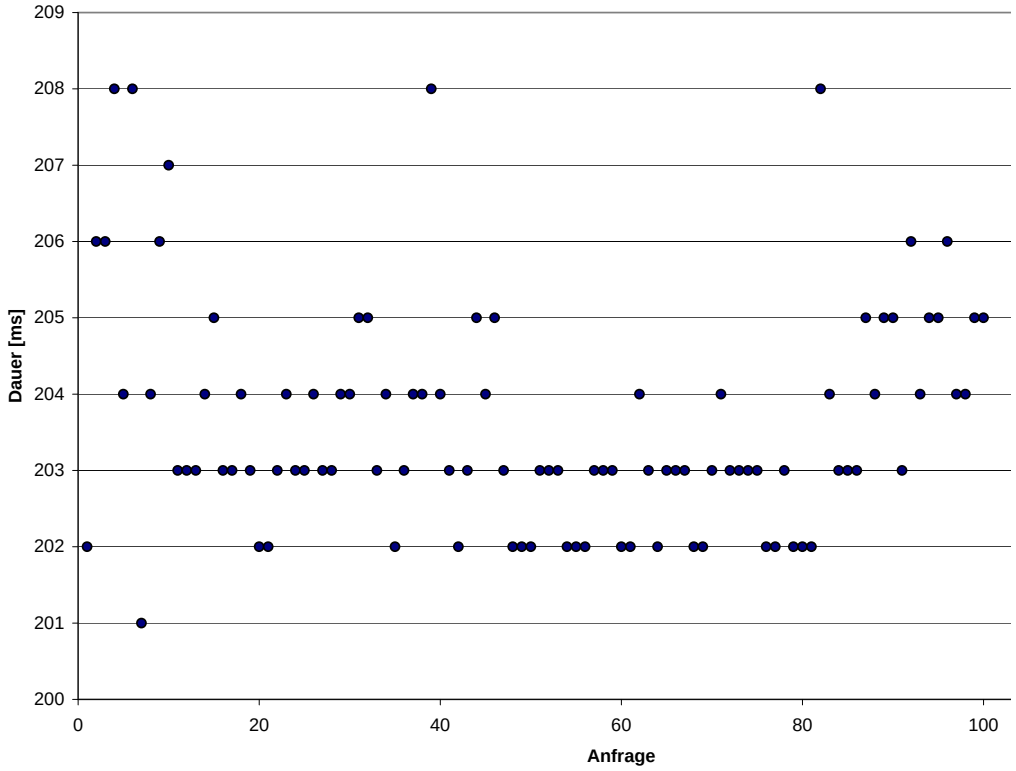


Abbildung 6.7.: Messreihe 1c: Dauer der XACML-Bearbeitung bei *einer* Anfrage

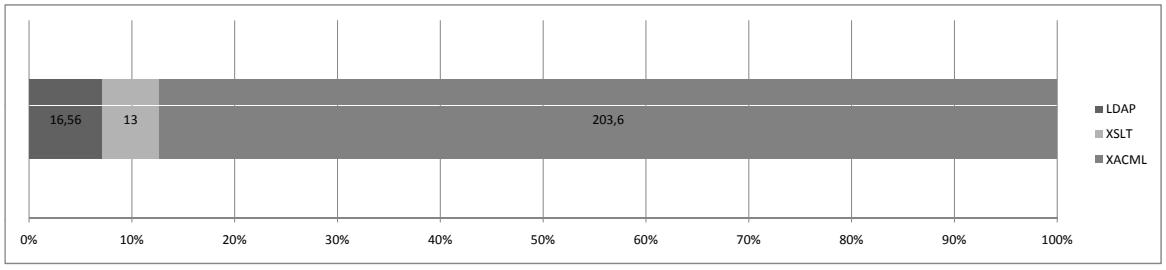


Abbildung 6.8.: Anteile an der Verarbeitungsdauer bei *einer* Anfrage

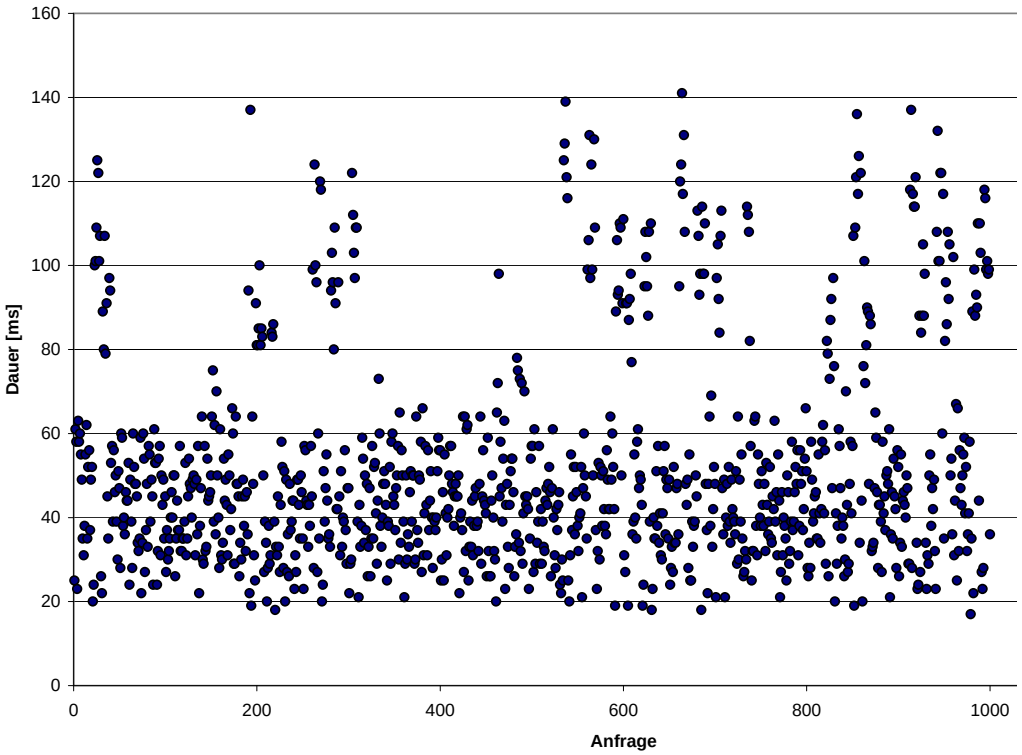


Abbildung 6.9.: Messreihe 2a: Dauer des Benutzerprofilabrufs bei zehn parallelen Anfragen

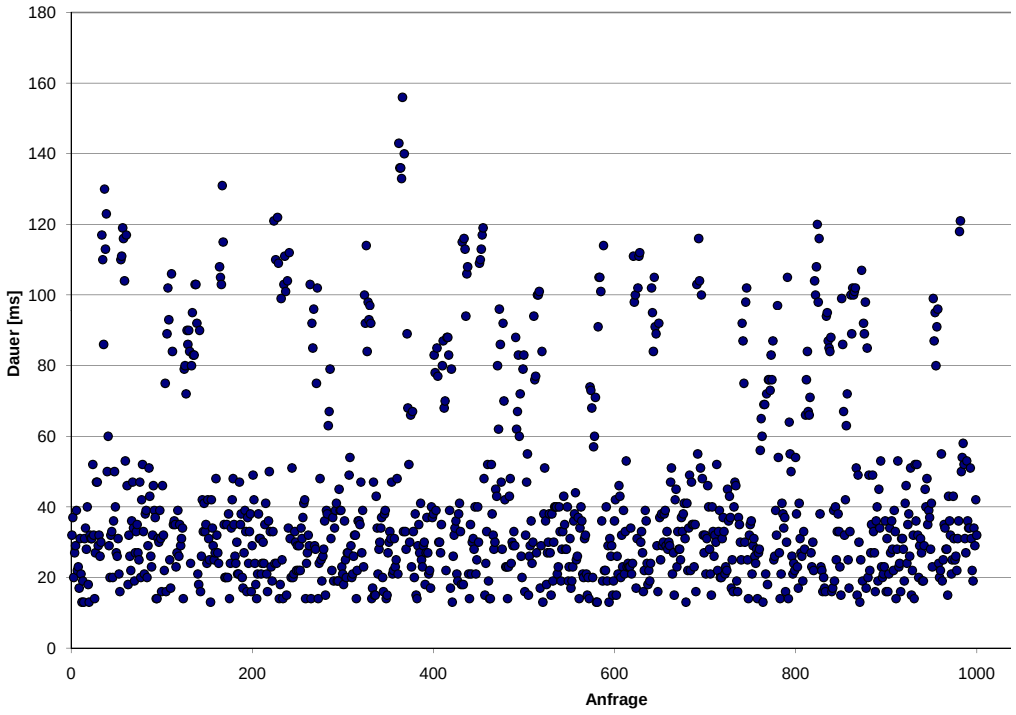


Abbildung 6.10.: Messreihe 2b: Dauer der XSLT-basierten Konvertierung bei zehn parallelen Anfragen

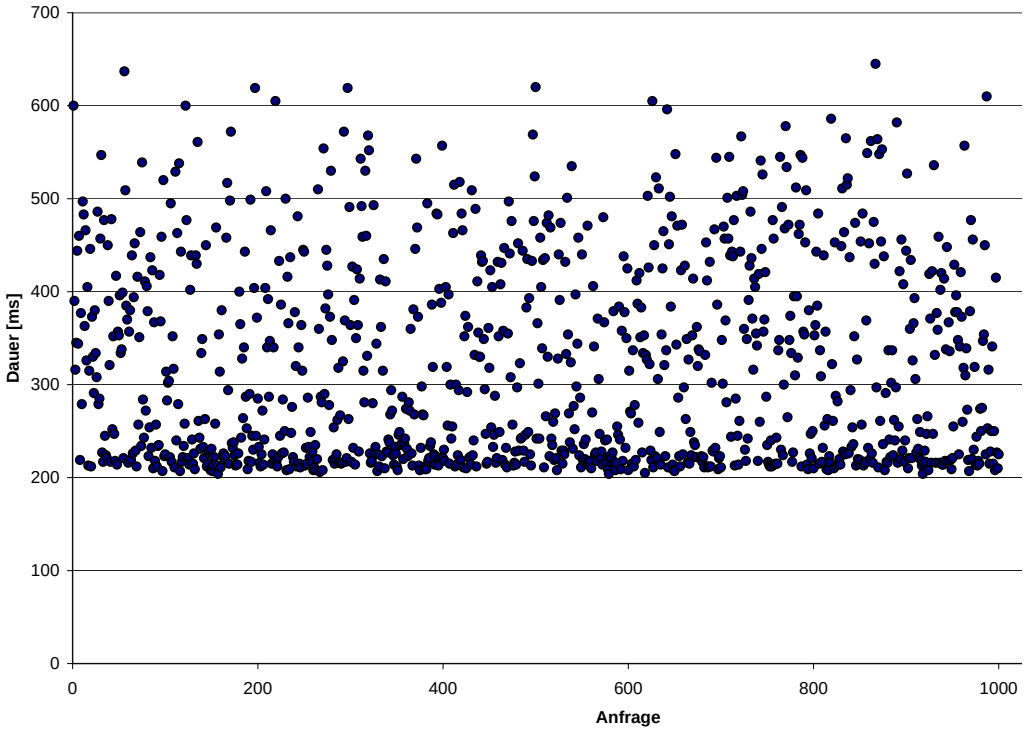


Abbildung 6.11.: Messreihe 2c: Dauer der XACML-Bearbeitung bei zehn parallelen Anfragen

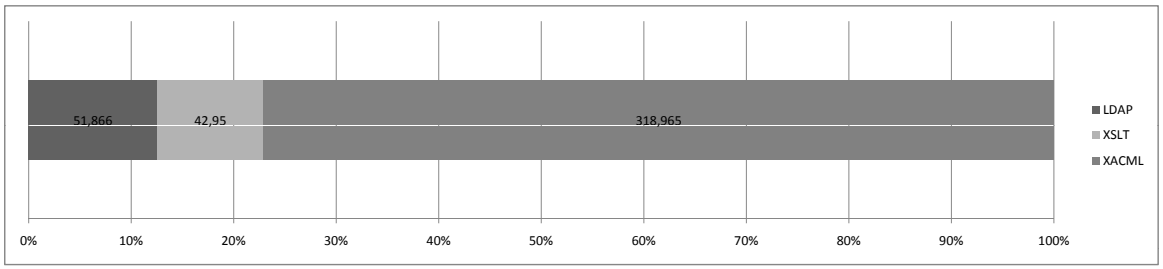


Abbildung 6.12.: Anteile an der Verarbeitungsdauer bei zehn parallelen Anfragen

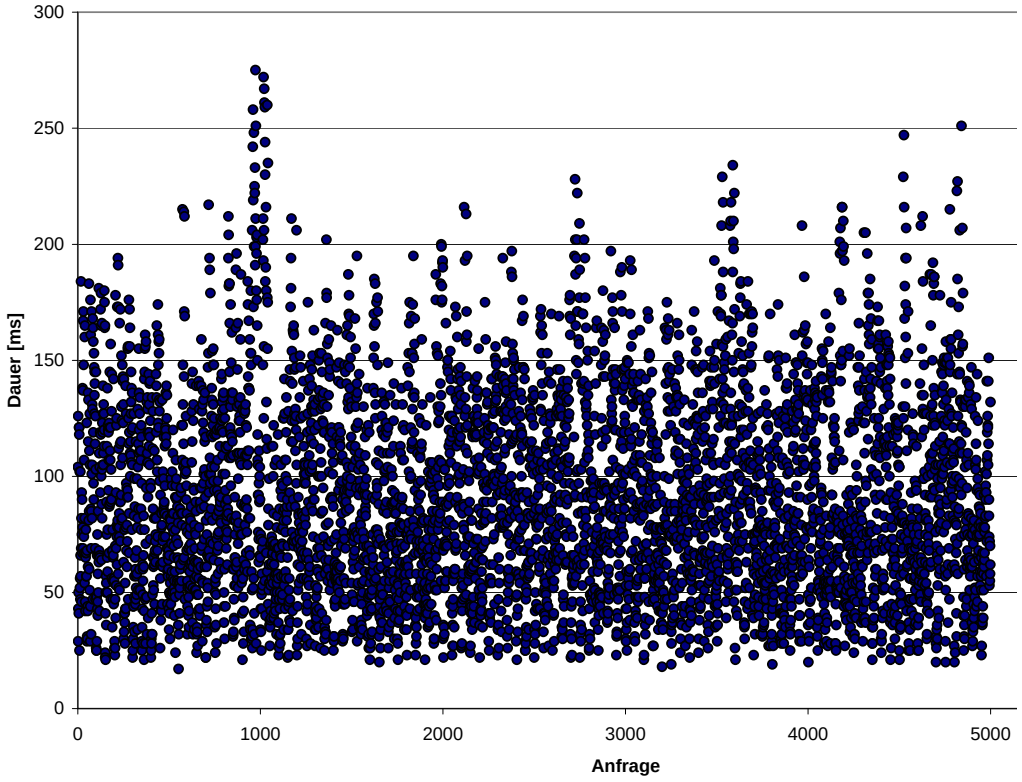


Abbildung 6.13.: Messreihe 3a: Dauer des Benutzerprofilabrufs bei 50 parallelen Anfragen

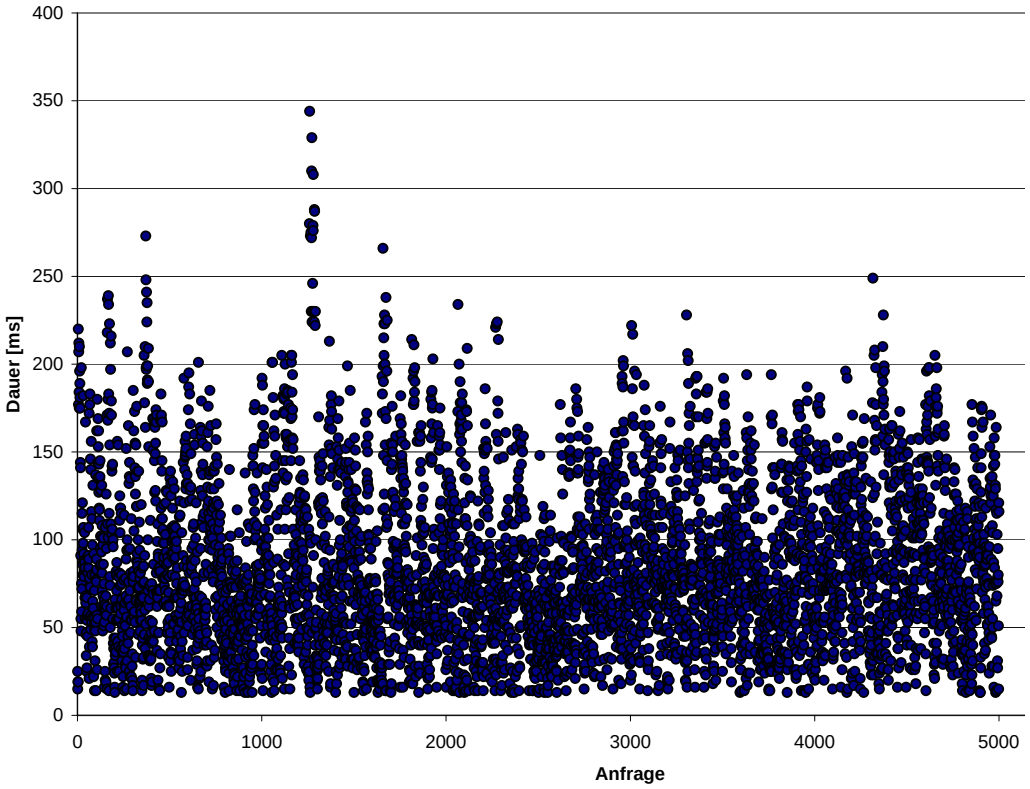


Abbildung 6.14.: Messreihe 3b: Dauer der XSLT-basierten Konvertierung bei 50 parallelen Anfragen

Während die Verarbeitungszeiten für die LDAP-Anfragen und die XSLT-basierte Konvertierung somit circa um den Faktor 3 zugenommen haben, ist die Auswertung der XACML-ARPs nur um das knapp 1,6-fache langsamer.

Die resultierende Verzögerung um rund 0,41 Sekunden kann dabei als bereits spürbar, aber durchaus akzeptabel betrachtet werden.

Die **dritte Messreihe**, in der 50 Anfragen parallel gestartet wurden, führte zu folgenden Werten:

- Die durchschnittliche Dauer zum Abruf der Benutzerprofile aus dem LDAP-Server beträgt rund 90,91ms. Mehr als zwei Drittel der Anfragen wurden wie in Abbildung 6.13 dargestellt in weniger als 130 Millisekunden beantwortet.
- Die Durchführung der XSLT-basierten Konvertierung dauert durchschnittlich 84,89ms; eine länger als 200 Millisekunden dauernde Bearbeitung war dabei, wie aus Abbildung 6.14 ersichtlich, relativ betrachtet nur sehr selten festzustellen.
- Die Bearbeitung der XACML-ARPs dauert wie in Abbildung 6.15 dargestellt durchschnittlich 419,31ms; nur in relativ wenigen Fällen dauert sie länger als 1.000, jedoch zum Teil bis zu über 2.500 Millisekunden.

Somit ergibt sich eine durchschnittliche Verzögerung von rund 595 Millisekunden, an der wie in Abbildung 6.16 gezeigt die XACML-Verarbeitung einen Anteil von rund 70% hat. Sie ist als für den Benutzer spürbar einzustufen, der zugrunde gelegten Hochlastsituation jedoch durchaus angemessen.

Im Hinblick auf die **Skalierbarkeit und mögliche Verbesserungen** ist festzuhalten, dass

- die Dauer einer von 50 parallelen LDAP-Anfragen durchschnittlich um den Faktor 5,5 höher ist als bei einer einzigen LDAP-Anfrage. Eine weitere Optimierung dieser auch unter hoher Last mit durchschnittlich rund 91ms bereits sehr guten Antwortzeiten erscheint für vergleichbare Szenarien nicht notwendig.
- jede der 50 parallelen XSLT-Verarbeitungen durchschnittlich um den Faktor 6,5 länger dauert als die Verarbeitung nur einer Anfrage. Obwohl dies das schlechteste der hier betrachteten Ergebnisse ist, überrascht es sehr positiv, da vergleichbare Untersuchungen in verwandten XSLT-Einsatzgebieten ergeben haben, dass ca. 98% der Rechenzeit auf die XSLT-Auswertung zurückfällt (vgl. [AHKS02]). Eine weitere Verbesserung könnte wie in Abschnitt 5.2.3 erläutert beispielsweise durch den Einsatz von präkompilierten XSLT-Stylesheets erreicht werden; da die Antwortzeiten jedoch auch in Hochlastsituationen mit durchschnittlich rund 85ms bereits sehr brauchbar sind, erscheint diese Maßnahme ebenfalls nicht dringend notwendig zu sein.
- durchschnittlich jede der 50 parallelen Auswertungen von XACML-ARPs gegenüber der Situation ohne Parallelität lediglich um das 2,1-fache länger dauert. Trotz dieses sehr guten Verhaltens unter Last trägt die Verarbeitung der XACML-ARPs am stärksten zur Gesamtdauer bei, da insbesondere eine Unterschreitung der Untergrenze von 200 Millisekunden nicht zu beobachten war. Da der Großteil der Verarbeitungszeit in dieser Komponente vom verwendeten XACML Policy Decision Point verbraucht wird, der

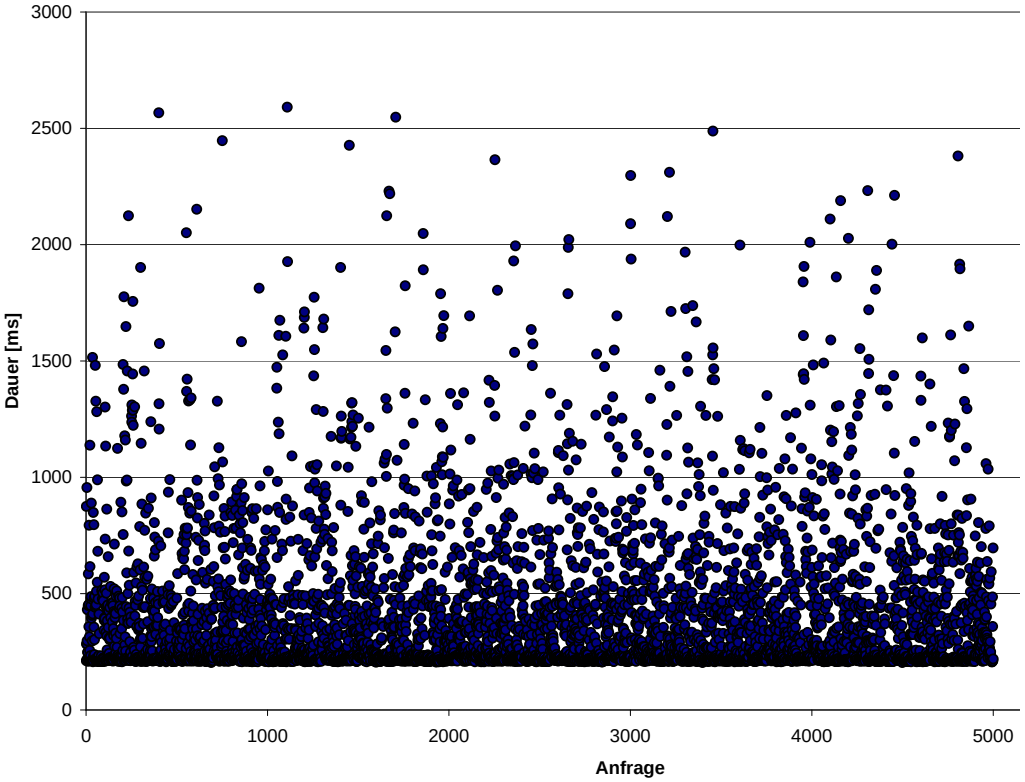


Abbildung 6.15.: Messreihe 3c: Dauer der XACML-Bearbeitung bei 50 parallelen Anfragen

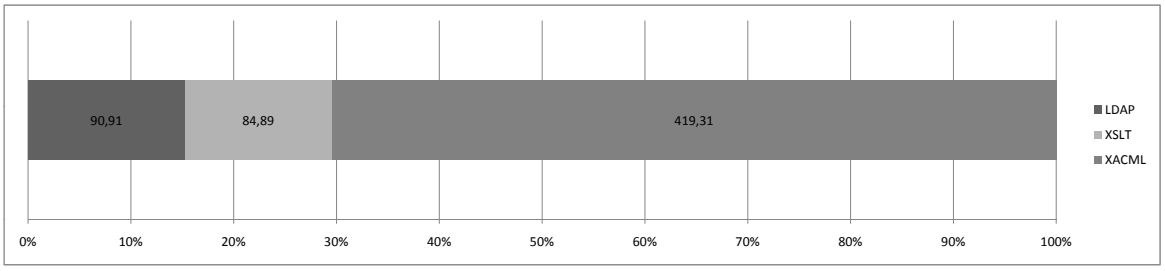


Abbildung 6.16.: Anteile an der Verarbeitungsdauer bei 50 parallelen Anfragen

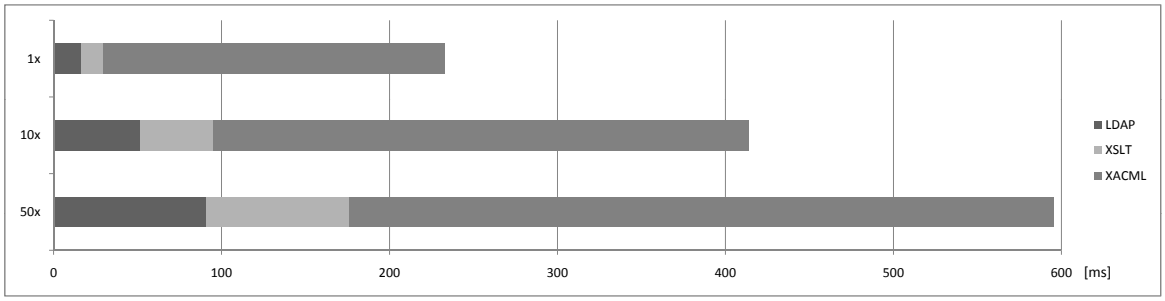


Abbildung 6.17.: Gegenüberstellung der Verarbeitungszeiten bei einer, zehn bzw. 50 Anfragen

wiederum von eigenen Implementierungen nicht maßgeblich beeinflusst werden kann, wäre die Verwendung eines anderen XACML PDPs die am nächsten liegende Optimierungsmöglichkeit; ihr konnte im Rahmen dieser Arbeit jedoch nicht nachgekommen werden, da noch keine frei verfügbaren Alternativen zur Referenzimplementierung von Sun existieren.

Die Ergebnisse der hier durchgeführten Untersuchungen sind in Abbildung 6.17 zusammengefasst. Bei einem praktischen Einsatz ist darüber hinaus zu beachten, dass sich die Verarbeitungsgeschwindigkeit durch die parallel laufenden Servlet-Container- und Shibboleth-Prozesse und deren Hauptspeicherverbrauch verschlechtern könnte. Die Performanz für den Produktivbetrieb eingesetzter Implementierungen muss deshalb noch wesentlich ausführlicher untersucht werden, um Richtwerte für die Dimensionierung der entsprechenden Infrastruktur ableiten zu können.

6.7. Zusammenfassung und Aspekte des praktischen Einsatzes

In diesem Kapitel wurden die Java-Implementierungen zweier in Kapitel 4 neu eingeführter FIM Komponenten in ihren Varianten für die FIM-Software Shibboleth vorgestellt. Sowohl beim XSLT-basierten Identitätsdatenkonverter als auch beim XACML-basierten FIM Privacy Management System hat sich gezeigt, dass eine vollständige Umsetzung des spezifizierten Funktionsumfangs mit tiefen Eingriffen in Shibboleth verbunden wäre, so dass dieser zugunsten einer nahtlosen und mit angemessenem Aufwand realisierbaren Integration in Shibboleth reduziert wurde.

Die resultierenden Implementierungen demonstrieren somit einerseits zwei Kernideen dieser Arbeit und stellen andererseits einen konkreten Mehrwert beim Einsatz in bestehenden Shibboleth-Infrastrukturen dar. Die rudimentären Performanzmessungen verdeutlichen, dass die Verwendung von XSLT und XACML zwar spürbare, aber bereits in der prototypischen Umsetzung akzeptable Verzögerungen von FIM-Transaktionen mit sich bringt; die Entscheidung, diese beiden Sprachen für Konvertierungsregeln bzw. Attribute Release Policies zu verwenden, wird somit durch die Implementierung gestützt, auch wenn deren weitere Verbesserung anzustreben ist.

Die am Shibboleth Identity Provider durchgeführten Änderungen wurden in Form eines Quelltext-Patches veröffentlicht und mit den Entwicklern von Shibboleth und einigen anderen Nutzern in Form von E-Mail- und Mailinglistenkorrespondenz diskutiert. Obwohl die Ideen dabei durchaus positiv aufgenommen wurden, besteht derzeit keine Möglichkeit, die Beiträge in der bereits in Arbeit befindlichen Version 2.0 von Shibboleth zu berücksichtigen, da sie zu umfangreich sind und zur Nutzung des vollen Funktionsumfangs größere architekturelle Änderungen an Shibboleth notwendig wären. Es wurde jedoch Bereitschaft signalisiert, die Thematik nach der Fertigstellung von Shibboleth 2.0 erneut aufzugreifen.

Bezüglich eines breiteren praktischen Einsatzes muss jedoch ferner berücksichtigt werden, dass Hilfsmittel für die Erstellung, Überprüfung und Pflege der Konvertierungsregeln und Attribute Release Policies benötigt werden. Für XSLT sind – aufgrund seiner Verbreitung und Anwendung insbesondere im Umfeld von Webapplikationen zur Erzeugung von HTML aus XML-Datenstrukturen – bereits zahlreiche Entwicklungs- und Testwerkzeuge verfügbar; diese könnten als Ausgangsbasis für ein umfassendes FIM-Werkzeug dienen, das auch die Koordination mit dem im Rahmen dieser Arbeit nicht implementierten Federation Schema Correlation Service übernimmt.

Bei XACML-Editoren ist zu berücksichtigen, dass diese nicht nur die in dieser Arbeit spezifizierte ARP-Semantik zielgerichtet unterstützten sollten, sondern auch gleichermaßen von Administratoren und Benutzern eingesetzt werden. Insbesondere im Hinblick auf letztere ist anzustreben, die Komplexität der Policysprache vollständig durch eine intuitive graphische Benutzeroberfläche zu verschatten, deren Entwicklung für eine vollständige Umsetzung der vorgestellten Konzepte unerlässlich bleibt.

Kapitel 7.

Anwendungsbeispiel: Das LRZ als Identity und Service Provider

Inhalt dieses Kapitels

In diesem Kapitel werden die in den Kapiteln 4 und 5 vorgestellten Architektur- und Werkzeugkonzepte sowie die erarbeitete Integrationsmethodik anhand eines konkreten, realistischen Beispiels veranschaulicht. Anstatt nur eines der in Kapitel 2 analysierten Szenarien zu vertiefen, steht im Folgenden das Leibniz-Rechenzentrum im Fokus, das szenarienübergreifend sowohl als Identity als auch als Service Provider fungiert und somit die Möglichkeit bietet, die **Gesamtarchitektur anhand eines durchgängigen Beispiels** zu demonstrieren; zudem lassen sich beim Hosting ausgewählter FIM-Komponenten für die Technische Universität München Synergien durch gemeinsame Komponentennutzung erzielen.

Ein ebenfalls wichtiger Aspekt dieses Kapitels ist die Gegenüberstellung der Möglichkeiten, die sich bereits bisher mit FIM realisieren ließen, mit den sich durch die in dieser Arbeit neu eingeführten und zum Teil implementierten FIM-Komponenten ergebenden Optionen.

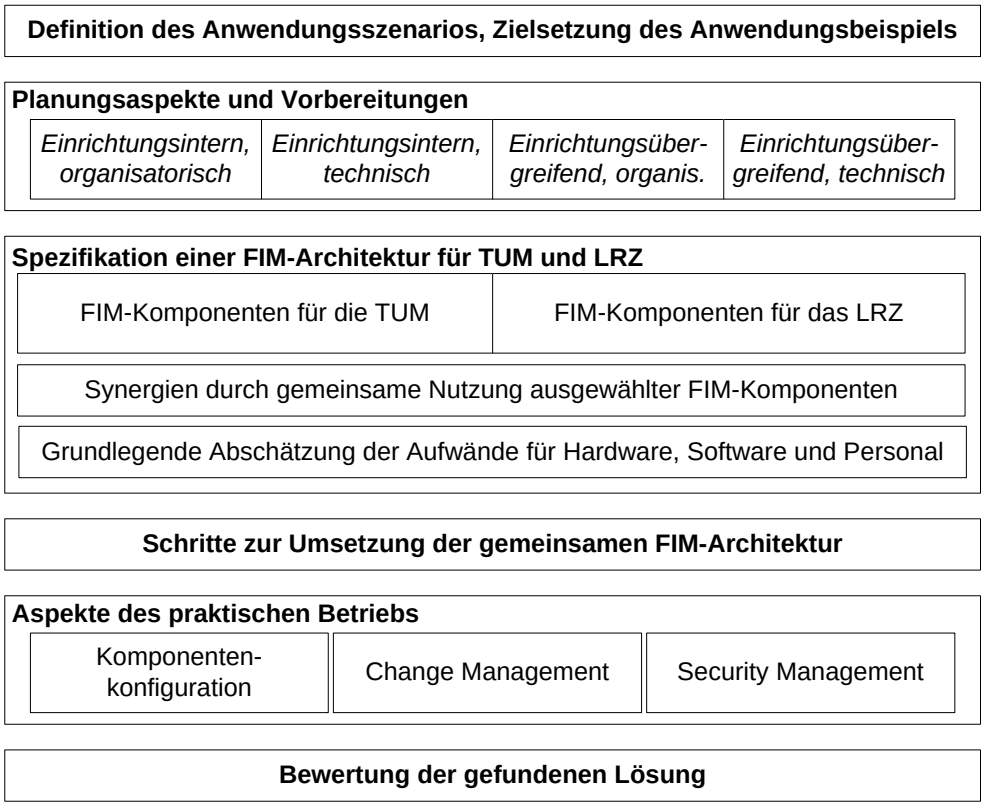


Abbildung 7.1.: Vorgehensmodell für dieses Kapitel

Zunächst wird in Abschnitt 7.1 diskutiert, wie die in Kapitel 2 betrachteten Szenarien zum hier untersuchten **Anwendungsszenario** zusammengefügt und welche FIM-spezifischen Ziele angestrebt werden. Abschnitt 7.2 geht im Anschluss auf **Planungsaspekte** ein, wobei neben grundlegenden organisatorischen Regelungen auch die organisationsinternen und -übergreifenden technischen Vorbereitungen am konkreten Beispiel betrachtet werden.

Auf Basis der in Kapitel 4 spezifizierten Referenzarchitekturen wird in Abschnitt 7.3 eine **FIM-Architektur für das Anwendungsszenario** erarbeitet, mit der die gesteckten technischen Zielsetzungen erreicht werden; die **Migrationsschritte** zur Umsetzung dieser Zielarchitektur werden anschließend in Abschnitt 7.4 diskutiert, wobei auch rudimentäre **Aufwandsabschätzungen** angegeben werden.

Abschnitt 7.5 dient der Untersuchung verschiedener **Aspekte des Betriebs der FIM-Lösung**, zu denen zum einen die prinzipielle Konfiguration der FIM-Werkzeuge und zum anderen die konkreten Veränderungen im Change und Security Management gehören. In Abschnitt 7.6 wird die exemplarisch umgesetzte FIM-Lösung abschließend bewertet und es wird auf verbleibende offene Punkte eingegangen. Abbildung 7.1 stellt das Vorgehensmodell für dieses Kapitel graphisch dar.

7.1. Definition von Anwendungsszenario und Zielsetzung

Mit Ausnahme von Szenario 2, anhand dessen das User Centric Identity Management am Beispiel von Microsoft CardSpace untersucht wurde, haben alle in Kapitel 2 diskutierten Szenarien einen Bezug zum LRZ:

- **Szenario 1** baut auf dem Identity & Access Management System der Technischen Universität München auf, das im Rahmen des DFG-Projekts IntegraTUM vom LRZ realisiert wird. Das LRZ fungiert im Rahmen des Projekts somit einerseits als Service Provider für ausgewählte Dienste und übernimmt andererseits die Rolle eines Identity Providers für die TUM in Analogie zu klassischen Outsourcingszenarien. Diese unabhängig von der technischen Realisierung prinzipielle **organisatorische Trennung der beiden Einrichtungen** wird in diesem Anwendungsbeispiel berücksichtigt.

- **Szenario 3** untersucht die Rolle des LRZ als Dienstleister im Münchner Wissenschaftsnetz (MWN) und geht insbesondere auf die Übertragbarkeit von FIM-Lösungen auf herkömmliche, d. h. nicht web-service- bzw. webbasierte Dienste und Applikationen ein. Dieser Aspekt dient zur **Veranschaulichung der Mehrwerte**, die sich durch die **Einführung der SP-Software** als eigenständige, von den Diensten unabhängige Komponente ergeben.

- **Szenario 4** illustriert die MWN-übergreifenden Aufgaben des LRZ am Beispiel des Grid-Computings; es veranschaulicht den hier zwangsläufig bereits vorhandenen Bedarf an organisationsübergreifendem Identity Management, die bislang vorherrschenden sehr einfachen Lösungen und die vielversprechenden Möglichkeiten einer FIM-Lösung durch die konsequente Weiterentwicklung der Grid-Middleware-Infrastruktur auf Basis von Web Services. Hier wird das Beispiel einer Föderation für DEISA aufgegriffen, um die **Mitgliedschaft einer Organisation in mehreren Föderationen** berücksichtigen zu können.

- **Szenario 5** schildert eine mögliche Weiterentwicklung der Virtuellen Hochschule Bayern, an der die TUM als Trägerhochschule mitwirkt. Das LRZ ist daran mindestens als Identity Provider für die TUM beteiligt; durch die im Rahmen des TUM-Projekts elecTUM aufgebaute Learning Management Infrastruktur ist zudem auch eine Teilnahme als Service Provider gegeben. Da sich durch **komplexere Applikationen** wie Learning Management Systeme aus offensichtlichen Gründen **höhere Anforderungen an die FIM-Infrastruktur** ergeben als beispielsweise beim reinen organisationsübergreifenden Single Sign-On, wird auch dieser Dienst der TUM mit einbezogen.

Die Aktualität und Realitätsnähe dieses Anwendungsszenarios ist zudem durch die sich konkretisierenden Pläne für eine hochschulspezifische deutschlandweite Shibboleth-Föderation im Rahmen der DFN-AAI gegeben, die hier – wie die bislang fiktive DEISA-Föderation – als organisatorisches Rahmenwerk herangezogen wird (vgl. Abschnitt 6.3.3).

Insgesamt resultieren daraus die folgenden **FIM-spezifischen Aufgaben des LRZ**:

- Das LRZ fungiert als **Identity Provider**

  - **für die TUM** in allen für diese relevanten Bereichen; dies wird an den Beispielen des LRZ und der VHB als Service Provider verdeutlicht.
  - **für prinzipiell alle Kunden des LRZ und deren Benutzer** mit Rechenberechtigung am LRZ; diese Aufgabe wird am Beispiel des Zugangs zum Grid-Computing im Rahmen von DEISA für Wissenschaftler im MWN veranschaulicht.

- Das LRZ ist **Service Provider**

  - **für alle Kunden im MWN**, wobei sich das Anwendungsbeispiel auf die TUM beschränkt.
  - **im Rahmen von Grid-Projekten**, für die stellvertretend wiederum DEISA als Beispiel gewählt wurde.
  - im Rahmen der Pläne der VHB zur FIM-basierten Nutzung der an den Trägerhochschulen vorhandenen Learning Management Systeme **als Outsourcingdienstleister der TUM**.

Die Ausgangssituation für alle nachfolgenden Erläuterungen ist der im Frühjahr 2007 aktuelle Stand der in den Szenarien 1 und 3 beschriebenen Projekte IntegraTUM und LRZ-SIM, in denen moderne I&AM-Infrastrukturen für die TUM und das LRZ aufgebaut werden. Sie decken sich weitgehend mit der im Architekturkonzept getroffenen Annahme, dass lokale I&AM-Systeme bereits vorhanden sind, ohne dass bei deren Planung FIM-Aspekte im Sinne der in Kapitel 3 vorgestellten Konzepte, Protokolle und Produkte explizit berücksichtigt wurden.

Das **Ziel dieses Anwendungsbeispiels** ist somit die Umsetzung der in Kapitel 4 erläuterten Konzepte und Methodik vor dem Hintergrund des oben erläuterten Aufgabenspektrums; neben der Randbedingung, die Lösung möglichst flexibel und erweiterbar zu gestalten, liegen somit insbesondere die folgenden **Schwerpunkte** vor:

- Die generellen **organisatorischen und technischen Voraussetzungen** für den Einsatz von FIM an TUM und LRZ müssen analysiert werden.
- Ebenso sind die organisatorischen und technischen Aspekte des FIM-Einsatzes im Zusammenspiel mit den anderen beteiligten Organisationen zu untersuchen.
- Die **Erweiterungen** der bestehenden, vom LRZ betriebenen **I&AM-Lösungen um FIM-Komponenten** und deren **nahtlose Integration** sind zu spezifizieren; insbesondere darf die Integration in die vorhandene **IT-Sicherheitsinfrastruktur** nicht vernachlässigt werden.
- Die resultierende FIM-Architektur ist im Hinblick auf den **Realisierungsaufwand** und die anfallenden Investitions- und Betriebskosten unter Berücksichtigung der sich ergebenden Mehrwerte zu beurteilen.
- Die konkreten Einzelschritte sind auf Basis der in Kapitel 4 vorgegebenen Migrations- und Integrationsmethodik konzeptionell durchzuführen.
- Der **Selektion der verwendeten FIM-Komponenten** ist zu begründen; ihr Einsatz soll anhand der Skizzierung ihrer **Konfiguration** verdeutlicht werden, wobei insbesondere die Unterschiede zu herkömmlichen FIM-Architekturen und die Vorteile, die sich

durch den Einsatz der in Kapitel 5 spezifizierten Komponenten ergeben, von Bedeutung sind.

- Die Auswirkungen auf das **IT Service Management** des LRZ sind darzulegen; wie in Kapitel 4 erfolgt dabei eine Beschränkung auf FIM-spezifische Aspekte des Change Managements und des Security Managements.

Abbildung 7.2 zeigt die aus den Szenarien 1 und 3 bekannten I&AM-Systeme der TUM und des LRZ in einer auf die für das Anwendungsbeispiel relevanten Dienste beschränkten Ansicht.

Die weiteren Abschnitte dieses Kapitels sind zur Veranschaulichung des Vorgehens bei der Einführung einer FIM-Lösung chronologisch im Sinne eines **Projekts zur Einführung von FIM** angeordnet und anhand der für die jeweilige Phase zutreffenden Aufgabenschwerpunkte strukturiert.

7.2. Planungsaspekte und Vorbereitungen

Die Einführung einer FIM-Lösung ist aufgrund der Komplexität der dadurch zu unterstützenden organisationsübergreifenden Geschäftsprozesse und der größeren Zahl in Betrieb zu nehmender technischer Komponenten ein umfangreiches Vorhaben, das entsprechend gründlich vorbereitet werden muss. Diese Phase unterscheidet sich insbesondere durch die **Neuartigkeit der Funktionalität** deutlich vom Change Management bei später variierenden Anforderungen, Dienstspektren und Föderationskonstellationen.

Zur nachfolgenden Erläuterung bietet sich eine Trennung von organisatorischen und technischen sowie organisationsinternen und organisationsübergreifenden Aspekten an, deren inhärent enge Verzahnung jedoch bei einer angestrebten praktischen Umsetzung geeignet berücksichtigt werden muss.

7.2.1. Einrichtungsinterne organisatorische Aspekte

Nachdem die Entscheidung zur Einführung von FIM getroffen wurde, ist eine mit der Planung und Realisierung zu beauftragende **Projektgruppe** zu bilden, an der die folgenden Mitglieder beteiligt sein sollten:

- Ausgewählte Personen aus dem Kreis der für das bestehende I&AM-System zuständigen LRZ-Mitarbeiter bringen die technischen Kompetenzen ein und stellen den **Kern der Projektgruppe** dar.
- **Vertreter der über FIM anzubietenden Dienste** bringen ihre spezifischen Anforderungen ein und koordinieren das notwendige Change Management auf Seiten der Dienste; im Beispiel betrifft dies primär das Learning Management System der TUM sowie die für DEISA zuständigen Mitarbeiter am LRZ.
- Ein **Spezialist im Bereich der System- und Netzwerksicherheit** aus der LRZ-Abteilung Kommunikationsnetze begleitet die grundlegenden Planungen sowie das Architekturdesign und ist für die Umsetzung der Schutzmaßnahmen bei der Inbetriebnahme verantwortlich.

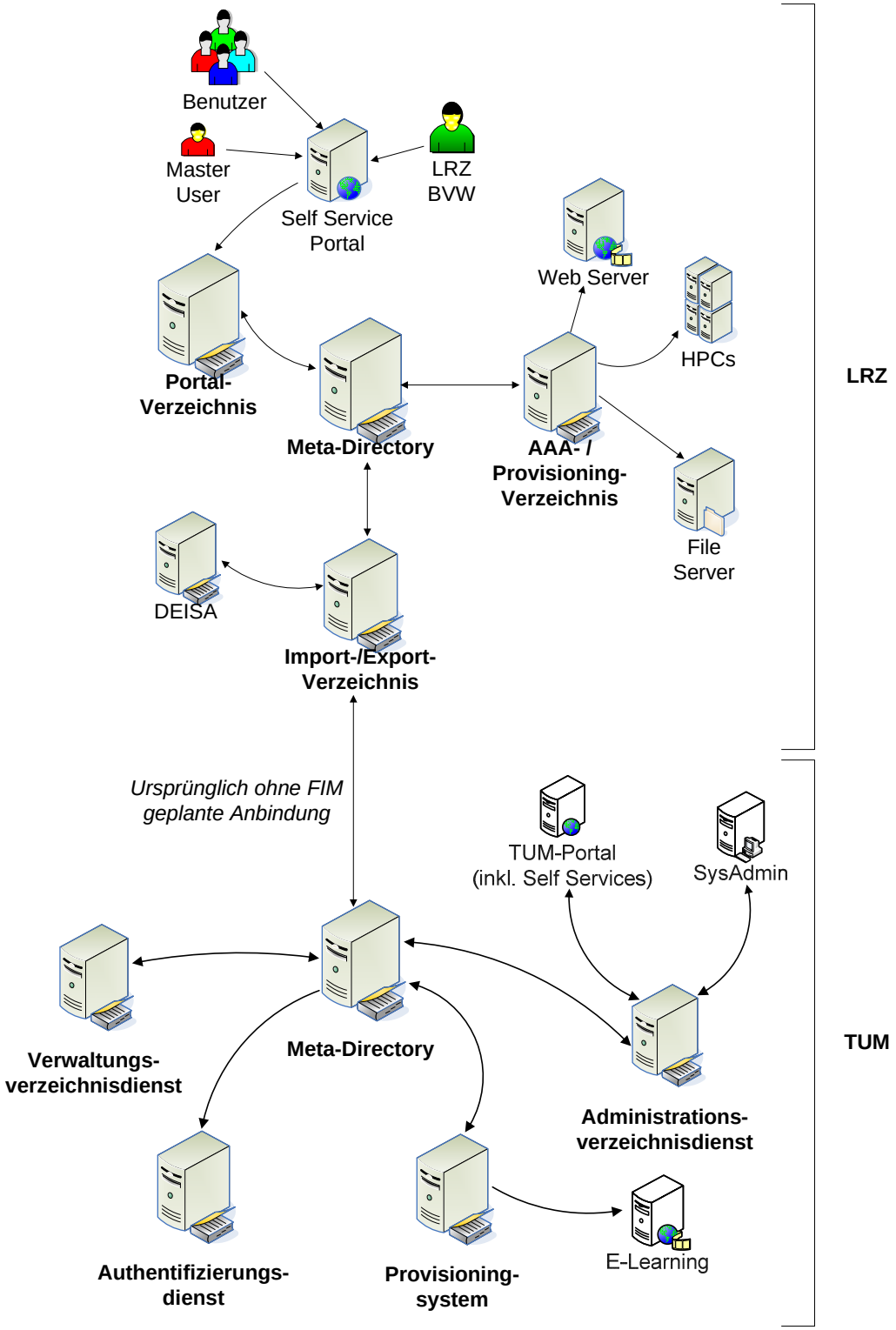


Abbildung 7.2.: Ausgangssituation im Anwendungsbeispiel: I&AM-Systeme an TUM und LRZ

- Für die Planung und Dokumentation der neuen Prozesse und die **Koordination mit dem organisationsweiten IT Service Management des LRZ** sollte ein diesen Aufgaben dedizierter Mitarbeiter zur Verfügung stehen, der die Planungsphase begleitet und in der späteren Betriebsphase als Ansprechpartner fungiert.

Die ersten organisatorischen Aufgaben dieser Projektgruppe umfassen die folgenden Punkte:

1. Die noch nicht mit der FIM-Thematik vertrauten **Projektmitglieder müssen geeignet geschult** und insbesondere auch für die organisatorischen Aspekte sensibilisiert werden.

2. Die **Projektziele müssen priorisiert** werden:

   - Wie in Abschnitt 4.6.5 diskutiert wurde, sollte die Realisierung der Rolle als Identity Provider zuerst in Angriff genommen werden, u. a. um den lokalen Benutzern rasch Mehrwerte bieten zu können und die folgende Implementierung der Service Provider Komponenten autark und unter realen Einsatzbedingungen testen zu können.
   - Es muss entschieden werden, ob die noch nicht FIM-fähigen anzubindenden Dienste wie das Learning Management System zur Ausschöpfung der vollen FIM-Funktionalität erweitert oder wie bisher über das I&AM-System gespeist werden sollen; gegebenenfalls sind frühzeitig **Verhandlungen mit den Herstellern** aufzunehmen. Im Unterschied zum Architekturkonzept dieser Arbeit ist bei herkömmlichen Lösungen wie Shibboleth eine Anpassung der Dienste zwangsweise erforderlich.

3. Aus dem Kreis der Projektmitglieder sind Mitarbeiter zu bestimmen, die die **Koordination mit den anderen Organisationen und Föderationsverwaltungen** übernehmen. Aufgrund der fachlichen Nähe sollte dies beim Teilszenario Grid-Computing ein Mitarbeiter aus diesem Bereich sein, wohingegen bei nicht unmittelbar anwendungsspezifischen Föderationen wie der DFN-AAI ein Ansprechpartner aus dem Bereich der I&AM-Lösung selektiert werden sollte. Gegebenenfalls ist zwischen organisatorischen und technischen Ansprechpartnern zu differenzieren.

4. Mit den lokal zuständigen **Datenschutzbeauftragten** sollte so früh wie möglich Kontakt aufgenommen werden, um entsprechende Verfahrensbeschreibungen vorzubereiten. Da sich insbesondere die IDP-Software von herkömmlichen datenverarbeitenden Systemen dadurch unterscheidet, dass sie der bedarfsorientierten Weitergabe personenbezogener Daten an Dritte dient, müssen Unklarheiten bezüglich der prinzipiellen Funktionsweise schnellstmöglich ausgeräumt werden. Im Rahmen der DFN-AAI wird diese Konstellation zusätzlich dadurch komplexer, dass das **LRZ als Auftragsdatenverarbeiter für die TUM** fungiert.

   Ein enger Kontakt mit den Datenschutzbeauftragten ist später auch beispielsweise bei der Konfiguration von IDP-weiten Attribute Release Policies erforderlich.

5. Die grundlegenden **Finanzierungsaspekte** sind zu klären. Während eine Konkretisierung der Kosten von der erst noch zu erarbeitenden Spezifikation der Zielarchitektur

abhängig ist, kann die Größenordnung des über den Personalaufwand hinausgehenden Investitionsvolumens bereits in dieser Phase abgeschätzt werden; insbesondere ist davon auszugehen, dass keine Software-Lizenzkosten anfallen, so dass die Kosten für Anschaffung und Betrieb der Hardware im Vordergrund stehen; auf sie wird im nachfolgenden Abschnitt 7.2.2 eingegangen.

6. Das **organisationsinterne Change Management** ist wie in Abschnitt 4.8 beschrieben für den Einsatz von FIM vorzubereiten; insbesondere sind FIM-spezifische temporäre oder ständige Teilnehmer für das zu erweiternde Change Advisory Board zu benennen und die neuen Use Cases, in denen dieses eingeschaltet werden muss, zu dokumentieren und bekanntzugeben.

Auf weitere für die Projektdurchführung erforderliche, aber nicht FIM-spezifische Aspekte wird an dieser Stelle nicht weiter eingegangen.

7.2.2. Einrichtungsinterne technische Aspekte

Bevor mit der konkreten Gestaltung der FIM-Architektur für das diskutierte Szenario begonnen werden kann, sind die vorhandenen I&AM-Infrastrukturen an LRZ und TUM zu analysieren, die in den Szenarien 1 und 3 in Kapitel 2 vorgestellt wurden; dabei werden die folgenden Randbedingungen offensichtlich:

- Weder am LRZ noch an der TUM sind bislang organisationsinterne Single Sign-On Systeme im Einsatz, da lediglich ein Unified Login realisiert wurde. Für die IDP-Software muss somit (auch im herkömmlichen Fall beim Einsatz von Shibboleth) ein zusätzlicher **webbasierter Authentifizierungsdienst** vorgesehen werden.
- Ebenso sind noch **keine I&AM Privacy Management Systeme** im Einsatz, da die Bereitstellung personenbezogener Daten ausschließlich über LDAP Access Control Lists und Filter in den eingesetzten I&AM-Konnektoren gesteuert wird. Die Einführung eines solchen Systems ist im vorliegenden Szenario aus FIM-Perspektive nicht notwendig, da bis auf Weiteres **keine Langzeitobligationen** notwendig sind.
- An beiden betrachteten Einrichtungen werden bereits **Self Services** eingesetzt, die auf Open Source Basis realisiert wurden und somit prinzipiell für die Erweiterung um FIM-spezifische Teildienste geeignet sind.
- **Privilege Management Systeme** sind derzeit nur für das Teilszenario Grid-Computing relevant; da die Bereitstellung geeigneter Schnittstellen zu FIM-Komponenten noch Gegenstand aktueller anderer Forschungsarbeiten ist, wird nachfolgend davon ausgegangen, dass das Privilege Management System die lokalen Datenbestände eines I&AM-Systems verwenden kann und nur im Rahmen der Grid-Dienste benötigt wird, so dass es in der allgemeinen FIM-Architektur vernachlässigt werden kann.

Unter der Annahme, dass mindestens **IDP- und SP-Software auf dedizierten Maschinen** zu betreiben sind, ergibt sich in dieser Phase unter der Berücksichtigung der zur Ausfallsicherheit redundanten Auslegung der Hardware eine Untergrenze von vier bereitzustellenden Servermaschinen für den FIM-Einsatz.

Hinsichtlich ihrer **Positionierung in der Netzwerktopologie des LRZ** können netzwerksicherheitsspezifische Vorarbeiten entfallen, da das LRZ bereits über die in Abschnitt 4.7.2.1 erläuterten Sicherheitszonentypen verfügt und eine rasche Inbetriebnahme neuer Maschinen ermöglicht.

In einem weiteren Schritt ist die **Analyse der eigenen Datenbestände** sowie der Anforderungen an die über FIM bezogenen Daten notwendig:

- Die in der Rolle als Identity Provider zur Verfügung zu stellenden Benutzerdaten werden mit Ausnahme der Anforderungen des VHB-Teilszenarios durch die vorhandenen I&AM-Systeme abgedeckt; die **Anforderungen an die Aktualität der Daten** wurden bislang nur von der DFN-AAI konkret spezifiziert und werden ebenfalls bereits erfüllt. Somit sind weder Anpassungen an den Quellsystemen der I&AM-Lösungen noch Änderungen an den organisationsinternen Datenakquisitions- und Verarbeitungsprozessen erforderlich.

  Im VHB-Szenario wird wie in Abschnitt 2.2.3 erläutert der lesende und schreibende Zugriff auf Prüfungsleistungen von Studenten angestrebt; diese werden aus Datenschutzgründen bewusst nicht im I&AM-System der TUM vorgehalten. Eine Bereitstellung dieser Daten ist somit mit der Erweiterung des Prüfungsverwaltungssystems der TUM zu einer eigenständigen Attribute Authority verbunden, auf die hier jedoch nicht explizit eingegangen wird, da sie einerseits zum derzeitigen Zeitpunkt aufgrund fehlender Schnittstellen der eingesetzten Prüfungsverwaltungssoftware noch nicht realisierbar ist und andererseits die nachfolgend zur TUM als Identity Provider getroffenen Aussagen auch auf die Rolle als Attribute Authority übertragen werden können.

- Für die Rolle des Service Providers sind Minimal- und Ideal-Anforderungen an die von anderen Identity Providern zu liefernden Daten zu stellen. Die hierfür notwendigen Informationen wurden bereits beim Aufbau der I&AM-Systeme erfasst und können übernommen werden. Hierbei ist zu beachten, dass es für die betroffenen Dienste in jedem Fall sinnvoll ist, auch die organisatorische Zugehörigkeit ihrer Benutzer auszuwerten. Während dies im Teilszenario DEISA seit jeher üblich ist, muss beispielsweise das Learning Management System entsprechend erweitert werden; insbesondere ist diesem auch die bislang implizit angenommene Zugehörigkeit der Benutzer zur TUM explizit zu kommunizieren, so dass eine kleinere **Erweiterung des entsprechenden I&AM-Konnektors** notwendig wird.

  Bezüglich des Learning Management Systems kann es darüber hinaus sinnvoll sein, beispielsweise zwischen Benutzern beliebiger anderer VHB-Trägerhochschulen und solchen Studenten zu unterscheiden, die einen gemeinsam mit einer anderen Hochschule durchgeführten Studiengang belegen, da über diese zusätzliche Informationen notwendig sein können.

- An TUM und LRZ werden unterschiedliche Datenmodelle verwendet, da mit der Verwaltung von Studenten und Mitarbeitern einerseits und dem Rechenzentrumsbetrieb andererseits auch differierende Anforderungen an das Identity Management einhergehen; ebenso werden für die DFN-AAI und das Grid-Projekt DEISA jeweils wiederum abweichende LDAP-Schemata verwendet. Somit ist die **Notwendigkeit zum Einsatz des Identitätsdatenkonverters** gegeben.

Parallel zu den in Abschnitt 7.2.1 skizzierten Vorabgesprächen mit den Datenschutzbeauftragten können bereits grundlegende Überlegungen zur späteren Konfiguration von Attribute Release Policies angestellt werden. Insbesondere muss auf Grundlage der Use Cases in den Teilszenarien entschieden werden, ob Benutzer einen direkten Einfluss auf die sie betreffenden Attribute Release Policies haben müssen, da sich in diesem Fall die Notwendigkeit zur Integration eines ARP-Editors in die Self Services als Anforderung an die Lösungsarchitektur ergibt.

Im vorliegenden Gesamtszenario ist diesbezüglich ausschlaggebend, dass über die DFN-AAI eine nicht a priori begrenzte Menge an Diensten bereitgestellt werden soll, sondern eine Dynamik der beteiligten Service Provider und deren Anforderungen an bereitzustellende Benutzerattribute zu erwarten ist. Eine **benutzergesteuerte Konfiguration der Datenfreigaben** ist somit mittelfristig zwingend erforderlich und sollte deshalb von Anfang an berücksichtigt werden.

7.2.3. Einrichtungsübergreifende organisatorische Aspekte

Da FIM nicht nur im MWN neu eingeführt wird, sondern sich beispielsweise auch die DFN-AAI, in die auch das Teilszenario VHB integriert werden soll, erst im Aufbau befindet und folglich nur auf die Erfahrungen aus den stark technisch orientierten bisherigen Testumgebungen zurückgegriffen werden kann, spielt die organisationsübergreifende Koordination eine wichtige Rolle.

Die hierbei vorherrschenden Kernaufgaben sind **Institution der Föderationsverwaltungen** und die **vertragliche Fixierung der Föderationsmitgliedschaften**; hierzu kann die folgende Partitionierung der Teilszenarien vorgenommen werden:

- Der DFN-Verein betreibt die Föderationsverwaltung der DFN-AAI und bereitet das Rahmenwerk für die Verträge mit den partizipierenden Hochschulen vor. Das darin enthaltene SLA regelt die Datenqualitätsanforderungen, die wie in Abschnitt 7.2.2 erläutert seitens TUM und LRZ bereits erfüllt werden. Für das VHB-Teilszenario, das die bayerischen Hochschulen und somit eine Teilmenge des DFN-AAI-Einzugsgebietes umfasst, ist die Integration in die DFN-AAI anzustreben, wodurch sich eine von dieser separierte Föderation erübrigt.
- Grid-Projekte wie DEISA überschreiten die geographischen Grenzen der DFN-AAI, so dass eine zusätzliche, naheliegenderweise dedizierte Föderation notwendig wird. Wie in Abschnitt 2.2.2.2 dargestellt wurde, basiert das DEISA Identity Management derzeit auf einer einheitlichen, verteilten LDAP-Benutzerverwaltung, so dass alle beteiligten Einrichtungen die möglichen Anforderungen gleichermaßen erfüllen. Aufgrund der bisherigen Rolle der niederländischen SARA Computing and Network Services als Betreiber des Wurzel-LDAP-Servers könnte dort auch die DEISA Föderationsverwaltung angesiedelt werden; der organisatorische Verwaltungsaufwand reduziert sich dabei durch die direkte Kopplung der Kriterien zur Aufnahme in diese Föderation mit denjenigen zur Teilnahme an DEISA selbst.
- Für das LRZ als Dienstleister im MWN, für das hier exemplarisch lediglich die TUM als Kunde betrachtet wird, ist die Fragestellung zu untersuchen, ob eine dedizierte MWN-Föderation notwendig wird oder eine Integration in die DFN-AAI möglich ist. Hierfür

ist ausschlaggebend, ob die anderen Hochschulen im Hoheitsgebiet des LRZ die Anforderungen zum Beitritt in die DFN-AAI erfüllen, bzw. ob die Anforderungen des LRZ weniger restriktiv als die der DFN-AAI wären. Nach Möglichkeit sollte der **Aufwand für den Betrieb einer eigenen Föderationsverwaltung vermieden** und stattdessen die Verbesserung der lokalen I&AM-Infrastrukturen an den betroffenen Hochschulen priorisiert und unterstützt werden.

Analog zu den in Abschnitt 7.2.1 erläuterten internen Schulungen sind darüber hinaus teilszenariospezifisch die Koordination der Ziele beim FIM-Einsatz und der Know-How-Transfer sicherzustellen; nachfolgend wird davon ausgegangen, dass die dabei vereinbarten Ziele mit den in Kapitel 2 bei den einzelnen Szenarien diskutierten Optionen übereinstimmen.

7.2.4. Einrichtungsübergreifende technische Aspekte

Durch jede der Föderationen muss in Anbetracht der in Kapitel 3 diskutierten, noch vorherrschenden Inkompatibilitäten zwischen den FIM-Ansätzen die Entscheidung für eine Protokoll- oder Produktbasis getroffen werden. Aufgrund des akademischen Umfelds und der kostenlosen Lizenzen ist **Shibboleth** dabei die erste Wahl, die im Rahmen der DFN-AAI auch bereits manifestiert wurde.

Bei der Differenzierung zwischen dem Architekturkonzept dieser Arbeit und demjenigen von Shibboleth wird nachfolgend deshalb davon ausgegangen, dass Shibboleth mit den im Rahmen dieser Arbeit durchgeführten Modifikationen eingesetzt wird, wobei zur Veranschaulichung die strukturierte Trennung der einzelnen FIM-Komponenten mit den in Abschnitt 7.3 erläuterten Ausnahmen beibehalten wird.

Darüber hinaus ist die **föderationsweite Bereitstellung der folgenden Dienste** zu planen:

- Die **Verwaltung und Distribution der Föderationsmetadaten** muss aufgebaut werden. Nachfolgend wird davon ausgegangen, dass das LRZ selbst keine Metadaten pflegt, die nicht die TUM- und LRZ-spezifischen FIM-Komponenten betreffen, und dass wie in Abschnitt 4.4.11 beschrieben – im Unterschied zu Shibboleth – ein Push-Verfahren zum Föderationsmetadatentransfer zum Einsatz kommt.

  In diesem Kontext ist pro Föderation zu klären, welche **PKIs für die Ausstellung von Serverzertifikaten** für die relevanten FIM-Komponenten verwendet werden können; für die Maschinen an TUM und LRZ ist die DFN-PKI zu verwenden, wobei zu beachten ist, dass vom DFN für Grid-Maschinen eine separate Grid Certificate Authority betrieben wird.

- Die zentrale Bereitstellung eines **IDP Discovery Services** erfolgt pro Föderation und durch die jeweilige Föderationsverwaltung, da die Teilszenarien nicht ausreichend organisatorisch gekoppelt sind, um gemeinsam einen multi-federation-fähigen IDP Discovery Service aufzubauen.

- Der **Federation Schema Correlation Service** kann föderationsübergreifend eingesetzt werden und muss somit nicht mehrfach instanziiert werden. Im Folgenden wird vereinfachend davon ausgegangen, dass er vom LRZ betrieben und anderen interessierten Einrichtungen zur Verfügung gestellt wird.

In der Regel ist ferner ein **föderationsweites Schema** mit der Definition der Syntax und Semantik der einzelnen Attribute zu spezifizieren. Die DFN-AAI orientiert sich hierbei stark an der in Abschnitt 3.8.1 diskutierten LDAP-Objektklasse `eduPerson`, während DEISA das ebenfalls bereits vorhandene, DEISA-spezifische LDAP-Datenmodell übernehmen kann.

Zusammen mit dem Schema sind unter Berücksichtigung der an der jeweiligen Föderation beteiligten Service Provider und Use Cases bereits Attribute Release Policies zu entwerfen. Neben *föderationsweiten* ARPs können insbesondere auch Vorlagen für *IDP-weite* ARPs erarbeitet werden, die von jedem Identity Provider beispielsweise in Zusammenarbeit mit den lokalen Datenschutzbeauftragten weiter verfeinert werden können; auf diese Aktivität wird in Abschnitt 7.5.1 näher eingegangen, da sie bei Bedarf im laufenden Betrieb erneut aufgegriffen werden muss.

Analog zu den ARPs sind ebenfalls föderationsweite Absprachen zu den SP-seitigen Attribute Acceptance Policies zu treffen; zwar sind mit AAPs insbesondere auch servicespezifische Anforderungen an die Datenqualität umzusetzen, der IDP-seitige Konfigurationsaufwand kann aber durch **einander ähnliche SP-seitige Attribute Acceptance Policies**, z. B. bei allen am VHB-Teilszenario eingesetzten Learning Management Systemen, deutlich reduziert werden.

Schließlich ist eine **Testumgebung** mit exemplarischen Identity und Service Providern zu planen; diese können beispielsweise von Organisationen verwendet werden, die nur eine der beiden Rollen wahrnehmen, und auch dauerhaft parallel zur Produktivumgebung betrieben werden, um potentiellen neuen Föderationsmitgliedern den technischen Einstieg zu erleichtern. Insbesondere sind auch damit vergleichbare Systeme für die Produktivumgebung vorzusehen, die z. B. für die **Überprüfung der Einhaltung der Datenqualitätsvorgaben** durch die Föderationsverwaltung eingesetzt werden können.

Nach Abschluss der erläuterten organisationsinternen und -übergreifenden Planungen und Vorbereitungen sind alle Parameter bekannt, die für die nachfolgende Konzeption der lokalen FIM-Architektur benötigt werden.

7.3. Spezifikation der Zielarchitektur

In diesem Abschnitt wird diskutiert, wie die an TUM und LRZ vorhandenen I&AM-Architekturen um FIM-spezifische Komponenten erweitert werden müssen, um die betrachteten Teilszenarien realisieren zu können. Der Schwerpunkt liegt dabei auf der Auswahl und Kombination der neuen Komponenten, wohingegen die konkreten Migrationsschritte im nachfolgenden Abschnitt 7.4 skizziert werden.

In den Abschnitten 7.3.1 und 7.3.2 werden zunächst die **TUM- und LRZ-seitig notwendigen neuen Komponenten** auf Basis der bereits vorhandenen Infrastruktur erläutert. Daran anschließend wird in Abschnitt 7.3.3 dargestellt, wie sich im Anwendungsszenario **Synergien durch die gemeinsame Nutzung ausgewählter FIM-Komponenten** ausnutzen lassen; in Abschnitt 7.3.4 wird schließlich auf den **zu erwartenden Aufwand bei der Umsetzung** eingegangen, der in der hier exemplifizierten Projektphase zu bestimmen ist.

Zur Verdeutlichung der Motivation für die verschiedenen Teilaufgaben und auf Basis des aktuellen Stands der Identity Management Projekte an TUM und LRZ erfolgen die Erläute-

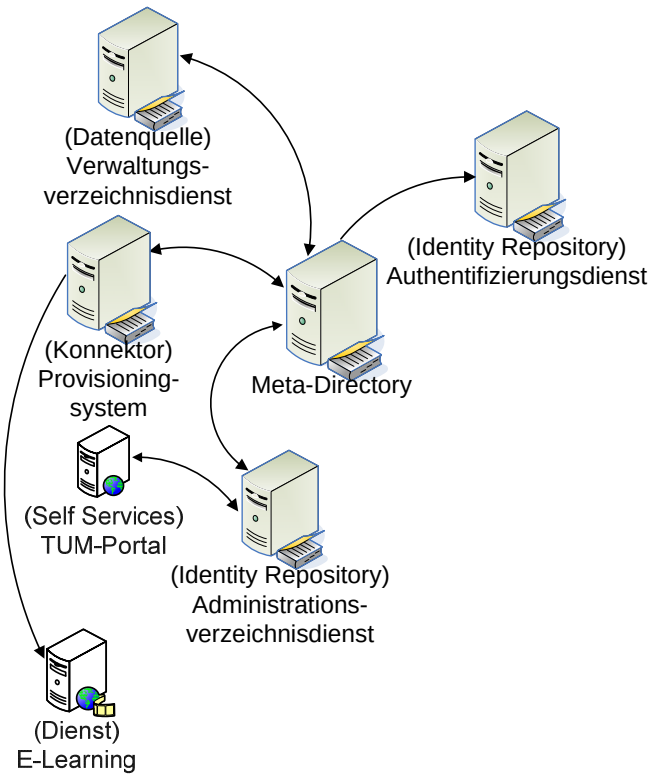


Abbildung 7.3.: I&AM-Architektur der TUM in Analogie zur Referenzarchitektur

rungen für beide Organisationen getrennt, obwohl die Infrastrukturen primär durch das LRZ betrieben werden.

7.3.1. Erweiterung der I&AM-Architektur der TUM

Abbildung 7.3 zeigt nochmals die bereits in Szenario 1 erläuterte I&AM-Architektur der TUM in einer bezüglich der Komponentenpositionierung an die in Kapitel 4 vorgestellte Referenzarchitektur angepassten Darstellung.

Nachfolgend wird auf die Einführung von FIM-Komponenten für die TUM in den Rollen als Identity bzw. als Service Provider eingegangen.

7.3.1.1. Architektur für die TUM als FIM Identity Provider

Eine erste grundlegende Entscheidung ist die **Wahl des für FIM-Transaktionen zu verwendenden Identity Repository**: Da ein dedizierter Authentifizierungsverzeichnisdienst vorhanden ist und wie in Abschnitt 7.2.2 erläutert kein Privilege Management System zum Einsatz kommen soll, ist somit primär die Datenquelle für allgemeine Attributsauskünfte festzulegen.

Nachdem das IntegraTUM-Sicherheitskonzept vorsieht, dass Zugriffe auf das zentrale Meta-Directory nur von möglichst wenigen anderen Komponenten durchgeführt werden sollen, ist

der so genannte Administrationsverzeichnisdienst zu wählen, da dieser auch für den durch Dienste schreibenden Zugriff konzipiert wurde und somit für FIM-Schreiboperationen geeignet ist. Da er unter anderem zur Lieferung der Benutzerdatenbestände an das Webportal der TUM und an die angeschlossenen Fakultäten dient, erfüllt er ebenfalls die diskutierten Voraussetzungen hinsichtlich des Umfangs und der Qualität der Personendaten.

Zur Vervollständigung der I&AM-Basiskomponenten ist wie in Abschnitt 7.2.2 dargelegt die Einführung eines **webbasierten Authentifizierungsdienstes** notwendig, der als Frontend für den bereits vorhandenen, LDAP-basierten Authentifizierungsverzeichnisdienst fungiert. Eine einfache Möglichkeit hierzu bietet ein Application Server wie Apache Tomcat, der auch für den Einsatz des Shibboleth Identity Providers benötigt wird (vgl. Abschnitt 6.3.1). Es liegt deshalb nahe, die Tomcat-Webauthentifizierung und die Shibboleth IDP-Software parallel auf derselben Hardware zu betreiben, obwohl es sich aus FIM-Perspektive um voneinander isolierte Komponenten handelt.

Darüber hinaus werden die folgenden FIM-Komponenten und ihre Integration in die Netzwerk- und Sicherheitsinfrastruktur benötigt, damit die TUM als Identity Provider fungieren kann:

- Das zentrale und essentielle Element der IDP-spezifischen Erweiterung der vorhandenen I&AM-Architektur ist die **IDP-Software**. Sie ist wie in Abschnitt 4.7.2 beschrieben auf Servern in der über das Internet erreichbaren demilitarisierten Zone (DMZ) zu betreiben. Da derzeit noch keine geeigneten Application Level Gateways für die FIM-Protokolle existieren, muss auf diese im Architekturkonzept erläuterte Schutzmaßnahme vorerst verzichtet werden.

  Analog dazu ist der Einsatz des **Gateways zum lokalen Datenbestand** erforderlich, da auf ihn nur verzichtet werden könnte, wenn ausschließlich Authentifizierungsbestätigungen ausgestellt werden sollten; dies trifft auf keines der Teilszenarien zu. Auch der Einsatz der **Schnittstelle zu den Föderationsmetadaten** ist unentbehrlich; bei Verwendung von Shibboleth ist diese wie bereits erläutert in die IDP-Software integriert.

- Der **FIM-Interaktionsdienst** ist wie in Abschnitt 4.4.5 diskutiert in die bereits vorhandenen **Self Services** zu integrieren, da sein autarker Betrieb aus Benutzerperspektive keine Vorteile bringt und unter der Annahme ausreichender Serverkapazitäten nicht erforderlich ist. An der Positionierung der Self Services in der Netzwerktopologie werden dadurch keine Änderungen notwendig, da diese im Rahmen des TUM-Webportals bereits über das Internet genutzt werden können. Es ist zu beachten, dass diese Komponente beim Betrieb einer herkömmlichen Shibboleth-Infrastruktur entfallen würde und die Self Services mit Ausnahme des unten diskutierten Editors für Attribute Release Policies unabhängig von FIM-Anwendungen zu betreiben wären.

- Der Betrieb einer dedizierten Datenbasis für die in den Abschnitten 4.4.1.1 und 5.5 spezifizierten Datensubskriptionen ist nicht erforderlich, da hierfür das vorhandene **Datenbank-Hostingangebot** des LRZ genutzt werden kann, dessen Netzwerksicherheitsinfrastruktur bereits den in Abschnitt 4.7.2 gestellten Anforderungen entspricht. Beim Einsatz von Shibboleth würde sich die Funktionalität auf das optionale Protokollieren der an Service Provider übertragenen Benutzerattribute beschränken, da die *Subscriptions & Notifications* der Liberty Alliance nicht unterstützt werden.

Entsprechend wird auch der in Abschnitt 5.5 spezifizierte **Notifications-Konnektor** nur im Rahmen einer über die Möglichkeiten von Shibboleth hinausgehenden Realisierungsarchitektur benötigt. Wie im Werkzeugkonzept beschrieben wurde, beschränken sich seine unmittelbaren Aufgaben auf das Weiterleiten ausgewählter Events im Identity Repository an die IDP-Software. Diese Funktionalität ist deutlich weniger komplex als diejenige der anderen bereits in der I&AM-Infrastruktur implementierten Konnektoren, so dass von einer zügigen Umsetzbarkeit ausgegangen werden kann.

- Da das **FIM Privacy Management System** in Form einer neuen ARP Engine in die Shibboleth IDP-Software integriert wurde, erübrigt sich ihr Betrieb auf dedizierter Hardware. Es ist jedoch die Notwendigkeit eines **Policy Repository** zu berücksichtigen, das einen geeigneten LDAP-Server voraussetzt: Eine Möglichkeit stellt hierbei der IntegraTUM Administrationsverzeichnisdienst dar, dessen grundlegende Eignung für die darauf bereits zugreifenden Self Services und Administratorenwerkzeuge durch das Konzept der I&AM-Infrastruktur gewährleistet ist. Zur Realisierung müssten dabei das vom Server unterstützte LDAP-Schema entsprechend erweitert und der Directory Information Tree um einen Teilbaum für die in Abschnitt 5.3.3.1 vorgestellte ARP-Unterstruktur ergänzt werden. Wie in Abschnitt 7.3.2 erläutert wird, ist jedoch eine Nutzung des am LRZ notwendig werdenden ARP Repository vorzuziehen.

  In diesem Zusammenhang muss vorgesehen werden, dass die vorhandenen Self Services um entsprechende graphische Administrationswerkzeuge erweitert werden. Während diese für das in dieser Arbeit vorgestellte XACML-basierte ARP-Konzept noch nicht verfügbar sind, würde im Fall einer herkömmlichen Shibboleth-Installation ein Werkzeug wie ShARPE zum Einsatz kommen (vgl. Abschnitt 3.3.1.2).

- Der **Identitätsdatenkonverter** wird an der TUM benötigt, da sich die Schemata beim Einsatz der DFN-AAI bzw. bei der sehr engen Kooperation mit dem LRZ nicht nur im Umfang der ausgetauschten Daten deutlich unterscheiden, sondern intern ebenfalls ein abweichendes Datenmodell eingesetzt wird.

  Der optionale Einsatz des in dieser Arbeit eingeführten **Federation Schema Correlation Services** ist offensichtlich nur dann sinnvoll, wenn er von mehreren Organisationen genutzt wird; aufgrund der gemeinsamen Aufgabe, die an TUM und LRZ lokal vorliegenden Daten in das Format der DFN-AAI konvertieren zu müssen, wird im Folgenden der Einsatz des FSCS vorgesehen (siehe auch Abschnitt 7.3.3).

Abbildung 7.4 zeigt die Erweiterung der I&AM-Infrastruktur um diese IDP-spezifischen FIM-Komponenten (in der Abbildung in Fettschrift hervorgehoben).

Durch den Betrieb dieser FIM-Infrastruktur am LRZ ergibt sich die folgende Eingliederung in das IT Service Management:

- Die **Hochverfügbarkeit der FIM-Komponenten** wird durch Hardwareredundanz gewährleistet: Jeder Server ist doppelt vorhanden, wobei jede Hälfte eines Serverpaars über unterschiedliche Netzwerkkomponenten angebunden und aus verschiedenen Stromquellen gespeist wird. Eine noch höhere Redundanz wird im Rahmen des betrachteten Szenarios derzeit nicht benötigt.

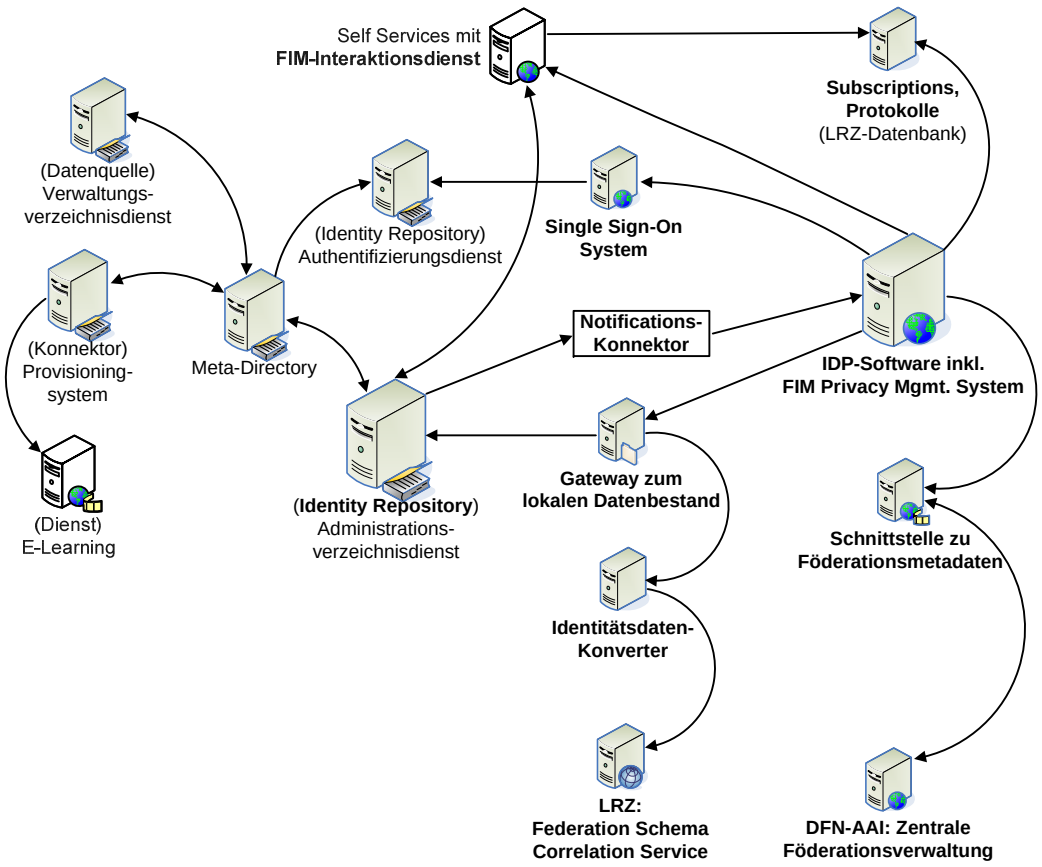


Abbildung 7.4.: Um IDP-spezifische Komponenten erweiterte FIM-Architektur für die TUM

- Alle Serversysteme sind in die **Software-Update-, Backup- und Systemmonitoring-Konzepte** des LRZ integriert, so dass keine Erweiterung der Systemmanagementinfrastruktur erforderlich wird.

- Im Rahmen des IntegraTUM I&AM-Systems wurde bereits eine Netzwerktopologie geschaffen, die Zonen für LRZ-internen, MWN-weiten bzw. weltweiten Zugang vorsieht, wobei auch die Möglichkeit gegeben ist, dass nur ausgehende Verbindungen zugelassen werden; somit können die FIM-Komponenten direkt den in Abschnitt 4.7.2.1 geforderten **Sicherheitszonen** zugeordnet werden, die wiederum im Rahmen des **Netzwerksicherheitsmonitorings** überwacht werden (siehe Abschnitt 7.5.3).

Auch für die Administration der FIM-Komponenten können die **Managementserver**, die mit dem I&AM-System eingeführt wurden, weiterverwendet und z. B. um XACML-Policyeditoren ergänzt werden; auf darüber hinausgehende Managementaspekte wie das Accounting und Billing von FIM-Transaktionen wird hier nicht eingegangen, da diese im Gesamtszenario vorläufig keine Rolle spielen bzw. die bereits vorhandenen, nicht FIM-spezifischen Mechanismen noch nicht ablösen sollen.

7.3.1.2. Architektur für die TUM als FIM Service Provider

Obwohl die TUM im vorliegenden Szenario lediglich für einen Dienst als Service Provider fungiert, liegt es nahe, dass externen Benutzern mittelfristig auch der Zugang zum TUM-Webportal und den TUM-Bibliotheksressourcen ermöglicht werden soll, um das E-Learning-Angebot um die von den beiden anderen Diensten gebotenen Collaboration- und Recherchemöglichkeiten zu erweitern. Somit ist von Anfang an eine **starke Integration der SP-seitigen FIM-Infrastruktur in das vorhandene I&AM-System** anzustreben; nachfolgend wird davon ausgegangen, dass die Komponente zur Auswertung von Attribute Acceptance Policies (AAPs) analog zu ARPs in die Shibboleth-SP-Software integriert werden kann und dass von der IDP- und der SP-Software wie in der Referenzarchitektur dargestellt eine gemeinsame Komponente zum Zugriff auf den lokalen Datenbestand genutzt wird (siehe Seite 282).

Der SP-seitig ebenfalls erforderliche Identitätsdatenkonverter und die Schnittstelle zu den Föderationsmetadaten sind bereits für die Rolle als Identity Provider vorgesehen und können ohne zusätzlichen Aufwand mitbenutzt werden.

Ein wesentlicher Aspekt bei der Umsetzung von FIM für das Learning Management System ist die Schaffung einer **dienstseitigen Schnittstelle zur SP-Software**: Während die notwendigen Benutzerattribute über das I&AM-System an die Dienste durchgereicht werden können, muss das Learning Management System zur Umsetzung des in Abschnitt 2.1.2.7 beschriebenen SP-first Use Cases um eine FIM-fähige Authentifizierungsvariante erweitert werden. Langfristig ist diesbezüglich insbesondere die Möglichkeit zur delegierten Autorisierung in Erwägung zu ziehen, bei der vom Identity Provider des Benutzers vorgegeben wird, welche E-Learning-Angebote genutzt werden dürfen bzw. sinnvoll in das eigene Curriculum integriert werden können. Aufgrund der Komplexität und der zum Teil großen Unterschiede einer Vielzahl von Prüfungsordnungen pro Hochschule sowie aufgrund der Heterogenität der Kursangebote kann diese technische Möglichkeit derzeit jedoch noch nicht mit angemessenem Aufwand ausgereizt werden.

Durch die Anpassung des Dienstes an die neue Authentifizierungsschnittstelle ergibt sich ohne zusätzlichen Aufwand die Möglichkeit zur **Nutzung des organisationsinternen Single Sign-On Systems**; sie ist im Hinblick auf FIM optional, bietet jedoch den Mehrwert eines durchgängigen organisationsinternen und -übergreifenden Single Sign-Ons.

Abbildung 7.5 zeigt die Erweiterung der FIM-Architektur der TUM um die SP-spezifischen Komponenten.

7.3.1.3. Externe Komponenten für die TUM als FIM Identity und Service Provider

Unter der in Abschnitt 7.2.3 getroffenen Annahme, dass das LRZ keine MWN-spezifische Föderationsverwaltung betreiben wird, reicht für die TUM als IDP und SP eine Anbindung an die Föderationsverwaltung der DFN-AAI aus.

Im Hinblick auf die Bereitstellung des E-Learning-Systems im Rahmen des VHB-Teilszenarios ist zu entscheiden, ob der von der DFN-AAI angebotene IDP Discovery Service beim Aufruf durch die TUM so parametrisiert werden kann, dass dem Benutzer lediglich eine Liste der VHB-Trägerhochschulen präsentiert wird. Dadurch würde diese möglichst übersichtlich gehalten und Benutzer anderer Hochschulen, deren Dienstnutzung selbst nach erfolgreicher

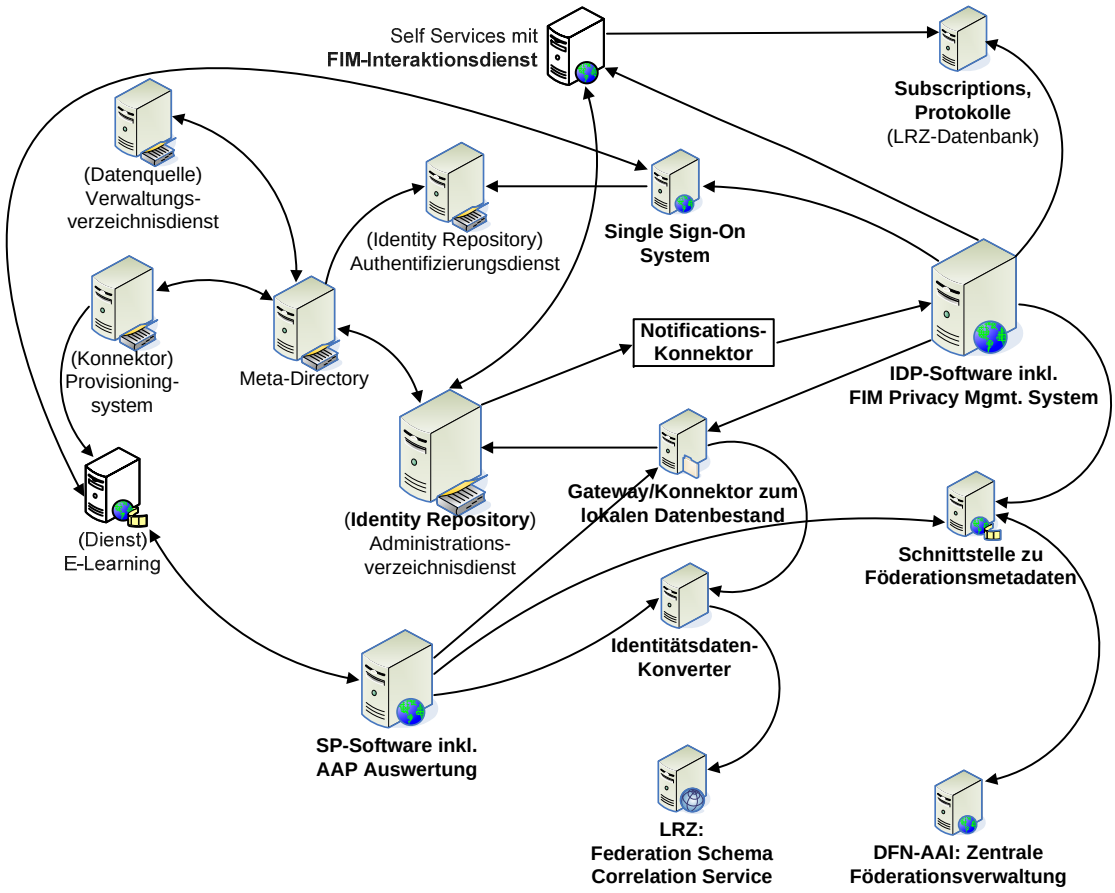


Abbildung 7.5.: Um SP-spezifische Komponenten erweiterte FIM-Architektur für die TUM

Authentifizierung an der fehlenden Autorisierung scheitern würde, könnten bereits frühzeitig abgewiesen werden.

Sofern dies nicht möglich sein sollte, aber gewünscht wird, muss alternativ ein SP-lokaler IDP Discovery Service vorgesehen werden. Zur Vereinfachung wird nachfolgend davon ausgegangen, dass die von der DFN-AAI bereitgestellten Dienste die erforderliche Flexibilität aufweisen.

7.3.2. Erweiterung der I&AM-Architektur des LRZ

Analog zu den Ausführungen für die TUM wird im Folgenden knapp auf die notwendigen Erweiterungen der I&AM-Architektur des LRZ um FIM-Komponenten eingegangen; Unterschiede ergeben sich vor allem bei den SP-spezifischen Aspekten, da die im Szenario betrachtete Dienstpalette breiter als an der TUM ist; zudem ist die parallele Teilnahme an mehreren Föderationen zu berücksichtigen.

Abbildung 7.6 zeigt die Ausgangssituation auf Basis des in Szenario 3 vorgestellten I&AM-Umfelds am LRZ in Anlehnung an die Referenzarchitektur aus Kapitel 4; es ist zu beach-

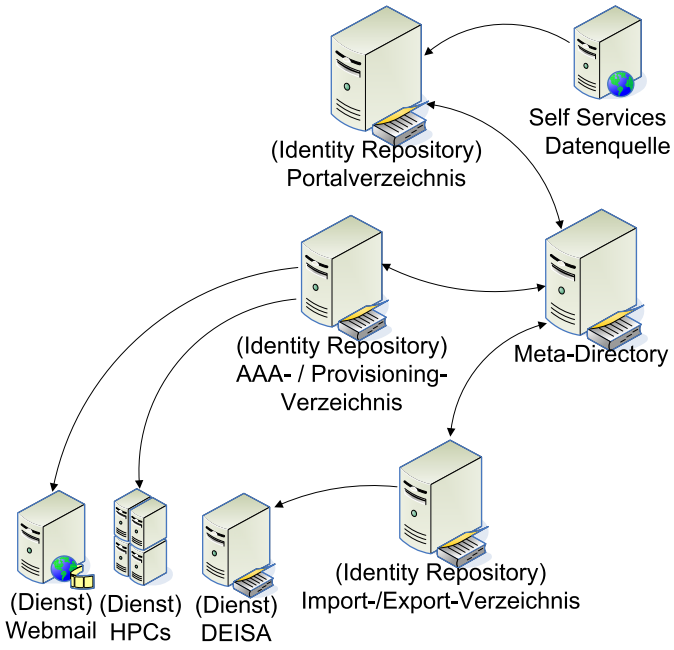


Abbildung 7.6.: I&AM-Architektur des LRZ in Analogie zur Referenzarchitektur

ten, dass aufgrund der Auslegung des LRZ Identity Management Webportals die den LRZ-Betreuern angebotenen Self Services gleichzeitig auch die primäre Datenquelle des Systems darstellen (vgl. Szenario 3).

7.3.2.1. Architektur für das LRZ als FIM Identity Provider

Wie an der TUM weist das LRZ Identity Management System die Eigenschaft auf, dass der Benutzerdatenbestand in mehr als einem Identity Repository vorgehalten wird, um die unterschiedlichen Anforderungen der lokalen Dienste erfüllen zu können. Da der Datenaustausch mit den Münchner Hochschulen seit jeher ein Ziel des LRZ Identity Management Projekts war, liegt mit dem so genannten **Import-/Export-Verzeichnisdienst** ein für die FIM-Anbindung sehr gut geeignetes **Identity Repository** vor.

Ebenfalls analog zur TUM fehlt am LRZ ein **Single Sign-On System**, das mindestens in Form eines webbasierten Authentifizierungsdienstes nachgerüstet werden muss; mit dem in Szenario 3 bereits erläuterten **Authentifizierungs- und Autorisierungsverzeichnisdienst** ist bereits ein für diesen Zweck geeigneter Datenbestand vorhanden, so dass wiederum die Einführung eines dazu passenden Webfrontends ausreichend ist.

Aufgrund der mit der TUM vergleichbaren Ausgangssituation ergeben sich die folgenden weiteren Aspekte bei der Konzeption der FIM-Architektur für das LRZ als Identity Provider:

- Die **IDP-Software**, die **Schnittstelle zu den Föderationsmetadaten** und der **Gateway zum lokalen Datenstand** sind als grundlegende FIM-Komponenten zwingend erforderlich. Im Unterschied zur TUM ergibt sich eine Anbindung an mehrere Födera-

tionsverwaltungen, die ohne Weiteres von *einer* Instanz der Schnittstelle zu den Föderationsmetadaten realisiert werden kann.

- Der **FIM-Interaktionsdienst** ist in das LRZ Self Service Portal zu integrieren. Diese Aufgabe wird dadurch erleichtert, dass das Portalframework im Rahmen einer Diplomarbeit zusammen mit dem I&AM-System des LRZ entwickelt und insbesondere auf eine modulare Erweiterbarkeit ausgelegt wurde (siehe [Ange06]).
- Die am LRZ bereits verfügbaren relationalen Datenbankmanagementsysteme können wie im Fall der TUM für die Speicherung der FIM-Datensubskriptionen durch die IDP-Software herangezogen werden. Zur Ausschöpfung der vollen FIM-Funktionalität ist wiederum der **Notifications-Konnektor** vorzusehen; da die I&AM-Systeme der TUM und des LRZ auf derselben Software basieren und somit dieselben Konnektorenframeworks verwenden, kann in beiden Fällen die gleiche Konnektorenimplementierung mit entsprechend unterschiedlicher Parametrisierung verwendet werden.
- Für das im Rahmen dieser Arbeit in Shibboleth integrierte **FIM Privacy Management System** wird abermals ein Policy Repository benötigt; im Unterschied zur oben beschriebenen Situation an der TUM stellt das I&AM-System des LRZ jedoch keinen dafür prädestiniert erscheinenden LDAP-Server zur Verfügung. Es bietet sich deshalb an, ein entsprechendes LDAP-basiertes ARP Repository einzuführen, dessen DIT-Struktur auf das Management von ARPs für verschiedene Organisationen ausgelegt ist, so dass sich daraus beispielsweise ein **ARP-Hosting-Dienst** entwickeln kann, der u. a. von der TUM genutzt wird.
- Aufgrund der Teilnahme an mehreren Föderationen mit unterschiedlichen und vom lokalen Schema abweichenden Datenmodellen wird auch am LRZ der **Identitätsdatenkonverter** benötigt. Auch hier kann von einem gewinnbringenden Einsatz des **Federation Schema Correlation Services** ausgegangen werden.

Abbildung 7.7 zeigt die Ergänzung der LRZ-I&AM-Infrastruktur um diese IDP-spezifischen FIM-Komponenten.

Für die Integration dieser Komponenten in das IT Service Management gelten die am Ende von Abschnitt 7.3.1.1 getroffenen Aussagen.

7.3.2.2. Architektur für das LRZ als FIM Service Provider

Durch die in Szenario 3 diskutierte Vielzahl an Diensten, die größtenteils nicht webbasiert sind, ergibt sich die Anforderung nach der Integration der FIM-Daten in das vorhandene I&AM-System sehr klar und ist einer vollständigen FIM-Anpassung jedes einzelnen Dienstes vorzuziehen; insbesondere ist auch eine Verarbeitung der Daten nicht nur durch die Dienste, sondern auch durch parallele und nachgelagerte Prozesse wie das Accounting und Billing notwendig. Die SP-Software mit der wie in Abschnitt 7.3.1.2 erläutert integrierten Komponente zur Auswertung von Attribute Acceptance Policies und der Konnektor zum lokalen I&AM-System sind somit unbedingt erforderlich.

Darüber hinaus ist eine Anpassung der Authentifizierungsbestandteile der vorhandenen webbasierten Dienste an das durch die Einführung des Single Sign-On Systems sowie die über FIM

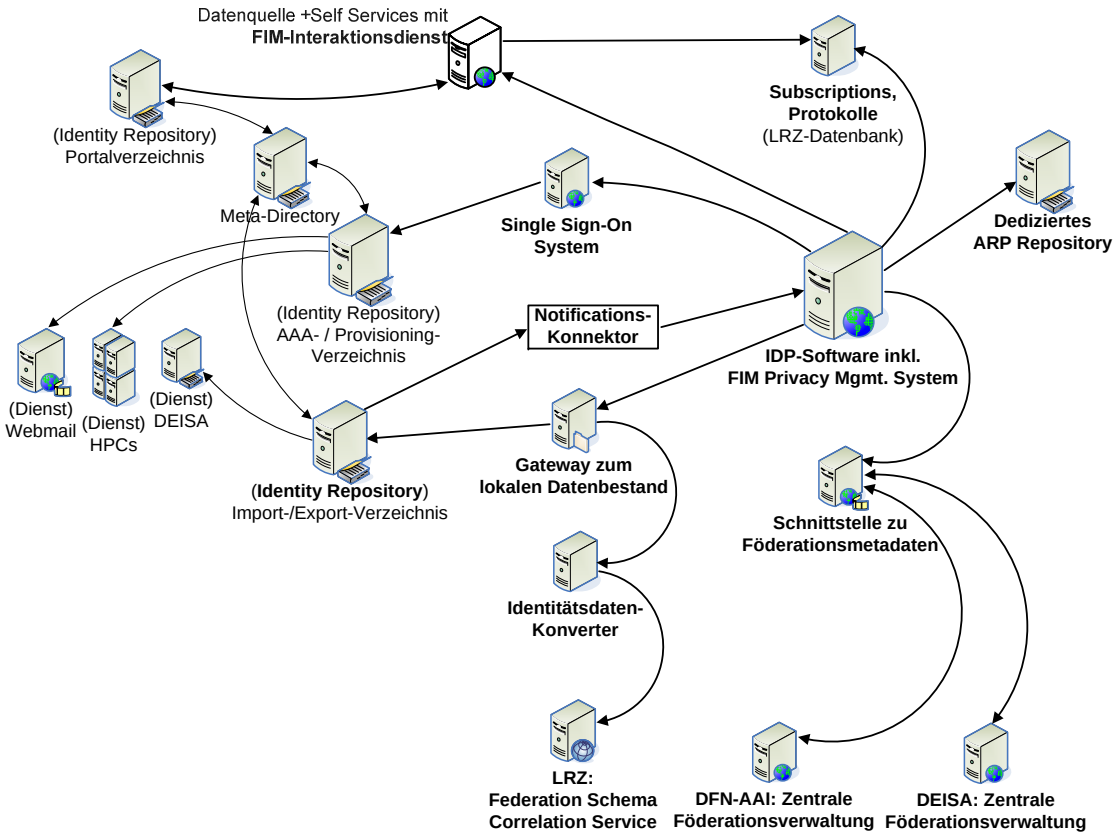


Abbildung 7.7.: Um IDP-spezifische Komponenten erweiterte FIM-Architektur für das LRZ

gebotenen Möglichkeiten anzustreben; so würde die Unterstützung der organisationsübergreifenden Authentifizierung bereits einen Mehrwert für die Kunden im MWN darstellen, wenn z. B. Dienste wie Webmail oder die Webschnittstelle zum persönlichen bzw. projektspezifischen Speicherplatz ohne wiederholte Passworteingabe genutzt werden könnten, ohne dass diese Dienste vollständig an FIM angepasst werden müssen, wie dies z. B. beim herkömmlichen Einsatz von Shibboleth der Fall wäre. Diese Umstellungen haben jedoch keinen direkten bzw. über die Schnittstelle der Dienste zur SP-Software hinausgehenden Einfluss auf die FIM-Architektur und werden hier nicht weiter ausgeführt.

Die gesamte Erweiterung der LRZ-FIM-Architektur ist in Abbildung 7.8 dargestellt.

7.3.2.3. Externe Komponenten für das LRZ als FIM Identity und Service Provider

Bedingt durch die Teilnahme an mehreren Föderationen müssen mehrere Föderationsverwaltungen angebunden werden; im betrachteten Szenario beschränkt sich dies auf die DFN-AAI sowie die DEISA-Föderation.

Die Nutzung der von diesen Föderationen bereitgestellten IDP Discovery Services unterliegt der in Abschnitt 4.4.10 diskutierten Problematik, dass der Service Provider beim Erstkontakt

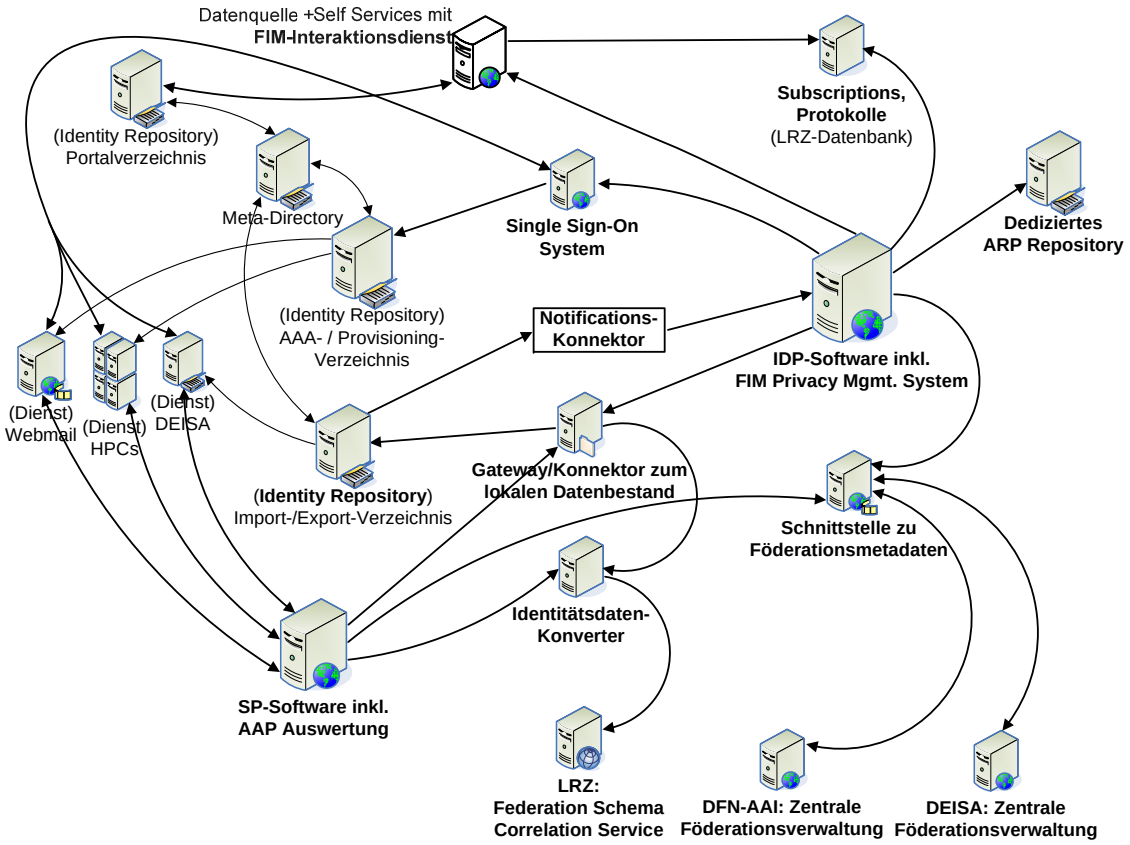


Abbildung 7.8.: Um SP-spezifische Komponenten erweiterte FIM-Architektur für das LRZ

mit dem noch nicht authentifizierten Benutzer im Rahmen des SP-first Use Cases im Allgemeinen nicht entscheiden kann, zu welchem IDP Discovery Service der Benutzer weitergeleitet werden soll. Im vorliegenden Fall kann dieses Problem umgangen werden, weil die Mengen der für DEISA bzw. im Rahmen der DFN-AAI angebotenen Dienste disjunkt sind: Bei der Nutzung eines DEISA-Dienstes kann der IDP Discovery Service der DEISA-Föderation, ansonsten derjenige der DFN-AAI verwendet werden. Mittelfristig ist diesbezüglich jedoch damit zu rechnen, dass ein **multi-federation-fähiger IDP Discovery Service** zum Einsatz kommen muss; ob dieser vom LRZ oder beispielsweise einem Verbund mehrerer Föderationen betrieben werden soll, kann erst zu einem späteren Zeitpunkt entschieden werden.

7.3.3. Synergien durch gemeinsame Komponentennutzung

Durch die auf Basis des Betriebs mehrerer zentraler IT-Dienste sehr enge Verzahnung der Geschäftsprozesse der TUM mit dem LRZ ist bei der parallelen Einführung von FIM für beide Organisationen zu analysieren, ob und wie die für FIM benötigten Komponenten gemeinsam genutzt werden können oder jeweils dediziert vorhanden sein müssen. Ausschlaggebend sind hierfür im Wesentlichen die folgenden Fragestellungen:

1. Ist die FIM-Komponente **technisch geeignet**, für mehr als eine Organisation eingesetzt

werden?

2. Können die Nutzer der FIM-Komponente aus **IT-Sicherheitsperspektive** voneinander isoliert werden bzw. keine ihnen nicht bereits anderweitig zugänglichen Informationen einsehen?

3. Reichen die eingesetzten **Ressourcen** wie z. B. die Serverhardware aus, um die Komponente für mehrere Organisationen zu betreiben?

Sofern diese Kriterien erfüllt werden, können durch die gemeinsame Nutzung einer Komponente insbesondere niedrigere Hardwareinvestitions- und Betriebskosten sowie reduzierte administrative Aufwände erreicht werden.

Im Folgenden wird davon ausgegangen, dass die zur Verfügung stehende Hardware für das an TUM und LRZ vorerst zu erwartende Aufkommen an FIM-Transaktionen vollkommen ausreicht und somit vorrangig die ersten beiden Fragestellungen zu untersuchen sind.

Für die in den Abschnitten 7.3.1 und 7.3.2 aufgeführten Komponenten bieten sich somit die folgenden Möglichkeiten:

- Das **Single Sign-On System** ist prinzipiell in der Lage, mehr als ein Identity Repository zur Authentifizierung eines Benutzers heranzuziehen und kann für eine beliebige Anzahl anzubindender Systeme konfiguriert werden. Da sich aus der erfolgreichen Authentifizierung **keine implizite Autorisierung** zur Nutzung von Diensten ableitet, kann das SSO-System auch aus Securityperspektive für beide Organisationen gemeinsam genutzt werden. Wie in Abschnitt 2.2.1.2 diskutiert wurde, handelt es sich bei der somit gemeinsamen Nutzung des SSO-Systems durch TUM und LRZ um eine aufgrund der organisatorischen und technischen Gegebenheiten mögliche Lösung für die organisationsübergreifende Authentifizierung, die jedoch im Allgemeinen nicht auf andere FIM-Szenarien übertragen werden kann. Im konkreten Szenario ergibt sich jedoch der aus Kundensicht wichtige Vorteil, dass TUM-seitige Benutzer *alle*, d. h. auch die vom LRZ betriebenen, IT-Dienste über *ein* SSO-System nutzen können und somit keine separate Authentifizierung an TUM- bzw. LRZ-Diensten erforderlich ist, selbst wenn noch nicht alle Dienste auf FIM umgestellt wurden, wodurch die Migrationsphase auch aus Kundenperspektive erleichtert wird.

- Der in Abschnitt 4.4.12 beschriebene **Identitätsdatenkonverter** sieht eine Parametrisierung von Konvertierungsaufrufen vor, die einen Einsatz für mehrere Organisationen ermöglicht. Es ist zu bedenken, dass ein Hosting des Identitätsdatenkonverters im Allgemeinen unerwünscht ist, damit die Nutzdaten und ggf. Detailinformationen zum lokalen Datenmodell keinen Dritten zugänglich gemacht werden. Im Fall der TUM gilt jedoch wiederum die Besonderheit, dass das gesamte I&AM-System bereits an das LRZ outgesourct wurde; somit bietet sich auch der Betrieb des Identitätsdatenkonverters durch das LRZ an.

  Beim damit eng verwobenen **Federation Schema Correlation Service** handelt es sich per Definition um einen gemeinsam zu nutzenden Dienst, der ebenfalls vom LRZ betrieben wird. Durch die partiell vorhandenen Parallelen zwischen den TUM- und LRZ-seitig eingesetzten Datenmodellen lässt sich der Administrationsaufwand beispielsweise

im Hinblick auf die Konvertierung in das föderationsweite Datenschema der DFN-AAI bereits kurzfristig reduzieren.

- Prinzipiell kann von beiden Organisationen auch die **Schnittstelle zu den Föderationsmetadaten** gemeinsam genutzt werden. Entscheidend hierfür ist, ob die Metadaten einer Föderation nur ihren Mitgliedern oder öffentlich zugänglich gemacht werden sollen. Da sowohl TUM als auch LRZ der DFN-AAI angehören, ist im Szenario somit zu entscheiden, ob die potentielle Einsichtnahme der TUM-spezifischen Systeme in die DEISA-Föderationsmetadaten ein aus Securityperspektive unerwünschtes Risiko darstellt. Da die versuchte Geheimhaltung von Föderationsmetadaten nur einen sehr schwachen Schutz darstellt (*„security by obscurity“*) und die Daten auch bereits TUM-seitigen DEISA-Nutzern Verfügung stehen, wird nachfolgend davon ausgegangen, dass gegen die gemeinsame Nutzung der Schnittstelle zu den Föderationsmetadaten keine Einwände bestehen.
- Für die **IDP-Software**, die **SP-Software** und den von diesen benötigten **Gateway zum lokalen Datenbestand** sind getrennte Instanzen für TUM und LRZ bereitzustellen:
  - Die in dieser Arbeit nicht modifizierten FIM-Protokolle sprechen die FIM-Komponenten verschiedener Organisationen über die verschiedenen, in den Föderationsmetadaten enthaltenen **Kommunikationsendpunkte** an, d. h. eine Differenzierung der angesprochenen Organisation ist nicht über die Nutz-, sondern nur über die Metadaten einer FIM-Kommunikation möglich. Die Bereitstellung eines solchen Kommunikationsendpunkts erfordert eine entsprechende Instanz der IDP- bzw. SP-Software.
  - Der Gateway zum lokalen Datenbestand unterstützt zwar mehrere lokale Identity Repositories einer Organisation, ist jedoch nicht auf den parallelen Einsatz durch mehrere Organisationen ausgelegt – in diesem Fall würde er als Alternative zu FIM einem organisationsübergreifenden virtuellen Verzeichnisdienst mit den in Abschnitt 2.2.1.2 diskutierten Problemen entsprechen, so dass eine derartige Lösung nicht angestrebt wurde, auch wenn sie in diesem speziellen Szenario eine praktikable Alternativlösung darstellen würde.

  Es bietet sich jedoch an, diese Instanzen aufgrund ihrer softwareseitig realisierten gegenseitigen Isolation und der erwarteten Auslastung jeweils auf gemeinsamer Serverhardware zu betreiben und somit auch den Administrationsaufwand z. B. für Backup und Betriebssystemaktualisierungen zu reduzieren.
- Wie in Abschnitt 7.3.2.1 beschrieben wurde, kann das vom LRZ betriebene Attribute Release Policy Repository auch von der TUM verwendet werden.

Zusammenfassend zeigt Abbildung 7.9 die aus der gemeinsamen Komponentennutzung resultierende FIM-Gesamtarchitektur für TUM und LRZ.

7.3.4. Grundlegende Aufwandsprognose

Um die mit der Einführung von FIM anfallenden Kosten grob abschätzen zu können, wird in diesem Abschnitt kurz auf die szenarienspezifischen Hard- und Softwarekosten eingegangen;

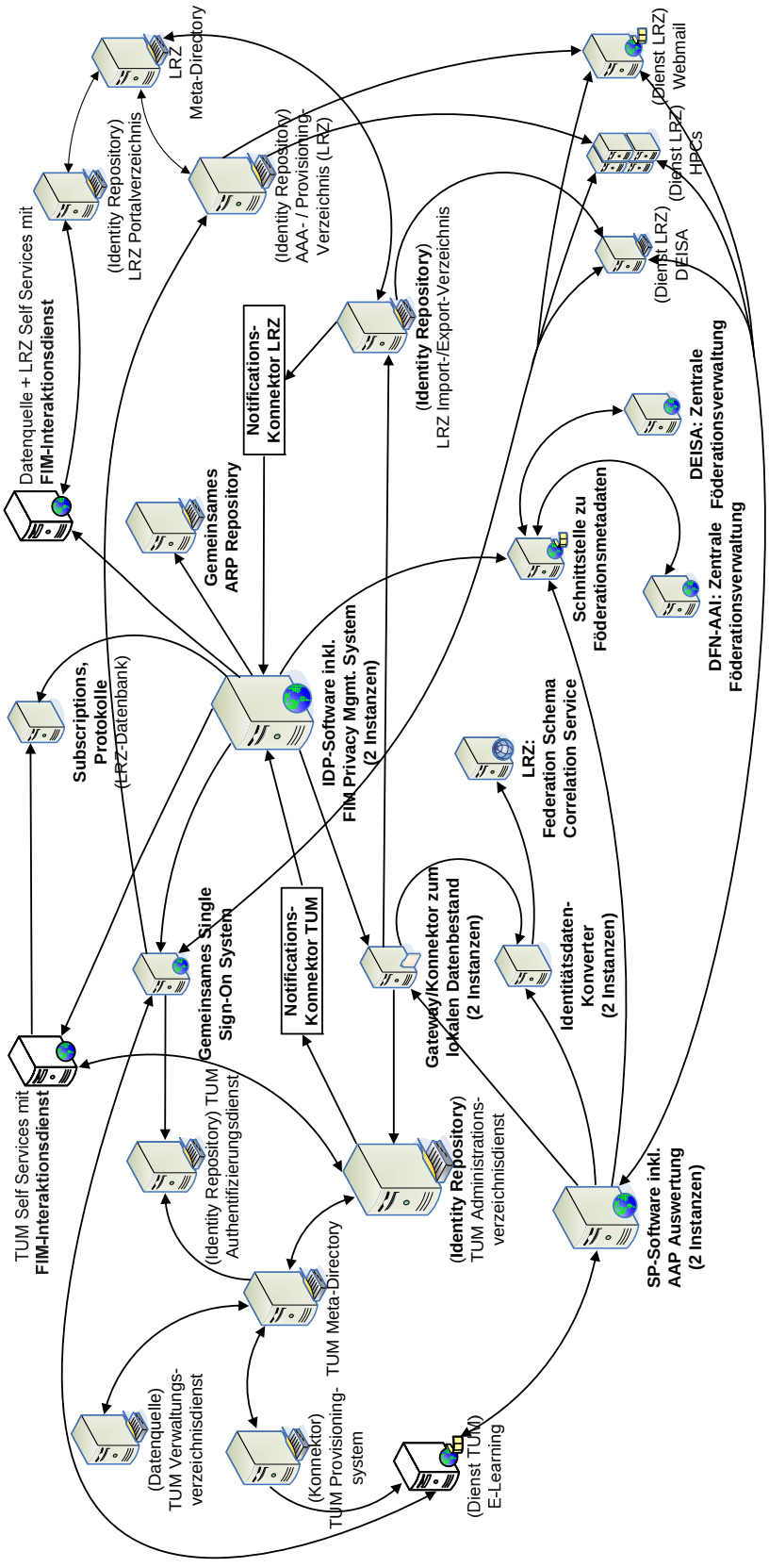


Abbildung 7.9.: FIM-Architektur für LRZ und TUM mit gemeinsamer Komponentennutzung

ferner wird der in den nächsten Abschnitten noch näher ausgeführte Personalaufwand knapp diskutiert.

Der **Hardwareaufwand** ergibt sich wie folgt aus der Notwendigkeit, die Hochverfügbarkeit sicherzustellen, und der Möglichkeit, mehrere FIM-Komponenten sinnvoll auf einem gemeinsamen Server betreiben zu können:

- Wie bereits in Abschnitt 7.2.2 dargelegt wurde, sollten die IDP-Software und die SP-Software auf jeweils dedizierte Server verteilt werden, da es sich um voneinander unabhängige Softwarepakete mit unterschiedlichen Nutzerkreisen handelt; auf den Maschinen für die IDP-Software wird wie in Abschnitt 7.3.1.1 diskutiert auch das SSO-System betrieben, um dieselbe Servlet-Container-Software verwenden zu können. Unter dem Aspekt der Hochverfügbarkeit ergibt sich somit der Bedarf für vier neue Maschinen.
- Die Schnittstelle zu den Föderationsmetadaten, der Gateway zum lokalen Datenbestand und der Identitätsdatenkonverter sind wie in Abschnitt 4.7.2.1 erläutert **unterschiedlichen Sicherheitszonentypen** zugeordnet und bei einer strikten Umsetzung somit auf verschiedenen Servern zu realisieren, woraus sich unter Berücksichtigung der Hochverfügbarkeit wiederum der Bedarf an sechs zusätzlichen Maschinen ergibt. Sofern der Schutzbedarf die dabei anfallenden Kosten nicht rechtfertigt, können die folgenden Alternativen in Erwägung gezogen werden:

  1. Die drei genannten Komponenten können **gemeinsam auf einer Maschine** betrieben werden, da der Ausfall jeder einzelnen Komponente vergleichbare Auswirkungen auf FIM-Transaktionen hat und davon ausgegangen werden kann, dass aktuelle Serverhardware durch diese Komponenten nicht vollständig ausgelastet wird. Zur Erhöhung der Ausfallsicherheit sollte wiederum auf eine zweite Maschine zurückgegriffen werden.
  2. Ebenso könnten die Komponenten **in die IDP- bzw. SP-Software integriert** werden; bei Shibboleth ist dies bereits der Fall. Es muss jedoch berücksichtigt werden, dass diese redundante Mehrfachinstallation den angestrebten Synergieeffekten entgegen wirkt und zu einem administrativen Mehraufwand führt; insbesondere müssen besondere Maßnahmen getroffen werden, um bestimmte Änderungsoperationen sehr zeitnah an allen vier Installationen (Instanzen der IDP- bzw. SP-Software für TUM bzw. LRZ) durchführen zu können.
  3. Sofern bereits andere geeignete Maschinen in entsprechenden Sicherheitszonen vorhanden sind, können diese FIM-Komponenten auf ihnen betrieben werden; hierzu bieten sich insbesondere Serversysteme an, die durch **Virtualisierung** mehrere Betriebssysteminstanzen parallel betreiben können, so dass eine Beeinflussung von bzw. durch andere Dienste ausgeschlossen werden kann. Bislang werden solche „virtuellen Maschinen“ am LRZ jedoch nur für Testumgebungen eingesetzt.

- Beim Federation Schema Correlation Service und dem ARP Repository handelt es sich um Dienste, die auch anderen Einrichtungen angeboten werden sollen, so dass der Betrieb auf dedizierten Maschinen mit entsprechender Ausfallsicherheit erfolgen sollte.
- Für die Subscriptions-Datenbasis wird das Datenbank-Hosting des LRZ gewählt; da das hierbei auftretende Datenvolumen sehr gering ist, muss auch keine Erweiterung der Hintergrundspeicher vorgesehen werden.

Es ist zu beachten, dass zur Minimierung der Hardwarekosten auf die Hochverfügbarkeit verzichtet und theoretisch auch die IDP- und SP-Softwareinstanzen auf einer gemeinsamen Serverhardware in Betrieb genommen werden könnten; in diesem Fall müssen jedoch beim Auftreten von Überlastsituationen Änderungen an der Anzahl der für FIM eingesetzten Maschinen und der Zuordnung von Diensten zu Maschinen in Kauf genommen werden, so dass von vornherein eine nachhaltige Umsetzung der Architektur anzustreben ist.

Die zusätzlich anfallenden **Kosten für die Inbetriebnahme**, z. B. durch die Vorbereitung der Räumlichkeiten und Netzwerkanschlüsse, und Aufwände für den Betrieb, beispielsweise Kosten für Strom und Wartungsverträge, unterscheiden sich nicht von anderen Diensten und werden hier nicht näher betrachtet.

Da es sich bei den FIM-Komponenten um Open Source Produkte handelt, fallen bei ihrer Einführung **keine Lizenzkosten** an. Auch zusätzliche Komponenten wie das Single Sign-On System und das ARP Repository stehen in dieser Form zur Verfügung; alternativ können auch kommerzielle Softwarekomponenten, die durch die für die I&AM-Systeme bereits vorhandenen Lizenzverträge abgedeckt werden, ohne Mehrkosten eingesetzt werden.

Bei den **Diensten**, die über FIM angeboten werden sollen, können hingegen **Kosten für die Anpassung** – beispielsweise ihrer Authentifizierungskomponenten – an die SP-Software anfallen. Insbesondere bei kommerziellen Systemen wie dem eingesetzten Learning Management System sind wie in Abschnitt 7.2.1 erwähnt entsprechende Verhandlungen mit den Herstellern zu führen. Die anfallenden Entwicklungskosten hängen somit u. a. vom Eigeninteresse des Herstellers und der Anzahl weiterer an einer entsprechenden Anpassung der Software interessierter anderer Einrichtungen ab und müssen pro Dienst ermittelt werden. Die bisherigen Erfahrungen mit der Anpassung proprietärer Software an I&AM-Systeme zeigt, dass hierbei zwar nur mit moderaten Kosten zu rechnen ist, die **Wartezeit bis zur Einsatzfähigkeit** aufgrund der typischen Softwarereleasezyklen aber häufig mehr als ein Jahr beträgt und geeignet berücksichtigt werden muss.

Der zu erwartende **Personalaufwand** hängt von einer Vielzahl von Faktoren wie den Vorkenntnissen und Erfahrungen der Mitarbeiter ab, die im Rahmen dieses Anwendungsbeispiels nicht im Detail untersucht werden können. Es wird deshalb davon ausgegangen, dass die Umsetzung der FIM-Architektur von Mitarbeitern mit guten Vorkenntnissen im Bereich I&AM, aber ohne praktische Erfahrung mit FIM-Software und ohne Unterstützung durch kostenintensives externes Consulting durchgeführt werden soll. In Abschnitt 7.4 wird zu jedem der durchzuführenden Migrationsschritte eine knappe **Aufwandsabschätzung** angegeben. Auf weitere projektplanungsrelevante Aspekte wie Urlaubsphasen, Erstellen von Dokumentationen und die Vorbereitung und Durchführung von Reviews wird nicht näher eingegangen; insgesamt kann jedoch wie in Abschnitt 7.4 erläutert im vorliegenden Umfeld eine **Implementierungsdauer von ca. einem Jahr** als realistisch angenommen werden, die in einem durchaus positiven Verhältnis zu den auf mehrere Jahre ausgelegten I&AM-Projekten steht.

Im Hinblick auf den dauerhaften Betrieb und auch in Vertretungssituationen angemessene Reaktionszeiten sind LRZ-seitig mindestens zwei Administratoren zu schulen und in die konkrete FIM-Infrastruktur einzuweisen. Während die eingesetzten FIM-Komponenten im Regelbetrieb keinerlei Eingriffe erfordern, hängt es u. a. von der Anzahl der Fehlerfälle insbesondere kurz nach Einführung von FIM, der Frequenz der in Abschnitt 7.5 diskutierten Änderungen im Rahmen des Change Managements sowie der Rate des durch den First Level Support vollständig bearbeiteten Incidentmeldungen ab, welcher Aufwand für den Betrieb

der aufgebauten FIM-Infrastruktur notwendig wird.

Für das Gesamtszenario, in dem auch die Arbeiten an den I&AM-Systemen der betrachteten Organisationen noch nicht abgeschlossen sind, ist somit anzustreben, die nach Abschluss der beiden I&AM-Projekte für den Dauerbetrieb zu reduzierende Personalkapazität so zu dimensionieren, dass dieser Personenkreis auch den Betrieb der FIM-Infrastruktur übernehmen kann.

7.4. Schritte zur Realisierung der Zielarchitektur

Die nachfolgenden Ausführungen orientieren sich sehr eng an der in Abschnitt 4.6 spezifizierten Migrationsmethodik; dabei wird die Besonderheit der parallelen Einführung von FIM in zwei Organisationen berücksichtigt und grob auf den jeweils erforderlichen Aufwand eingegangen.

Die Umsetzung der Zielarchitektur lässt sich in den nachfolgendend beschriebenen Schritten realisieren, wobei auf sich zwangsweise ergebende zeitliche Abhängigkeiten explizit eingegangen wird:

1. Für das benötigte Single Sign-On System ist eine Produktentscheidung zu treffen; da an TUM und LRZ weder z. B. Smartcards noch biometrische Authentifizierungsverfahren flächendeckend im Einsatz sind, reduziert sich die zu treffende Auswahl auf webbasierte Dienste zur Überprüfung eingegebener Benutzername-/Passwortkombinationen. Wie in Abschnitt 7.3.1.1 diskutiert wurde, wird diese Funktionalität von Servlet-Containern geboten, die auch zum Betrieb von Shibboleth erforderlich sind. Die Inbetriebnahme des SSO-Systems dient somit als Nebeneffekt auch dem Erfahrungsgewinn mit der für den späteren Betrieb der IDP-Software benötigten Grundlage.

   Die **Anbindung des SSO-Systems an die jeweiligen Identity Repositories** von TUM und LRZ stellt einen nur geringen Konfigurationsaufwand dar; für die Einarbeitung in die Administration der Software und erste Tests ist eine Dauer von zwei Wochen zu veranschlagen. Mit der **Anbindung von Diensten an das SSO-System** kann erst im Anschluss begonnen werden; um den laufenden Betrieb der Dienste nicht zu gefährden, müssen – sofern diese noch nicht vorhanden sind – Testumgebungen aufgebaut werden, in denen eine Umstellung des dienstspezifischen Authentifizierungsverfahrens auf das SSO-System vorab erprobt werden kann. Zusammen mit den Vorbereitungen für die Änderung der Produktivumgebung und ggf. in Problemfällen notwendig werdenden Rücksprachen mit den Softwareherstellern kann von einer durchschnittlichen Dauer von mindestens vier Wochen pro umzustellendem Dienst ausgegangen werden, wobei die betroffenen Dienste parallel bearbeitet werden können.

2. Im nächsten Schritt ist mit der Arbeit an den **Self Services** zu beginnen; wie die anderen Dienste sind sie zunächst auf die Verwendung des Single Sign-On Systems umzustellen. Ferner müssen sie u. a. durch die Integration eines Editors für benutzerspezifische Attribute Release Policies um FIM-spezifische Funktionen erweitert werden. Sowohl für die Self Services der TUM als auch für diejenigen des LRZ stehen bereits Test- und Entwicklungsumgebungen zur Verfügung, die hierfür genutzt werden können.

Obwohl für Single Sign-On Systeme standardisierte Schnittstellen und z. B. für das Pflegen von Shibboleth ARPs vorgefertigte Softwarepakete zur Verfügung stehen, hat sich sowohl TUM- als auch LRZ-seitig gezeigt, dass der Aufwand für eine Erweiterung der Self Services aufgrund der Komplexität der zugrundeliegenden Portalframeworks und der Notwendigkeit für umfassende Tests und für die Erstellung für Benutzer geeigneter Dokumentationen nicht unterschätzt werden darf; deshalb werden jeweils 4 Wochen veranschlagt, wobei die Self Services beider Einrichtungen parallel bearbeitet werden können.

3. Auf Basis der in Abschnitt 4.5.1 diskutierten gegenseitigen Abhängigkeiten der IDP-spezifischen FIM-Komponenten folgt die **Vorbereitung des FIM Privacy Management Systems**; da die Auswertung von XACML-ARPs in Shibboleth integriert wurde, verschiebt sich die Installation dieser Komponente bis Schritt 9. Es kann jedoch bereits mit der Kodierung der IDP-weiten Attribute Release Policies in XACML begonnen werden: Wie in Abschnitt 7.2.1 erläutert wurde, ist hierzu die Abstimmung mit den zuständigen Datenschutzbeauftragten und das Durchlaufen entsprechender Genehmigungsverfahren notwendig, die bis zur Produktivführung abgeschlossen sein müssen. Auf nähere Details zur Konfiguration der ARPs wird in Abschnitt 7.5.1 eingegangen. Durch den erhöhten Koordinationsaufwand mit den Datenschutzbeauftragten und den Dienstanbietern in den Föderationen ist für die betrachteten Teilszenarien mit einem projektseitigen Arbeitsaufwand von zwei Personenwochen über eine Dauer von einem Monat zu rechnen.

   Analog dazu kann zusammen mit den lokalen Dienstadministratoren begonnen werden, Attribute Acceptance Policies für die angebotenen Dienste zu formulieren. Durch die Verwendung der SP-Software ergeben sich neue Datenakquisitions- und Verarbeitungsprozesse, die mit den Datenschutzbeauftragten und zum Teil mit den anderen Föderationsteilnehmern abzustimmen sind. Es ist von einem mit dem für die initiale ARP-Erstellung vergleichbaren Aufwand auszugehen.

   In beiden Fällen können die bereits vorhandenen Testumgebungen zur Veranschaulichung und für erste Überprüfungen der korrekten Funktionsweise herangezogen werden; für die Zusammenstellung von Testdatensätzen und die **Automatisierung der Tests** muss mit einem Aufwand von mindestens einer Woche gerechnet werden, da hierfür noch keine Standardwerkzeuge existieren.

4. Zur Vorbereitung der nächsten Schritte ist der **Federation Schema Correlation Service** in Betrieb zu nehmen. Da er vorerst nur von TUM und LRZ genutzt werden soll, reduziert sich der initiale Konfigurationsaufwand auf ein Minimum, so dass das System innerhalb einer Woche bereitstehen und getestet sein sollte.

5. Da die föderationsweiten Datenmodelle der DFN-AAI und der DEISA-Föderation bereits bekannt sind, kann mit der **Implementierung der Konvertierungsregeln** für die beiden lokalen LDAP-Schemata in XSLT begonnen werden. Vergleichbare Aufgabenstellungen in den lokalen I&AM-Systemen haben gezeigt, dass hierfür TUM- und LRZ-seitig mit einem Aufwand von jeweils zwei Wochen ausgegangen werden kann. Dadurch, dass es sich um den ersten Einsatz des Federation Schema Correlation Services handelt, ist jedoch anzunehmen, dass die durch ihn ermöglichte Aufwandsersparnis noch nicht auf Anhieb ausgeschöpft werden kann; zusammen mit einer Revisionsphase, in der

die Nutzung des FSCS forciert wird, ist somit von einem Aufwand von insgesamt sechs Wochen auszugehen.

6. Im Anschluss an die Vorbereitung des Identitätsdatenkonverters können die beiden Instanzen des **Gateways zum lokalen Datenbestand** in Betrieb genommen werden. Der Aufwand hierfür ist marginal, da sich die Konfiguration auf das Festlegen der Zugangsdaten zu den anderen Komponenten beschränkt; insbesondere sind der Zugang zu den beiden Identity Repositories zu ermöglichen und einfache LDAP-Suchfilter zu definieren, die ein Auslesen des Benutzerdatensatzes bei gegebenem Benutzeridentifikator ermöglichen. Zusammen mit Tests dieser Konfiguration ist von einem Gesamtaufwand von weniger als einer Woche auszugehen.

7. Für die beiden Identity und Service Provider muss die **Aufnahme in die jeweiligen Föderationen** beantragt werden. Hierzu sind vorab die DNS-Namen und IP-Adressen der beiden für die IDP- und SP-Software eingesetzten Maschinen festzulegen und entsprechende **Serverzertifikate** zu beantragen. Bei reibungslosem Ablauf sind diese Vorgänge innerhalb einer Woche abschließbar.

   Durch die Aufnahme in die Föderationen wird der **Zugang zu den Föderationsmetadaten** ermöglichst, so dass die entsprechende Schnittstellenkomponente in Betrieb genommen werden kann. Zwar ist der Konfigurationsaufwand hierfür minimal, es sind jedoch einerseits die Schnittstellen zum Einspielen eigener Metadatenänderungen zu testen und andererseits die Mechanismen zur lokalen Umsetzung der föderationsweiten Policies bereitzustellen; wie in Abschnitt 5.3.4.2 erläutert wurde, ist hierzu beispielsweise ein **XSLT-Stylesheet zur Policytransformation** zu implementieren, das mit dem föderationsweiten und TUM- bzw. LRZ-seitig lokalen Datenmodell parametrisiert werden muss. Hierfür ist mit einer weiteren Woche für Implementierung und Tests zu rechnen.

   Es ist zu beachten, dass in dieser Phase – sofern dies von der Föderationsverwaltung unterstützt wird – noch nicht die vollständigen Metadaten von TUM und LRZ in die jeweiligen Föderationsmetadaten aufgenommen werden sollten, damit potentiell interessierte Benutzer nicht mit der noch nicht funktionsfähigen Infrastruktur in Kontakt kommen. Das Einspielen der produktiven Metadaten erfolgt erst in Schritt 10.

8. Zur Vorbereitung der Inbetriebnahme der IDP-Software sind die vom LRZ gehosteten **Subscriptions-Datenbanken** vorzubereiten. Nach der üblichen kurzen Bereitstellungszeit des Datenbankzugangs ist lediglich das benötigte Datenbankschema einzuspielen, da Tests erst im Zusammenspiel mit der IDP-Software durchgeführt werden können, so dass der projektseitige Aufwand für diesen Schritt vernachlässigt werden kann.

9. Als wichtigster Schritt zur Bereitstellung der Funktionalität als Identity Provider können nun die beiden Instanzen der **IDP-Software installiert und konfiguriert** werden. Da von den in Abschnitt 4.4.1.1 diskutierten komponentenspezifischen Funktionen wie dem Accounting von FIM-Transaktionen im vorliegenden Szenario vorerst kein Gebrauch gemacht werden soll, reduziert sich die Konfiguration auf die Integration mit den anderen FIM-Komponenten durch die Spezifikation der jeweils zu verwendenden Kommunikationsendpunkte, die zu diesem Zeitpunkt mit Ausnahme des in Schritt 15 eingeführten Notifications-Konnektors bereits vollständig bekannt sind.

Da die Konfiguration von Shibboleth wie in Abschnitt 6.3 erläutert auch bei vorab bekannten Parametern nicht trivial ist und komplexe Fehleranalysen erfordern kann, ist von einem Zeitaufwand von zwei Wochen bis zur Fertigstellung inklusive der Durchführung erster grundlegender Tests auszugehen.

10. Nach der Inbetriebnahme der IDP-Software sind die **TUM- und LRZ-spezifischen Föderationsmetadaten** zu aktualisieren, so dass mit föderationsweiten Tests begonnen werden kann; dabei sind insbesondere die folgenden Funktionen zu verifizieren:

    - Können TUM und LRZ in den Listen der föderationsweiten IDP Discovery Services ausgewählt werden und resultiert daraus eine korrekte Weiterleitung des Benutzers zum lokalen Single Sign-On Service?
    - Funktionieren die vorkonfigurierten föderations- und IDP-weiten Attribute Release Policies wie erwartet?
    - Können die Dienste der an den Föderationen beteiligten Service Provider im vorgesehenen Umfang genutzt werden?
    - Werden die Benutzerattribute bei den Diensten im z. B. nach dem föderationsweiten Datenschema korrekten Format angezeigt?

    Diese Tests sind mindestens über einen Zeitraum von mehreren Tagen zu wiederholen und, sofern dafür geeignete Werkzeuge zur Verfügung stehen, möglichst zu automatisieren und auch im Betrieb regelmäßig durchzuführen. Bei Problemen sind Rücksprachen mit der Föderationsverwaltung bzw. einzelnen Service Providern erforderlich. Bei korrekter Funktionalität kann ein Testzeitraum von einer Woche als ausreichend angesehen werden, wobei sich mehrere Personen an den Tests beteiligen sollten.

11. Nach Abschluss der Tests der IDP-Software kann die für die Rolle als **Identity Provider** benötigte FIM-Infrastruktur in den **Produktionsbetrieb** überführt werden. Hierzu sind die entsprechenden neuen Funktionen der Self Services für den Benutzerbetrieb freizugeben und die lokalen Benutzer über die neuen Möglichkeiten zu informieren. Dieser Schritt ist im Rahmen des Change Managements insbesondere mit dem Service Desk zu koordinieren, da in den ersten Wochen nach Produktivführung mit einer besonders hohen Anzahl von **Supportanfragen**, für die dem First Level Support noch keine Lösungen bekannt sind, zu rechnen ist. Entsprechend sind auch im Second Level Support entsprechende Ressourcen für die Bearbeitung von Incidentmeldungen und Problemen vorzusehen, die Weiterentwicklungen in den folgenden Schritten verzögern können. Insgesamt wird ein Aufwand von zwei Wochen veranschlagt.

12. Dem IDP-seitigen Vorgehen entsprechend sind die **TUM- und LRZ-seitigen Instanzen der SP-Software** zu konfigurieren; hierfür gelten zur IDP-Software analoge Aussagen und es ist wiederum mit einem Aufwand von zwei Wochen zu rechnen. Dieser Schritt ist erst dann sinnvoll, wenn die lokalen Dienste unabhängig von ihrer direkten FIM-Fähigkeit auf die Einspeisung externer Benutzerdatensätze vorbereitet sind; im DEISA-Teilszenario ist dies von Anfang an der Fall.

13. Analog zur IDP-Software werden nach Bereitstellung der SP-Software Tests im föderationsweiten Kontext fällig, für die zunächst eine Aktualisierung der Föderationsmetadaten durchzuführen ist. Die prinzipielle Funktionsweise kann im Zusammenspiel mit

den lokalen Identity Providern überprüft werden. Die Verifikation der korrekten Datenkonvertierung setzt das Zusammenspiel mit eventuell in der Föderation vorhandenen Test-IDPs sowie die stichprobenartige Mitwirkung anderer Identity Provider voraus. Auch diese Tests sollten über einen Zeitraum von mehreren Tagen durchgeführt und möglichst automatisiert werden, so dass von einem Aufwand von einer Woche auszugehen ist.

14. Die Authentifizierungskomponenten der bereits an FIM angepassten Dienste sind auf die Möglichkeit zur Verwendung der SP-Software umzustellen. Da davon ausgegangen werden kann, dass im Rahmen der Weiterentwicklung der Dienste bereits ausführliche Tests vorgenommen wurden, besteht der primäre Aufwand im Change Management und der Koordination des Umstellungstermins, der auch mit den potentiellen externen Kunden abzusprechen ist, wovon jedoch die FIM-Projektgruppe nur am Rand betroffen ist.

15. Die **Implementierung des Notifications-Konnektors** rundet die Einführung der FIM-Komponenten ab; da von seiner Funktionalität in den betrachteten Teilszenarien vorerst noch kein Gebrauch gemacht wird, nachdem diese Komponente erst flächendeckend bei allen Föderationsteilnehmern eingeführt werden muss und die bei Shibboleth noch fehlende Unterstützung durch die IDP-Software erfordert, ist diese Aktivität nicht zu priorisieren. Wiederum auf Basis der bisherigen Konnektorenimplementierungen kann davon ausgegangen werden, dass für die Programmierung und erste Tests ein Aufwand von zwei Wochen anzusetzen ist; da TUM und LRZ dasselbe I&AM-Produkt einsetzen, ist nur eine einmalige Implementierung mit entsprechender Parametrisierung für beide Organisationen notwendig.

Der geschätzte Aufwand beträgt somit in Summe 35 Wochen bzw. knapp neun Monate. Da sich durch Fehlersituationen, deren Analyse durch die bislang fehlende Betriebserfahrung erschwert wird, nicht zu vernachlässigende Verzögerungen ergeben können und durch die Notwendigkeit zur Zusammenarbeit von Personen aus verschiedensten Bereichen Terminkonflikte wahrscheinlich sind, sollte realistisch von einer Dauer von ca. 12 Monaten ausgegangen werden.

Mit der Überführung der IDP- und SP-Software in den Benutzerbetrieb beginnt die Produktionsphase, die Gegenstand des nächsten Abschnitts ist.

7.5. Operative Aspekte des FIM-Einsatzes an TUM und LRZ

Nach der stark technisch geprägten Phase der Einführung der FIM-Komponenten folgt die Betriebsphase; aufgrund der weitreichenden Automatisierung in den einzelnen FIM-Komponenten zeichnet sie sich dadurch aus, dass administrative Eingriffe primär nur in unerwarteten Fehlersituationen sowie im Rahmen des Change Managements notwendig werden.

Den in dieser Arbeit vorgestellten Konzepten folgend wird die Integration in die IT Service Management Geschäftsprozesse nachfolgend an den Beispielen des Change Managements und des Security Managements veranschaulicht, nachdem ein Überblick über die Ausgangssituation bei der Konfiguration der verwendeten FIM-Komponenten gegeben wurde.

7.5.1. Grundlegende Konfiguration der FIM-Werkzeuge

Die Konfiguration der FIM-Komponenten weist die folgende für das spätere Change Management wichtige Ausgangssituation auf:

- Der **Federation Schema Correlation Service** bzw. die eingesetzten **Identitätsdatenkonverter** verfügen über Regelwerke zur Konvertierung der TUM- und LRZ-seitig lokalen Benutzerdaten in die von der DFN-AAI bzw. der DEISA-Föderation benötigten Formate und werden auch nur von diesen Einrichtungen benutzt. Hierbei existieren partielle Überlappungen hinsichtlich der TUM- bzw. LRZ-seitig eingesetzten Konvertierungsregeln, den Großteil bilden jedoch dedizierte XSLT-Stylesheets.
- Die **Attribute Release Policies** sind ebenfalls auf die beiden betrachteten Föderationen und das Zusammenspiel zwischen TUM und LRZ ausgelegt:
  - An DEISA Service Provider werden Attribute im Umfang des vorher verwendeten DEISA-LDAP-Schemas übermittelt.
  - Im Rahmen der DFN-AAI ist zwischen verschiedenen **Klassen von Service Providern** zu unterscheiden:
    * Sofern keine der nachfolgenden Regelungen zutrifft, werden lediglich Authentifizierungsbestätigungen, aber keine allgemeinen Attributsauskünfte ausgestellt.
    * Der hochschulübergreifende Zugriff auf Bibliotheksressourcen erfolgt im Allgemeinen pseudonymisiert und delegiert autorisiert, d. h. es werden vom Identity Provider lediglich ein eindeutiger Benutzeridentifikator, der nicht aus den Stammdaten der Person abgeleitet, sondern randomisiert erzeugt wird, und ein Attribut mit Angaben über Berechtigungen übermittelt; die Wertemenge für Berechtigungsangaben ist dabei DFN-AAI-weit festgelegt und kann bei Bedarf SP-spezifisch ergänzt werden.
    * Für die Nutzung des DFN-AAI Angebots zum Download lizensierter Software ist darüber hinaus die Übermittlung der E-Mail-Adresse des Benutzers erforderlich, an die individuelle Lizenzschlüssel geschickt werden können.
    * Um die E-Learning-Systeme anderer Hochschulen nutzen zu können, sind wie in Szenario 5 beschrieben die Stammdaten des Benutzers und studiengangsspezifische Informationen bereitzustellen.
    * Darüber hinaus können individuelle Absprachen mit einzelnen Service Providern getroffen werden; beispielsweise kann im Rahmen der von zwei Hochschulen gemeinsam durchgeführten Studiengänge eine komplette Offenlegung des Benutzerprofils erforderlich sein.
      Eine dieser Kategorie entsprechende Regelung ist auch für Mitglieder der TUM hinsichtlich ihrer Nutzung von LRZ-Diensten zu treffen.
- Komplementär zu den ARPs wird über die **Attribute Acceptance Policies** sichergestellt, dass
  - das LRZ alle über TUM-seitige Benutzer zur Diensterbringung relevanten Attribute erhält,

  - dem E-Learning System der TUM alle benötigten Stammdaten und Studiengangsinformationen vorliegen, wobei auch hier wiederum zwischen Angeboten im Rahmen des VHB-Teilszenarios und gemeinsamen Studiengängen mit anderen Hochschulen unterschieden werden kann.

- In die **Metadaten** der beiden angebundenen Föderationen wurden die Informationen über die beiden Instanzen der IDP- und SP-Software mit ihren jeweiligen Serverzertifikaten eingepflegt.

Die anderen Konfigurationsoptionen der im Beispiel betrachteten Komponenten beziehen sich in erster Linie auf deren interne Kommunikationsbeziehungen sowie die beispielsweise den Benutzern angezeigten Hilfetexte und unterliegen somit keinen FIM-spezifischen Änderungen. Im folgenden Abschnitt werden im Rahmen des Change Managements zu planende Modifikationen u. a. an den oben erläuterten Konfigurationsbestandteilen untersucht.

7.5.2. FIM-spezifisches Change Management an TUM und LRZ

Prinzipiell gelten für das Anwendungsbeispiel alle in Abschnitt 4.8 zum Change Management getroffenen Aussagen; aus diesem Grund wird nachfolgend nur auf ausgewählte Aspekte eingegangen, die für die betrachteten Teilszenarien charakteristisch sind.

Die DFN-AAI setzt das in Abschnitt 4.1.2 diskutierte Ziel einer Föderation, nicht nur für genau einen Zweck geschaffen zu sein, im Gegensatz beispielsweise zur (fiktiven) DEISA-Föderation bereits gut um. Hieraus ergibt sich jedoch zwangsweise, dass auf **Änderungen an der Föderationszusammensetzung** in den folgenden Situationen lokal reagiert werden muss:

- Beim **Hinzukommen neuer Service Provider** zur DFN-AAI ist zu untersuchen, ob die somit neu angebotenen Dienste relevant für die lokalen Benutzer sind. Ist dies der Fall, so muss geklärt werden, ob

  - über die Teilnahme an der DFN-AAI hinaus ein bilateraler Vertrag mit dem Service Provider zu schließen ist.
  - eine dienstespezifische Verfahrensgenehmigung erforderlich wird, die mit den lokalen Datenschutzbeauftragten zu koordinieren ist.
  - die vorhandenen IDP-weiten Attribute Release Policies um Vorgaben für Datenfreigaben an den neuen Service Provider zu erweitern sind; hierbei ist wiederum zu beachten, dass die Benutzer über diese Änderung informiert werden müssen, d. h. die neuen Regeln sind nicht nur in Form von ARPs zu kodieren, sondern auch in Prosa zu formulieren.

  Diese Aktionen sind im Allgemeinen vom lokalen Change Advisory Board zu genehmigen, können in bestimmten Fällen wie beispielsweise dem sukzessiven Hinzukommen zahlreicher Hochschulen mit E-Learning-Angeboten aber auch als *pre-authorized changes* definiert werden, deren Umsetzung und Dokumentation den fachlich Zuständigen überlassen bleibt.

- Für das **Hinzukommen neuer Identity Provider** ist ein Prozess zu definieren, wie diesen die Nutzung des TUM Learning Management Systems zu erlauben ist. Im einfachsten Fall kann über die Attribute Acceptance Policies gesteuert werden, dass der Dienst von Nutzern aller Identity Provider in Anspruch genommen werden darf; andernfalls müssen die AAPs nach Eingang und Genehmigung eines entsprechenden Antrags des neuen IDPs um explizite Angaben für diesen erweitert werden, um seine Nutzer zuzulassen.

- Beim **Ausscheiden von Föderationsmitgliedern** ist entsprechend zu prüfen, ob und welche bilateralen Verträge dadurch aufgelöst werden müssen oder welche technischen Alternativen zur Weiterführung des FIM-basierten Datenaustausches in Frage kommen.

Generell sind Veränderungen an den Föderationszusammensetzungen auch im vom LRZ angebotenen Federation Schema Correlation Service zu berücksichtigen, indem den neuen Mitgliedern die Nutzung dieses Dienstes angeboten wird bzw. bei deren Ausscheiden geklärt wird, ob sie ihn noch weiterhin z. B. im Rahmen anderer Föderationen verwenden wollen, oder ob die nicht mehr benötigten Konvertierungsregelsätze entfernt werden können. Für **Einrichtungen im Münchner Wissenschaftsnetz** kann zudem die Inanspruchnahme des ARP Repository Hostings empfohlen werden, sofern nicht analog zur TUM generell alle relevanten FIM-Komponenten durch das LRZ betrieben werden sollen.

Es ist ebenfalls zu beachten, dass die Einführung von FIM an TUM und LRZ in diesem Anwendungsbeispiel parallel zur Bildung der entsprechenden Föderationen stattfindet; somit ist insbesondere davon auszugehen, dass die bislang definierten **föderationsweiten Datenmodelle noch nicht endgültig** sind und die Anforderungen an die zu übermittelnden Daten mit den durch FIM gebotenen Möglichkeiten mittelfristig steigen werden. Erweiterungen der föderationsweiten Datenschemata müssen deshalb mindestens in den Datenkonvertierungsregelsätzen und Attribute Release Policies nachgezogen werden, was wiederum mit einer Anpassung der Datenschutzfreigaben und der Notwendigkeit, die Benutzer über diese Änderungen zu informieren, verbunden ist. Offensichtlich liegt es damit im Interesse der TUM und des LRZ, daran mitzuwirken, dass derartige Änderungen einen für den damit verbundenen Aufwand angemessenen Umfang haben und nachhaltig sind; diese Möglichkeiten zur Einflussnahme sind durch die Teilnahme sowohl als Identity als auch als Service Provider durchaus gegeben.

Zu den regelmäßig erforderlichen Modifikationen, die als *pre-authorized changes* deklariert werden sollten, gehört ferner die Aktualisierung der typischerweise nur zwei Jahre gültigen Serverzertifikate auf den Maschinen und in den Metadaten. Sie kann insbesondere dadurch erleichtert werden, dass die Beantragung und Installation neuer Zertifikate synchron für alle relevanten FIM-Komponenten durchgeführt wird, um den Aufwand, der zur Anzahl notwendiger Interaktionsschritte mit der PKI Registration Authority proportional ist, im beiderseitigen Interesse zu minimieren.

Ebenso sind Softwareupdates an den FIM-Komponenten, insbesondere den vier Instanzen der IDP- und SP-Software, geeignet durch das Change Management zu koordinieren; hierfür bietet sich generell die Nutzung des vom LRZ bereits vorgegebenen Wartungsfensters an.

Mittelfristig ist damit zu rechnen, dass sich durch die **Teilnahme an mehreren Föderationen** Komplikationen ergeben können:

- Da im Allgemeinen nicht davon ausgegangen werden kann, dass im Fall der Teilnahme an weiteren Föderationen jeweils nur disjunkte Mengen lokaler Dienste genutzt werden sollen, wird die Einführung eines **multi-federation-fähigen IDP Discovery Services** notwendig. Dieser kann zwar beispielsweise auf dem Server der SP-Software betrieben werden, so dass keine zusätzliche Hardware erforderlich wird; er ist aber anfälliger gegenüber Fehlern in den Föderationsmetadaten, so dass mit einem erhöhten **Monitoring- und Supportaufwand** zu rechnen wäre. Sein Einsatz am LRZ sollte deshalb nur erfolgen, wenn zusammen mit den Föderationsverwaltungen keine geeignetere Lösung gefunden werden kann.

- Beim föderationsweiten Umstieg auf neue Softwareversionen der IDP- und SP-Software ist auf deren **Abwärtskompatibilität** zu achten; sofern diese nicht uneingeschränkt gegeben ist, wie es z. B. bei Shibboleth bereits mehrfach der Fall war, kann es notwendig werden, zumindest vorübergehend mehrere Instanzen in unterschiedlichen Versionen betreiben zu müssen.

Schließlich ist zu berücksichtigen, dass die Aufrechterhaltung der für FIM benötigten Nutzdaten komplexer wird, da sich die I&AM-Systeme nicht mehr bevorzugt an den verfügbaren Datenquellen orientieren können, sondern die organisationsübergreifenden Datenflüsse berücksichtigen müssen. Während das LRZ seine Datenquellen z. B. durch die eigene Implementierung der webbasierten Managementfrontends sehr gut kontrollieren kann, müssen Umstellungen z. B. an der Studentenverwaltungssoftware der TUM geeignet vorbereitet werden; beispielsweise können durch Umbenennung oder Neueinführung eines Studiengangs Anpassungen z. B. von Konvertierungsregeln für föderationsweite Datenschemata notwendig werden.

Die intensive Mitwirkung des LRZ an der Realisierung der Hochschulgeschäftsprozesse der TUM muss somit durch ein über die rein technischen Komponenten hinausgehendes einrichtungsübergreifendes Change Management unterstützt werden; nachdem für diesen Fall noch keine Leitfäden existieren, da beispielsweise die Best Practices Sammlung ITIL nur organisationsinterne Prozesse ausführt, stellt das Zusammenwachsen der Organisationen durch gemeinsame Prozesse eine Herausforderung dar, die allein durch technische Mittel nicht gelöst werden kann.

7.5.3. FIM-spezifisches Security Management am LRZ

Sowohl für die TUM als auch für das LRZ ergibt sich mit der Einführung von FIM die Neuerung, dass vormals ausschließlich intern verwendete Personendaten über das Internet abrufbar gemacht werden, da der Umfang der bereitgestellten Daten sehr deutlich beispielsweise über die einrichtungsübergreifende Authentifizierung mit dezentraler Passworteingabe im Rahmen des DFN-Roamings hinausgeht. Somit werden auch an die vom Security Management zu treffenden Schutzmaßnahmen neue Anforderungen gestellt, da bereits ein einziger Sicherheitsvorfall, bei dem beispielsweise sämtliche Personendaten ausgespäht werden, nachträglich nicht kompensiert werden kann und mit potentiell großen Schäden am Ansehen des LRZ verbunden ist.

Die initiale Platzierung der FIM-Komponenten gemäß dem in Abschnitt 4.7.2.1 ausgearbeiteten Zonenkonzept trägt bereits zu einer weitreichenden Reduktion der Angriffsfläche – zu-

mindest im Hinblick auf externe Angriffe – bei, so dass sich die Schutzmaßnahmen auf die über das Internet erreichbaren Maschinen konzentrieren können.

Wie im Architekturkonzept erläutert wurde, ist aus technischer Perspektive zwischen netzwerk- und systembasierten Sicherheitsmechanismen zu unterscheiden, die am LRZ wie folgt bereitgestellt werden:

- Auf **Netzwerkebene** werden am LRZ zusätzlich zu Paketfilterfirewalls auch Intrusion Detection und Intrusion Prevention Systeme (IDS/IPS) eingesetzt. Diese arbeiten sowohl signaturbasiert als auch auf Grundlage von Heuristiken, um gutartigen vom unerwünschten Netzwerkverkehr unterscheiden zu können:
  - Signaturen werden dabei üblicherweise nur für bekannte Angriffe, nicht aber für den zuzulassenden Datenfluss verwendet; somit sind für die eingesetzten Systeme zuverlässige Quellen zu wählen und anzubinden, die Signaturen neu bekanntwerdender FIM-spezifischer Angriffe bereitstellen.
  - Auf Heuristiken basierende Systeme müssen trainiert werden, um Auffälligkeiten in den Datenflüssen korrekt erkennen zu können. Hierzu ist insbesondere in der Anfangsphase eine enge Zusammenarbeit zwischen den für die IDS/IPS-Systeme und die FIM-Komponenten Zuständigen erforderlich; dieser Aspekt muss auch im Change Management berücksichtigt werden, da sich beispielsweise durch den Betritt zu weiteren Föderationen neue FIM-Zugriffsmuster ergeben können, die ansonsten als Angriffe eingestuft werden könnten.
- Wie in Abschnitt 7.3.1.1 erläutert wurde, existieren noch keine **Application Level Gateways** für die FIM-Protokolle, obwohl diese durch eine Auswertung der Inhalte der verschlüsselt übertragenen FIM-Nachrichten wesentlich bessere Kontrollmöglichkeiten bieten als IDS/IPS-Systeme. Insbesondere der Schutz der IDP-Software, die einen Hauptangriffspunkt zur Ausspähung der lokalen Daten darstellt, ist deshalb ein wichtiges Kriterium bei der späteren Produktselektion z. B. für Web Services Firewalls.
- Auf **Systemebene** ist der Einsatz von hostbasierten Intrusion Detection Systemen notwendig, mit deren Hilfe erkannt werden kann, ob ein Server kompromittiert wurde und ob beispielsweise Systemprogramme modifiziert worden sind; diese Aufgabe ist praktisch nicht trivial zu bewältigen, da durch die am LRZ separierten Zuständigkeiten für Dienstbetrieb, Security Management und System Management im Einzelfall zu klären ist, ob eine Änderung am System z. B. durch ein erwünschtes Softwareupdate oder einen erfolgreichen Angriff zustande gekommen ist.

  Analoge Aussagen gelten für Konfigurationsoptionen wie IDP-weite Attribute Release und Acceptance Policies, insbesondere wenn ein größerer Personenkreis administrative Berechtigungen hat; für die Überwachung dieser in LDAP-Servern hinterlegten Daten müssen zudem erst dedizierte Werkzeuge geschaffen werden.
- Einen nicht zu vernachlässigenden Aufwand stellt das in Abschnitt 4.7.4 diskutierte **Auditing** dar, das aufgrund des Mangels an geeigneten Werkzeugen vorerst überwiegend manuell durchgeführt werden muss. Nur durch die regelmäßige Durchführung dieser Kontrollmaßnahmen können Auffälligkeiten erkannt werden, die dann als Regeln für die automatisierten Monitoringwerkzeuge formuliert werden können.

Parallel dazu sind die **organisatorischen Maßnahmen**, die bereits für den Betrieb der I&AM-Systeme geschaffen worden sind, auf die FIM-Komponenten auszudehnen: Sie umfassen neben dem physischen Zugangsschutz zu den Servermaschinen insbesondere auch die Sensibilisierung der Mitarbeiter bezüglich des Umgangs mit den Diensten und Personendaten; über das Zusammenspiel mit den Change Management und Release Management Prozessen muss beispielsweise sichergestellt werden, dass keine Fehlkonfigurationen der FIM-Komponenten in der Produktivumgebung auftreten, die zu unautorisierten Zugriffen auf personenbezogene Daten führen können.

Ähnlich zum Change Management zeigt sich somit, dass ein erfolgreicher Dauerbetrieb nicht ausschließlich durch technische Maßnahmen gewährleistet werden kann.

7.6. Bewertung der Lösung für das Anwendungsbeispiel

Das gewählte Anwendungsbeispiel weist durch die Kombination mehrerer in Kapitel 2 vorgestellter Szenarien eine relativ hohe Komplexität auf; sie wurde bewusst gewählt, da sie einerseits die realen Gegebenheiten reflektiert und andererseits verdeutlicht, dass die erarbeitete FIM-Architektur ohne Mehrfachaufwand für mehr als ein FIM-Szenario innerhalb einer Organisation eingesetzt werden kann. Die Komplexität wird andererseits durch die einander recht ähnlichen I&AM-Lösungen an den beiden betrachteten Einrichtungen klar begrenzt.

Vor diesem Hintergrund hat sich gezeigt, dass das in Kapitel 4 vorgestellte Architekturkonzept im Hinblick auf die Selektion der einzuführenden FIM-Komponenten **einfach an die szenarienspezifischen Anforderungen angepasst** werden kann, da auf Komponenten wie das Privilege Management System ohne weitere Eingriffe in die übrige Architektur verzichtet werden kann. Auch die Integration der FIM-Komponenten in die jeweils vorhandene I&AM-Infrastruktur bereitet auf Basis der explizit vorgesehenen Gatewaykomponenten und des Identitätsdatenkonverters keine Schwierigkeiten; gegenüber den in Kapitel 3 erläuterten bisherigen FIM-Ansätzen stellt dies – unabhängig vom in dieser Arbeit erweiterten Funktionsumfang von FIM-Lösungen – bereits einen deutlichen Mehrwert dar.

Im Anwendungsbeispiel wurde exemplarisch anhand der Self Services demonstriert, wie bereits vorhandene Infrastrukturkomponenten um FIM-spezifische Funktionen erweitert werden können, ohne dass der Betrieb zusätzlicher neuer Hilfsdienste erforderlich wird. Im kombinierten TUM-/LRZ-Szenario bietet es sich zudem an, **mehrere FIM-Komponenten organisationsübergreifend gemeinsam zu nutzen**; hierfür wurden die entsprechende Konfiguration einiger Komponenten wie des Single Sign-On Systems und der Schnittstelle zu den Föderationsmetadaten sowie die Möglichkeit zum Betrieb mehrerer Instanzen desselben Dienstes auf einer Servermaschine demonstriert.

Auch wenn der dennoch notwendige Investitionsaufwand für die Anschaffung und den Betrieb zahlreicher neuer Servermaschinen verdeutlicht, dass es sich bei FIM um keinen Dienst handelt, der „nebenher“ betrieben werden kann, wurde dennoch veranschaulicht, dass die systematische Aufgliederung der konzipierten FIM-Architektur in rund ein Dutzend Komponenten nicht zwangsweise zur Notwendigkeit derselben Anzahl an getrennt zu betreibenden Diensten und Servern führt. Somit kann über die in Kapitel 6 untersuchte Performanz der Neuentwicklungen hinaus von einer **praktischen Anwendbarkeit des Konzepts** ausgegangen werden.

Die ebenfalls in Kapitel 4 vorgestellten Konzepte für die **Migration**, das **Change Management** und das **Security Management** konnten ohne Änderungen, die über eine szenarienspezifische Anpassung hinausgehen, erfolgreich angewandt werden. Diesbezüglich hat sich gezeigt, dass neben der technisch geprägten Einführung von FIM-Komponenten insbesondere auch neue und zum Teil organisationsübergreifende Lösungen für das IT Service Management notwendig sind, die in der Praxis derzeit fehlen und die auch in anderen Bereichen noch konzeptionell zu untersuchen sind.

Im Hinblick auf einen konkreten praktischen Einsatz der in dieser Arbeit vorgestellten Architektur- und Werkzeugkonzepte bleibt jedoch festzuhalten, dass eine Vielzahl von Funktionen, beispielsweise des konzipierten FIM Privacy Management Systems und des Notifications-Konnektors, derzeit aufgrund der offensichtlich werdenden Diskrepanzen zwischen dem vorgestellten Konzept und aktuell verfügbaren FIM-Implementierungen wie Shibboleth noch nicht zum Einsatz kommen kann. Die in dieser Arbeit aufgezeigten zusätzlichen Möglichkeiten motivieren somit dazu, im Rahmen von Nachfolgearbeiten **konkrete Beiträge zu Systemen wie Shibboleth** zu liefern, wie dies bei den in Kapitel 6 erläuterten Komponenten bereits erfolgt ist.

Zusammenfassend zeigt sich, dass die in Abschnitt 4.1.3 für das Architekturkonzept gesteckten Ziele auch im Anwendungsbeispiel vollständig erreicht wurden:

- Die Integration von I&AM- und FIM-Komponenten konnte auf Basis der geschaffenen **Schnittstellen mit minimalem szenarienspezifischem Konzeptionsaufwand** realisiert werden.
- Die erarbeitete **Integrationsmethodik** konnte direkt auf das Szenario angewandt werden.
- Das **Zusammenspiel mit dem Security Management** ist im Szenario ohne größere Eingriffe in die vorhandene Infrastruktur möglich.
- Die **Anwendbarkeit der FIM-Architektur** wurde für zwei Organisationen auf Basis der für diese relevanten Teilmengen der in Kapitel 2 vorgestellten Szenarien 1, 3, 4 und 5 demonstriert.
- Die **Nachhaltigkeit** der exemplarischen Lösung ist durch ihre Flexibilität und **definierte Anknüpfungspunkte für das Change Management** gegeben.

Zur Umsetzung dieser Lösung tragen die in Kapitel 5 spezifizierten Werkzeugkonzepte maßgeblich bei; insbesondere der Identitätsdatenkonverter und das FIM Privacy Management System stellen dabei einen Funktionsumfang bereit, der auch für wesentlich komplexere Szenarien geeignet wäre.

Kapitel 8.

Zusammenfassung und Ausblick

Die Notwendigkeit, IT-Dienste effizient organisationsübergreifend nutzen zu können, entwickelt sich vielen Bereichen zu einem kritischen Erfolgsfaktor. Technische Authentifizierungs- und Autorisierungsinfrastrukturen setzen als Basis eine geeignete Verwaltung der lokalen Benutzer voraus; ihre Planung sowie der Aufbau und Betrieb sind die Kernaufgaben des Identity Managements.

Als Federated Identity Management wird die aktuell vorherrschende Form des organisationsübergreifenden Identity Managements bezeichnet, bei der die Benutzer mit so genannten Identity Providern (IDPs) assoziiert werden, über die ihre Profildaten selektiv an Service Provider (SPs) transferiert werden können. Hierdurch können sowohl die Effizienz bei der Akquisition der Daten als auch deren Qualität gegenüber der traditionellen manuellen Mehrfacherfassung deutlich gesteigert und beispielsweise durch Single Sign-On auch die Benutzerfreundlichkeit verbessert werden.

Im folgenden Abschnitt 8.1 werden die wichtigsten Aspekte dieser Arbeit zusammengefasst; eine Diskussion der Ergebnisse und deren Weiterverwendungsmöglichkeiten folgt in Abschnitt 8.2. Die Arbeit wird durch eine Diskussion der verbleibenden offenen Punkte und einen Ausblick auf verwandte Forschungsfragestellungen in den Abschnitten 8.3 und 8.4 abgeschlossen.

8.1. Zusammenfassung dieser Arbeit

Da sowohl Identity Management als auch Federated Identity Management noch relativ junge Disziplinen sind, die zu mehreren konkurrierenden Lösungsansätzen und zum Teil stark abweichender Interpretation von Begrifflichkeiten geführt haben, wurden in **Kapitel 2** die grundlegenden Organisationskonzepte, Prozesse, Workflows und Kommunikationsprotokolle der drei aktuell am weitesten verbreiteten Identity Management Varianten eingeführt:

1. Das Identity & Access Management (I&AM) zielt auf die ausschließlich organisationsinterne, zentralisierte Verwaltung von Benutzern ab. Hierzu werden die Datenbestände aus autoritativen Quellsystemen wie Personal- und Kundenverwaltungssoftware aggregiert und korreliert, um sie entweder den lokalen IT-Diensten zum Abruf zur Verfügung zu stellen oder diese über einen als User Provisioning bezeichneten Prozess zu speisen.

Eine daraus resultierende Grundannahme dieser Arbeit ist, dass einrichtungsinterne I&AM-Systeme bereits vorhanden sind und möglichst ohne tiefgehende Modifikationen als Basis für das organisationsübergreifende Identity Management weiter verwendet werden sollen.

2. Das Federated Identity Management (FIM) soll die Möglichkeit bieten, vorhandene Benutzerdatenbestände organisationsübergreifend zu nutzen, um beispielsweise die redundante manuelle Registrierung z. B. externer Mitarbeiter in den lokalen I&AM-Systemen zu vermeiden; neben dem administrativen Mehraufwand sollen damit insbesondere Inkonsistenzen durch ungepflegte, veraltete Daten eliminiert werden, die auch zu einer Reihe von IT-Sicherheitsproblemen führen können.

3. Das User Centric Identity Management (UCIM) stellt einen mit FIM vergleichbaren Ansatz dar, bei dem die Benutzerdaten jedoch nicht von Identity Providern, sondern von jedem Benutzer selbst verwaltet werden. Der Fokus liegt entsprechend weniger auf organisationsübergreifenden Kooperationen, sondern stärker auf der Nutzung einer Vielzahl von IT-Diensten verschiedener Service Provider durch Privatkunden; UCIM soll somit beispielsweise die fehleranfällige und oftmals lästig werdende manuelle Anmeldung bei jedem einzelnen Dienstleister ersetzen.

Um Anforderungen an FIM-Lösungen umfassend zu ermitteln, mussten somit auch die als Ausgangsbasis dienenden I&AM-Systeme sowie die durch UCIM ermöglichte Funktionalität analysiert werden. Da eine Anforderungsanalyse auf Grundlage der in den Standardspezifikationen aufgeführten, überwiegend sehr einfachen Fallbeispiele weder vollständig noch nachhaltig wäre, wurden fünf sehr realitätsnahe, komplexere Szenarien untersucht:

- Szenario 1 stellt das I&AM-System der Technischen Universität München vor, das derzeit im Rahmen des DFG-Projekts IntegraTUM realisiert wird; hierbei ist charakteristisch, dass eine größere Zahl zentraler IT-Dienste vom Leibniz-Rechenzentrum erbracht wird, deren im Szenario angestrebte FIM-basierte Nutzung bereits eine Reihe relevanter Anforderungen an potentielle FIM-Lösungen aufzeigt.

- Szenario 2 betrachtet UCIM-Systeme am Beispiel von Microsoft CardSpace, das durch die Integration ins Betriebssystem Microsoft Windows Vista eine weite Verbreitung findet; aus diesem Szenario wurden insbesondere Anforderungen an die effiziente und intuitive Interaktion von Benutzern mit Identity Management Systemen abgeleitet, die auch von FIM-Lösungen berücksichtigt werden müssen.

- Szenario 3 geht auf die Rolle des LRZ als zentraler IT-Dienstleister im Münchner Wissenschaftsnetz ein; neben einer größeren Anzahl Kunden und mehr als 100.000 Benutzern ist in diesem Szenario insbesondere das breite Dienstspektrum maßgeblich, zu dem auch zahlreiche Systeme gehören, die nicht wie von den bisherigen FIM-Ansätzen gefordert über eine web-service- oder webbasierte Schnittstelle verfügen, aber dennoch im Rahmen einer FIM-Lösung integriert werden sollen. Die Anwendung von FIM wurde dabei der bislang angestrebten organisationsübergreifenden Identity Management Lösung durch direkte Kopplung von Verzeichnisdiensten gegenübergestellt, deren sich gegenüber FIM abzeichnende Nachteile herausgearbeitet wurden.

- Szenario 4 schildert die Aufgaben des LRZ im Grid-Computing am Beispiel des Projekts DEISA und vergleicht dabei die bislang mit sehr einfachen herkömmlichen Mitteln realisierte Grid-Benutzerverwaltung mit den durch FIM gegebenen Möglichkeiten, wobei die sich aus dem Grid-Umfeld ergebenden, partiell sehr systemnahen Anforderungen berücksichtigt werden.
- Szenario 5 illustriert die auch im wissenschaftlichen Umfeld komplexen Anforderungen an FIM-Lösungen am Beispiel der hochschulübergreifenden Nutzung von Learning Management Systemen; dabei spielt insbesondere die Übertragung aus Datenschutzperspektive höchst sensibler personenbezogener Daten wie Prüfungsleistungen eine wichtige Rolle.

Bezüglich der Auswahl der Szenarien ist darüber hinaus zu berücksichtigen, dass ihre Affinität zu akademischen Einrichtungen keine Vereinfachung gegenüber industriellen Einsatzszenarien darstellt. Vielmehr ergibt sich einerseits durch die de facto vorherrschende Heterogenität im Hochschulumfeld ein breiteres Spektrum an Anforderungen pro Szenario, so dass sowohl Überlappungen als auch Sonderfälle kompakter gezeigt werden konnten; andererseits wurde dadurch die Basis für ein durchgängiges, szenarienübergreifendes Anwendungsbeispiel in Kapitel 7 gelegt.

Aus jedem Szenario wurden neben funktionalen auch organisatorische, datenschutzspezifische, IT-sicherheitstechnische und nicht-funktionale Anforderungen abgeleitet, wobei in einigen Bereichen mehrere grundlegende Anforderungen zu jeweils einer einzigen zusammengefasst wurden.

Um die dennoch mehr als 60 resultierenden Anforderungen effizient zur Bewertung der existierenden und im Rahmen dieser Arbeit konzipierten Lösungen einsetzen zu können, wurden sie schließlich begründet gewichtet und zu einem gesamtheitlichen Anforderungskatalog zusammengestellt, der in Bezug auf Herleitungssystematik, Umfang und Detaillierungsgrad neuartig ist.

Am Anfang von **Kapitel 3** wurden mit SAML, den Spezifikationen der Liberty Alliance und WS-Federation diejenigen Industriestandards untersucht, die den Begriff Federated Identity Management in den letzten Jahren maßgeblich geprägt haben. Bei einer Bewertung auf Basis des Anforderungskatalogs wurde dabei sehr schnell deutlich, dass die von diesen FIM-Ansätzen gebotenen Möglichkeiten weit hinter den Erwartungen zurückbleiben, da sie zahlreiche im organisationsinternen Identity Management längst etablierte Möglichkeiten nicht auf den organisationsübergreifenden Anwendungsfall übertragen: Beispielsweise können Benutzerdaten

- nur abgerufen werden, während der Benutzer den Dienst gerade verwendet.
- von Service Providern nur gelesen, aber nicht geschrieben werden.
- nur an die Dienste selbst übermittelt werden, wodurch einerseits das beim Service Provider vorhandene I&AM-System effektiv umgangen wird und andererseits alle Dienste einzeln und vollständig an FIM angepasst werden müssen.

Zudem zeigt sich, dass grundlegende Datenschutzanforderungen wie die benutzergesteuerte, nur selektive Freigabe des eigenen Benutzerprofils im Unterschied zu UCIM-Ansätzen in

zwei der drei FIM-Standards nicht manifestiert ist und auch die Liberty Alliance außer einer ständig wiederholten interaktiven Nachfrage beim Benutzer keine Anforderungen an die Umsetzung von Datenschutzkonzepten stellt. Der enge Fokus der Standardisierungsbemühungen auf die Datenübertragungsprotokolle bedingt zudem ein bei allen teilnehmenden Einrichtungen homogenes Datenmodell, das in der Praxis selbst bei Unternehmen aus derselben Branche meist nicht gegeben ist und somit nicht realistisch vorausgesetzt werden kann.

Bei der nachfolgenden Analyse von FIM-Forschungsansätzen stellte sich heraus, dass diese zwar punktuelle Verbesserungen beisteuern und beispielsweise durch tiefgehende Sicherheitsanalysen der FIM-Protokolle auch praktisch relevante Ergebnisse erzielen, ein gesamtheitlicher Ansatz jedoch fehlte. Aus diesem Grund wurden die Betrachtungen auf verwandte Gebiete wie das Privacy Management, das User Provisioning und Schema-Koordinationstechniken aus dem Gebiet föderierter Datenbankmanagementsysteme ausgedehnt, um deren Übertragbarkeit auf FIM-Szenarien zu analysieren. Während keiner dieser anderen Ansätze direkt auf FIM angewandt werden konnte, wurden mehrere Ideen im Rahmen der Architektur- und Werkzeugkonzepte dieser Arbeit berücksichtigt.

Eine kurze Untersuchung der aktuellen Weiterentwicklungen der UCIM-Ansätze hat eine sich abzeichnende Konsolidierung und Annäherung an den FIM-Standard SAML gezeigt, so dass langfristig mit interoperablen Lösungen zu rechnen ist.

Die Schwerpunkte des in **Kapitel 4** erarbeiteten Architekturkonzepts, dem ein an den Anforderungen orientierter, ganzheitlicher Ansatz zugrunde liegt, sind

- die nahtlose Integration von FIM-Komponenten in vorhandene I&AM-Systeme auf Basis der Definition entsprechender Schnittstellenkomponenten.
- die Berücksichtigung der Heterogenität der an einer Föderation beteiligten Organisationen insbesondere im Hinblick auf die lokal eingesetzten Datenmodelle.
- die policygesteuerte, selektive Freigabe personenbezogener Daten durch kombinierte Auswertung föderationsweiter, organisationsweiter und benutzerspezifischer Vorgaben.
- das Zusammenspiel der integrierten FIM- und I&AM-Lösung mit den IT Service Management Prozessen, die am Beispiel des Change Managements und des Security Managements vertieft wurden.

Die Zielsetzung und der Umfang des Architekturkonzepts wurden dabei aus einer szenarienunabhängigen Gegenüberstellung der mit bisherigen FIM-Ansätzen möglichen Lösungen mit einem fiktiven Idealzustand aus den Perspektiven von Identity Providern und Service Providern sowie aus föderationsweiter Sicht abgeleitet.

Im Konzept wurden zunächst die verfügbaren I&AM-Komponenten und anschließend die benötigten FIM-Komponenten im Hinblick auf ihre Aufgaben, Funktionalität, Schnittstellen, Kommunikationsmuster und Sicherheitsmechanismen sowie ihr intern verwendetes Datenmodell und Aspekte der Hochverfügbarkeit und des Managements analysiert. Dabei wurden jeweils die Verwendung der Komponente in der Gesamtarchitektur bzw. bei neu eingeführten FIM-Komponenten ihr Design begründet und das Zusammenspiel mit den anderen Komponenten diskutiert. Die Partitionierung in die drei elementaren Nutzdatenkategorien Authentifizierungsbestätigungen, Autorisierungsbestätigungen und allgemeine Benutzerattributsauskünfte wird dabei auch in der Selektion und Zusammenstellung der Komponenten reflektiert.

Die wesentlichen Neuerungen der in Abbildung 4.3 auf Seite 167 visualisierten integrierten I&AM- und FIM-Architektur umfassen

- die Einführung einer Schnittstellenkomponente zwischen den als IDP- bzw. SP-Software bezeichneten herkömmlichen FIM-Komponenten, die nur geringfügig erweitert wurden, und der als Identity Repository bezeichneten zentralen Benutzerdatenbasis des vorhandenen I&AM-Systems.

  Diese Schnittstellenkomponente nimmt insbesondere die als Identitätsdatenkonverter bezeichnete, neu eingeführte FIM-Komponente in Anspruch, die eingehende FIM-Anfragen von einem föderationsweiten oder SP-spezifischen in das lokal eingesetzte Datenmodell umwandelt und analog dazu bei den ausgehenden FIM-Antworten verfährt.

  Der Identitätsdatenkonverter kommuniziert wiederum mit einem als Federation Schema Correlation Service bezeichneten neuen föderationsweiten Dienst, der die Verwaltung und gezielte Selektion der von mehreren Einrichtungen wiederverwendbaren Konvertierungsregelsätze unterstützt.

- die Integration einer neuen, als FIM Privacy Management System bezeichneten FIM-Komponente in die IDP-seitigen Workflows. Sie steuert über so genannte Attribute Release Policies (ARPs), welche personenbezogenen Daten unter welchen Bedingungen an welche Service Provider übermittelt werden dürfen. Dabei wurden insbesondere Konzepte aus dem organisationsinternen Privacy Management wie die Unterstützung von Langzeit-Obligationen, die beispielsweise die maximal erlaubte Speicherungsdauer von Benutzerdaten regeln, auf das FIM-Umfeld übertragen.

- analog zu den IDP-seitigen ARPs so genannte Attribute Acceptance Policies auf der Seite des Service Providers, die primär der Sicherstellung der benötigten Datenqualität dienen und deren Funktionsumfang wiederum deutlich über bisherige Ansätze hinausgeht.

- die Ausdehnung von FIM-Operationen auf durch Service Provider initiierte selektive Schreibzugriffe, die Möglichkeit zur föderierten Datensynchronisation über eine als Notifications-Konnektor bezeichnete FIM-Komponente sowie die optional nutzbare Auslegung der FIM-Workflows auf Situationen, in der ein Benutzer offline ist, d. h. den jeweiligen Dienst gerade nicht nutzt.

Soweit möglich wurden dabei bereits vorhandene, nicht FIM-spezifische Komponenten wie Privilege Management Systeme zur Verwaltung von Autorisierungsinformationen in die Gesamtarchitektur integriert anstatt ihre Funktionalität nachzubilden. Die hierfür ausgewählten Systeme weisen wie die neu eingeführten Komponenten die Eigenschaft auf, basierend auf ihrer policygesteuerten Konfiguration nahtlos in die bereits vorhandenen Managementinfrastrukturen integriert werden zu können.

Aufbauend auf einer Analyse der gegenseitigen Abhängigkeiten aller in der Architektur verwendeten Komponenten wurde anschließend eine Integrationsmethodik spezifiziert, die eine klare und einfach an szenarienspezifische Gegebenheiten anzupassende Reihenfolge bei der Einführung von FIM in Organisationen vorgibt. Dabei wurde zwischen vorbereitenden Maßnahmen, die auch lokale organisatorische Aspekte wie die als Identity Provider zu liefernde

Datenqualität berücksichtigen, und der technischen Realisierung unterschieden; insbesondere wird auch auf die Rollendualität eingegangen, wenn eine Organisation sowohl als Identity Provider als auch als Service Provider fungieren soll.

Nach einer grundlegenden Untersuchung FIM-spezifischer Angreifermodelle wurde ferner die Integration der FIM-Gesamtarchitektur in das IT Security Management untersucht. Als Schutzmaßnahme auf Netzwerkebene wurde eine Zonenbildung ausgearbeitet, die durch die Auswahl und Positionierung von Paketfilterfirewalls und Application Level Gateways verfeinert wurde. Auf Anwendungsebene wurden Möglichkeiten zur Gewährleistung einer Ende-zu-Ende-Vertraulichkeit, zur Authentifizierung von Kommunikationspartnern durch jede FIM-Komponente und zur Sicherstellung der Integrität von Nutz- und Metadaten diskutiert; hierbei spielen insbesondere auch das Systemmonitoring und das Auditing von FIM-Transaktionen eine zentrale Rolle, die derzeit aufgrund noch fehlender Möglichkeiten, z. B. zur Korrelation von Protokolleinträgen sowie zur effizienten föderationsweiten Zusammenarbeit bei Sicherheitsvorfällen, erschwert werden.

Die Notwendigkeit zur Anpassungen organisationsinterner Prozesse und zur organisationsübergreifenden Kooperation zeigte sich auch bei der Analyse des FIM-spezifischen Change Managements sehr deutlich. Hierbei wurde zwischen organisationsinternen und föderationsweiten Anwendungsfällen unterschieden und ein Ausblick auf föderationsübergreifende Änderungsereignisse gegeben. Im organisationsinternen Fall wurden vornehmlich Änderungen an der Konfiguration aller für FIM relevanten Komponenten untersucht und mögliche *pre-authorized changes* diskutiert; bei der föderationsweiten Betrachtung standen Änderungen an der Föderationskonstellation durch das Hinzukommen und Ausscheiden von Föderationsteilnehmern im Vordergrund.

Auf dieser Basis wurden mehrere Architekturmuster definiert, die bei der Analyse neuer Szenarien eingesetzt werden können, und FIM-Referenzarchitekturen für Identity Provider, Service Provider, Attribute Authorities, Authorization Provider und Trusted Third Parties spezifiziert; auch hierbei wurde die Kombination aus Identity Provider und Service Provider vertieft, um die Möglichkeit zur Nutzung gemeinsamer Komponenten für beide FIM-Rollen zu demonstrieren.

Eine das Architekturkonzept abschließende Bewertung auf Basis des Kriterienkatalogs zeigte, dass insbesondere durch die Schaffung der Schnittstellenkomponenten deutliche Fortschritte erzielt werden konnten; die konsequente Kombination bisheriger FIM-Ansätze mit neuen oder verbesserten Komponenten trug dazu bei, dass – zumindest auf konzeptioneller Ebene – alle *essentiellen* Anforderungen vollständig und alle *wichtigen* Anforderungen mindestens größtenteils erfüllt werden können (vgl. Abbildung 4.39 auf Seite 288).

In **Kapitel 5** wurden die wichtigsten der neu eingeführten FIM-Komponenten nach sukzessiver Verfeinerung der konkreten technischen Anforderungen in einem Top-down-Verfahren im Detail spezifiziert:

- Für den Identitätsdatenkonverter wurden zunächst die Anforderungen an die benötigte Funktionalität sowie das zu unterstützende charakteristische FIM-Kommunikationsverhalten analysiert. Dieses erwies sich als nahezu bipartit, da FIM-Transaktionen überwiegend zwischen Service Providern einerseits und Identity Providern andererseits abgewickelt werden und nur in den bislang seltenen Fällen der Delegation eine Kommunikation zwischen Service Providern notwendig wird.

Zur Umsetzung der auf Datenkonvertierungsebene benötigten Funktionalität wurde die Entscheidung getroffen, analog zu existierenden I&AM-Systemen auf XSLT-Stylesheets zurückzugreifen, da diese eine standardisierte und flexible Basis darstellen, für die in vielen Einrichtungen schon Wissen und Werkzeuge vorhanden sind.

Um eine redundanzfreie Wiederverwendbarkeit zu ermöglichen, verarbeitet der Identitätsdatenkonverter beliebig lange, aus XSLT-Stylesheets bestehende Regelketten, wobei auch Bestandteile anderer Regelketten referenziert werden können. Er setzt somit insbesondere das Ziel um, nach Möglichkeit ein föderationsweit gemeinsames Datenschema zu verwenden, aber eventuell notwendig werdende Abweichungen ebenfalls zu unterstützen.

Als Werkzeug zum Austausch von Konvertierungsregelsätzen dient der Federation Schema Correlation Service, der diese in einer in der Regel dünnbesetzten Matrix vorhält, deren Serialisierung zur Speicherung in einem LDAP-basierten Repository demonstriert wurde. Über das Rechtekonzept, das den Zugriff auf die Regelsätze einzelner Organisationen steuert, können Konstellationen wie die Pflege der eigenen Regelsätze durch Dritte oder die Nutzung dedizierter Konvertierungsregeldienste realisiert werden. Der Federation Schema Correlation Service bietet dabei auch Funktionen zur grundlegenden Unterstützung der Selektion geeignet erscheinender, bereits vorhandener Regelsätze, über die insbesondere der für neue Föderationsmitglieder nicht unwesentliche initiale Arbeitsaufwand beim Eintritt in die Föderation deutlich reduziert werden kann.

- Im Rahmen der Spezifikation des FIM Privacy Management Systems wurde nach einer vertiefenden Analyse bestehender Ansätze die Entscheidung für XACML als für Attribute Release Policies zu verwendende Policysprache getroffen, da diese u. a. mit komplexen Bedingungen und Obligationen bereits alle relevanten Sprachelemente bietet und einfach z. B. um Namenskonzepte für die Adressierung von Diensten und Benutzerattributen erweitert werden konnte.

  Ein wesentlicher Bestandteil dieses Konzepts ist somit die detaillierte Beschreibung der ARP-spezifischen Verwendung von XACML-Policies bezüglich ihrer exakten Syntax und Semantik; sie wird von einer Spezifikation des Auswertungsworkflows ergänzt, der sich vom Abruf der für eine Anfrage relevanten Policies aus einem LDAP-Server über die Bildung des auszuwertenden XACML Policy-Sets und die Übergabe an einen standardkonformen XACML Policy Decision Point bis zur Auswertung der resultierenden Obligationen sowie die Rückgabe an die aufrufende FIM-Komponente erstreckt.

  Im Unterschied zu bisherigen Ansätzen wird dabei nicht nur zwischen freigegebenen und zurückzuhaltenden Benutzerattributen unterschieden, sondern im Zusammenspiel mit der im Architekturkonzept neu eingeführten FIM-Interaktionskomponente ermöglicht, dass der Benutzer selbst über die Freigabe von Attributen entscheidet, für die noch keine Policies vorliegen, und daraus optional zur Laufzeit neue ARPs erzeugt werden können. Dieses Konzept stellt somit einen mit Sicherheit auch aus Benutzerperspektive interessanten Kompromiss aus bislang rein policybasierten Systemen wie Shibboleth und rein interaktiven Ansätzen wie demjenigen der Liberty Alliance dar.

- Auch für die bei Service Providern eingesetzten, zu ARPs funktional komplementären Attribute Acceptance Polices wurde XACML als Policysprache gewählt; neben der analogen Spezifikation von Syntax, Semantik und Verarbeitungsworkflows wurde auch auf die Synergieeffekte durch den Einsatz einer gemeinsamen Policysprache eingegangen.

In mehreren Beispielen wurde nicht nur die ARP- und AAP-spezifische Verwendung von XACML demonstriert, sondern auch gezeigt, wie mit Hilfe von XSLT-Stylesheets ganze Policies in XACML konvertiert werden können. Diese Möglichkeit wird einerseits z. B. für die Migration von bereits bestehenden Shibboleth-Deployments benötigt und kann andererseits für die automatisierte Anpassung föderationsweit vorgegebener ARPs und AAPs an das lokal eingesetzte Datenmodell verwendet werden.

- Am Beispiel des so genannten Notifications-Konnektors, der bei einem Identity Provider für die Propagation von Datenänderungen an betroffene Service Provider zuständig ist, wurde erläutert, wie ein gegenüber den bisherigen FIM-Standards deutlicher Zugewinn an Funktionalität mit aus dem I&AM-Umfeld bekannten, relativ einfachen Mitteln erreicht werden kann; er veranschaulicht zudem das effiziente Zusammenspiel mehrerer FIM-Komponenten im Sinne eines durchgängigen Workflows.

Als Tragfähigkeitsnachweis für die erarbeiteten Werkzeugkonzepte wurden der Identitätsdatenkonverter und das XACML-basierte FIM Privacy Management System implementiert. In **Kapitel 6** wurde zunächst die Motivation erläutert, die im Hochschulumfeld weit verbreitete Software Shibboleth als Ausgangsbasis für eigene Entwicklungen zu verwenden; nach einem kurzen Überblick über die Architektur und Quelltextstruktur von Shibboleth wurden die wesentlichen Elemente der Java-Implementierung erläutert und die Ergebnisse einer Diplomarbeit zur Verwendung von XACML mit Shibboleth zusammengefasst. Bei beiden Komponenten hat sich gezeigt, dass der volle Funktionsumfang aufgrund der architekturellen Beschränkungen von Shibboleth nicht umgesetzt werden konnte; die Kernideen wurden jedoch realisiert, anderen Shibboleth-Anwendern in Form eines Quelltext-Patches zur Verfügung gestellt und mit den Entwicklern von Shibboleth diskutiert. Zwar ist eine Aufnahme der eigenen Entwicklungen in die kommende Version 2.0 von Shibboleth aufgrund ihres Umfangs und der Zeitplanungen nicht mehr möglich; diese Thematik soll aber nach Abschluss der Arbeiten an Shibboleth 2.0 erneut diskutiert werden.

Ein nicht unwesentlicher Aspekt der praktischen Einsetzbarkeit der implementierten Komponenten ist deren Performanz, da die durch sie bedingten Verzögerungen im Fall der interaktiven Dienstnutzung einen unmittelbaren Einfluss auf die Antwortzeiten der Dienste haben. Zur Analyse wurde der eigene Code rudimentär instrumentiert, so dass die Verarbeitungszeiten bei einer, zehn bzw. 50 parallelen Anfragen und somit im Ruhezustand sowie bei durchschnittlicher und bei maximaler Auslastung gemessen werden konnten. Eine Diskussion der Messergebnisse zeigte, dass bereits die Prototypen der neuen Komponenten durchaus praktisch eingesetzt werden können, dass mittelfristig jedoch insbesondere der XACML Policy Decision Point noch optimiert werden muss, da er bereits im Ruhezustand mit rund 200 Millisekunden am stärksten zu einer für den Benutzer spürbaren Latenz beiträgt.

Die Anwendbarkeit und Übertragbarkeit des Architekturkonzepts und der Integrationsmethodik wurden in **Kapitel 7** anhand eines komplexen, realitätsnahen Beispiels demonstriert, in dem die für die Technische Universität München und das Leibniz-Rechenzentrum relevanten Aspekte der in Kapitel 2 vorgestellten Szenarien zusammengefasst wurden. In Form eines exemplarischen Projekts zur Einführung von FIM an beiden Einrichtungen wurde zunächst gezeigt, welche technischen und organisatorischen Vorbereitungen zu treffen sind, um anschließend die notwendigen FIM-Komponenten selektieren und die anzustrebende FIM-Architektur spezifizieren zu können.

Als Besonderheit dieses Anwendungsbeispiels hat sich gezeigt, dass aufgrund des Betriebs beider I&AM- und FIM-Infrastrukturen durch das LRZ zahlreiche Komponenten der Gesamtarchitektur gemeinsam genutzt werden können, wodurch sich die zu erwartenden Hardware- und Betriebskosten sowie der Personalaufwand zur Einführung deutlich reduzieren. Parallel dazu wurden anhand der sich in der Einführungsphase befindenden deutschlandweiten Föderation DFN-AAI und einer fiktiven Föderation für das Grid-Projekt DEISA Besonderheiten bei der Teilnahme einer Einrichtung an mehreren Föderationen diskutiert.

Nach einer Beschreibung der notwendigen Migrationsschritte, in der die in Kapitel 4 spezifizierte Integrationsmethodik geringfügig szenarienspezifisch angepasst und um eine Abschätzung der Aufwände für die Einzelschritte ergänzt wurde, bildete eine Diskussion der operativen Aspekte wie die grundlegende Konfiguration der FIM-Werkzeuge sowie die Integration in das IT Service Management am LRZ den Abschluss der Beiträge dieser Arbeit.

8.2. Weiterverwendung der Ergebnisse dieser Arbeit

Bevor in den nächsten beiden Abschnitten auf die noch offenen FIM-spezifischen und verwandten Forschungsfragestellungen eingegangen wird, werden nachfolgend die konkreten Möglichkeiten zur Weiterverwendung der Ergebnisse dieser Arbeit skizziert.

Der in Kapitel 2 erstellte, ausführliche Anforderungskatalog kann einerseits zur Beurteilung neuer und weiterentwickelter FIM-Ansätze dienen, andererseits jedoch auch als Basis für die Evaluation konkreter Softwareprodukte herangezogen werden; für diesen Zweck muss er beispielsweise um Kriterien wie Kosten für Lizenzen und Support erweitert und szenarienspezifisch gegebenenfalls um irrelevante Anforderungen gekürzt werden.

In Kapitel 3 wurden bei der Analyse der für diese Arbeit wichtigen Standards und Forschungsansätze mehrere andere Forschungsgebiete hinsichtlich ihrer Relevanz für FIM eingeordnet; durch die Berücksichtigung dieser Zusammenhänge können Nachfolgearbeiten Synergien nutzen und zur Schaffung weiterer Schnittstellen – insbesondere zum umfassenden Bereich der Privacy Enhancing Technologies – beitragen.

Das in Kapitel 4 vorgestellte Architekturkonzept kann auf Basis der Spezifikation der Einzelkomponenten, Architekturmuster und Referenzarchitekturen als Leitfaden beim Aufbau eigener, szenarienspezifischer FIM-Architekturen verwendet werden. Die spezifizierte Integrationsmethodik und die Diskussionen der Auswirkungen auf das Change Management und das Security Management können dabei wie im Anwendungsbeispiel demonstriert z. B. als Vorlage oder Checkliste für eigene Aktivitäten dienen. Da durch die Einführung der dedizierten SP-Software mit einem Konnektor zum lokalen I&AM-System die Notwendigkeit zur vollständigen FIM-Anpassung aller Dienste entfällt und Offline-Zugriffe, Schreiboperationen und Datenaktualisierungen vorgesehen sind, ist die Wiederverwendbarkeit und Nachhaltigkeit des Architekturkonzepts auch für die erst in den nächsten Jahren zu erwartenden Erweiterungen der industriellen FIM-Standards gegeben.

Die durch die in Kapitel 5 spezifizierten neuen FIM-Werkzeuge gegebenen Möglichkeiten decken bereits zahlreiche Anforderungen ab, die mit zunehmender Verbreitung von FIM erst sukzessive in der Praxis notwendig werden. Insbesondere das Konzept des FIM Privacy Management Systems, das einen hybriden Ansatz aus policybasierter Steuerung und Benutzerinteraktivität verfolgt und mit der Unterstützung von komplexen Bedingungen und (Langzeit-)Ob-

ligationen mehrere aktuelle Forschungsansätze in sich vereint, kann sich ebenso wie der flexible Identitätsdatenkonverter zu einer Schlüsselkomponente zukünftiger FIM-Architekturen und -Produkte entwickeln. Die in Kapitel 6 vorgestellten prototypischen Implementierungen können bereits mit Shibboleth eingesetzt werden, wobei jedoch der mit der Portierung auf neue Versionen von Shibboleth verbundene Aufwand berücksichtigt werden muss. Im Rahmen einer Weiterentwicklung dieser Komponenten ist darüber hinaus mit den Entwicklern der Software zu klären, ob und wie eine Lösung für die derzeitigen architekturellen Beschränkungen von Shibboleth gefunden werden kann; bezüglich einer sanften Migration können auf Basis der bei der Implementierung gemachten Erfahrungen bereits erste konkrete Vorschläge vorgelegt werden.

Schließlich kann das in Kapitel 7 vorgestellte Anwendungsbeispiel als Leitfaden für die Einführung von FIM an der TUM und dem LRZ dienen, deren Notwendigkeit sich im Rahmen der DFN-AAI bereits praktisch abzeichnet.

8.3. Ausblick auf weitere FIM-spezifische Arbeitsbereiche

In dieser Arbeit konnten einige für FIM durchaus wichtige Themen nur oberflächlich behandelt werden. Die nachfolgende Liste gibt einen Überblick über Aufgaben und Fragestellungen, die von Nachfolgearbeiten aufgegriffen werden sollten:

- Das gesamte FIM-Umfeld erfordert eine Sensibilisierung der Benutzer, insbesondere im Hinblick auf den Datenschutz und die Möglichkeit, über Attribute Release Policies die Flüsse der eigenen personenbezogenen Daten steuern und kontrollieren zu können. Ein hierbei in der Arbeit bereits mehrfach erwähnter Aspekt ist die Bereitstellung graphischer Benutzeroberflächen, mit denen auch wenig interessierte Benutzer die sie betreffenden Einstellungen effizient und intuitiv vornehmen können.

  Im Kontext dieser Arbeit trifft dies insbesondere auf einen Editor für XACML-basierte Attribute Release Policies zu, der in die webbasierten Self Service Portale vorhandener I&AM-Infrastrukturen integriert werden kann, da ein manuelles Editieren nicht zumutbar und zu fehleranfällig ist. Neben den technischen Aspekten stehen somit insbesondere das Design und die Usability einer derartigen Webapplikation im Vordergrund; zudem sind umfassende Tests mit repräsentativen Anwenderkreisen anzustreben.

- Im Unterschied zu UCIM-Systemen, die bewusst auf die Unterstützung mehrerer Identitäten pro Benutzer ausgelegt sind, fokussieren die bisherigen FIM-Deployments auf eine 1:1–Zuordnung von Benutzern zu Identitäten, Rollen und Identity Providern. Im Hinblick auf eine weitere Verbreitung von FIM ist jedoch davon auszugehen, dass Personen z. B. beruflich und privat in unterschiedlichen Rollen oder mit verschiedenen digitalen Identitäten arbeiten wollen.

  Diese Differenzierung wurde in dieser Arbeit zwar beispielsweise im Namensraumkonzept für Benutzerattribute bereits beachtet, muss aber noch durchgängiger von Single Sign-On Systemen und insbesondere bei Service Providern berücksichtigt werden. In diesem Zusammenhang sind auch die von UCIM-Systemen gebotenen Möglichkeiten zur Zusammenstellung von Antworten an Service Provider aus Attributen verschiedener Rollen oder Identitäten auf die IDP-Software im FIM-Umfeld zu übertragen.

- Ebenfalls analog zu UCIM-Systemen ist die stärkere Integration von Attributszertifikaten zu ermöglichen; diese unterstützen eine vom Identity Provider weitgehend unabhängige Sicherstellung der Richtigkeit und Qualität der Benutzerdaten durch Dritte und sind somit insbesondere für zukünftige dynamische Föderationen relevant, in denen nicht a priori Service Level Agreements zwischen den Föderationsteilnehmern geschlossen werden.

- Die Übertragung von Delegationskonzepten auf FIM-Protokolle ist sowohl bezüglich von Benutzern als auch bezüglich von Service Providern initiierter Delegationsoperationen noch weitgehend offen. Während sie im benutzergesteuerten Fall einem temporären Abtreten eigener Berechtigungen an andere Personen entspricht, wird sie SP-seitig zur Auflösung organisationsübergreifender Dienstabhängigkeiten benötigt.

  Sie ist in beiden Fällen mit dem Risiko verbunden, dass ein Dritter die Identität einer Person annimmt und möglicherweise unkontrolliert missbrauchen kann. Bei einer technischen Umsetzung werden deshalb gegebenenfalls neue Arten von FIM-Transaktionen, die Delegationsaspekte explizit berücksichtigen, sowie über das IDP-seitig reine Protokollieren übermittelter Attribute hinausgehende Kontrollinstanzen notwendig.

Darüber hinaus ist zu berücksichtigen, dass sich über die Weiterentwicklung der clientseitigen Software (vgl. Liberty-enabled User Agents in Abschnitt 3.2.2.1) eine Vielzahl neuer Möglichkeiten ergibt, um die über den Client mittelbare FIM-Kommunikation und die Interaktion mit dem Benutzer effizienter zu gestalten. Dadurch, dass z. B. alle modernen Webbrowser über inzwischen sowohl von Anwendern als auch von Benutzern sehr einfach zu verwendende Plug-In-Mechanismen verfügen, sind die beispielsweise bei frühen Versionen von SAML gestellten Randbedingungen, die vorgesehen haben, dass an die Clientsysteme keinerlei Ansprüche gestellt werden dürfen, zukünftig neu zu überdenken.

8.4. Ausblick auf verwandte offene Forschungsfragestellungen

An mehreren Stellen dieser Arbeit hat sich gezeigt, dass Konzepte aus anderen Fachgebieten FIM-spezifisch erweitert werden müssen.

Auf technischer Ebene betrifft dies insbesondere das Trust Management: Hier fehlen zum einen konkrete Konzepte, wie die für die Konfiguration von Attribute Release und Acceptance Policies notwendigen Trust Levels beispielsweise aus gegebenen Service Level Agreements abgeleitet werden bzw. sich im Rahmen des Reputation Managements dynamisch ändern können. Zum anderen fehlen Organisationsmodelle für Föderationen, die über die bislang praktisch eingesetzten Varianten des *direct* bzw. *brokered trust* hinausgehen. Die Berücksichtigung beider Aspekte ist für die Abbildung der Geschäftsprozesse und die Skalierbarkeit von Föderationen im Hinblick auf die Anzahl der teilnehmenden Einrichtungen mittelfristig unabdingbar.

Aus organisatorischer Sicht sind insbesondere die IT Service Management Prozesse an die durch FIM ermöglichten einrichtungsübergreifenden Kooperationen anzupassen. Insbesondere werden an das Change Management neuartige Anforderungen gestellt, da Änderungen nicht mehr nur lokal stattfinden und je nach Gewicht der eigenen Organisation in einer Föderation nicht abgelehnt oder an lokale Zeitpläne angepasst werden können. Auch für das Configuration

Management und das Release Management müssen neue Methoden entwickelt werden, die das Zusammenwachsen von Organisationen durch gemeinsame Geschäftsprozesse besser abdecken.

Schließlich sind auch weiterführende Untersuchungen im Security Management ausschlaggebend für den erfolgreichen Betrieb von FIM-Infrastrukturen und deren Akzeptanz durch die Benutzer. So müssen einerseits Sicherheitslösungen für virtualisierte Serverumgebungen gefunden werden, über die virtuelle Maschinen gezielt verschiedenen Sicherheitszonen zugeordnet werden können. Andererseits müssen auch für organisationsübergreifende Verbände wie Föderationen und Grids Lösungen für die sich durch neuartige Angriffe und Angreifermodelle ergebenden Probleme gefunden werden.

Insgesamt zeichnet sich damit ab, dass das Federated Identity Management zwar einen essentiellen Beitrag zur Unterstützung organisationsübergreifender Geschäftsprozesse liefert, aber auch in vielen anderen Fachgebieten ähnliche Weiterentwicklungen vormals organisationsinterner Konzepte notwendig sind, um nicht nur die technische, sondern auch die prozessorientierte Integration vollständig zu erreichen.

Anhang A.

Abkürzungen und Terminologie

Dieser Anhang gibt einen Überblick über die in der Arbeit verwendeten Abkürzungen bzw. Akronyme und erläutert knapp die Fachbegriffe.

A.1. Abkürzungen

In der folgenden Tabelle sind die in dieser Arbeit verwendeten Abkürzungen enthalten; zahlreiche FIM-spezifische Begriffe werden in Anhang A.2 näher erläutert.

Abkürzung	**Bedeutung**
AA	Attribute Authority (FIM-Rolle)
AAA	Authentifizierung, Autorisierung und Accounting
AAI	Authentifizierungs- und Autorisierungsinfrastruktur
AAP	Attribute Acceptance Policy (beim Service Provider)
AAR	Projekt „Authentifizierung, Autorisierung und Rechteverwaltung“
ACL	Access Control List
ALG	Application Level Gateway
AP	Authorization Provider (FIM-Rolle)
ARP	Attribute Release Policy (beim Identity Provider)
BBAE	Browser-Based Attribute Exchange
CAB	Change Advisory Board (nach ITIL)
CIM	Common Information Model
DFG	Deutsche Forschungsgemeinschaft
DFN	Deutsches Forschungsnetz
DFN-AAI	Authentifizierungs- und Autorisierungsinfrastruktur des DFN
DIT	Directory Information Tree (Baumstruktur der Daten im LDAP-Server)
DMZ	Demilitarisierte Zone (in Firewallarchitekturen)
DNS	Domain Name System
DVO	Dynamische Virtuelle Organisation
EAI	Enterprise Application Integration
FIM	Federated Identity Management
FSCS	Federation Schema Correlation Service
FUP	Federated User Provisioning

Abkürzung	**Bedeutung**
I&AM	Identity & Access Management
IDP	Identity Provider (FIM-Rolle)
IDS	Intrusion Detection System
ID-WSF	Liberty Alliance Identity Web Services Framework
IETF	Internet Engineering Task Force
IF	Identity Federation
ITIL	IT Infrastructure Library
IPS	Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol
LMS	Learning Management System (Anbieterseitige E-Learning-Software)
MWN	Münchner Wissenschaftsnetz
NIS	Network Information Service
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PET	Privacy Enhancing Technologies
PIP	Policy Information Point
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PMS	Privacy Management System
PR	Policy Repository
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SLB	Service Load Balancer (Komponente zur Lastverteilung)
SLO	Single Logout (komplementär zu SSO)
SP	Service Provider (FIM-Rolle)
SPML	Service Provisioning Markup Language
SSO	Single Sign-On
TTP	Trusted Third Party
UCIM	User-Centric Identity Management
UP	User Provisioning
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VHB	Virtuelle Hochschule Bayern
WAYF	Where Are You From? (Komponente von Shibboleth)
WS-*	Web Services Stack (Protokollfamilie)
XACML	eXtensible Access Control Markup Language
XSLT	eXtensible Stylesheet Language Transformation

A.2. Terminologie

In der nachfolgenden Tabelle wird das in dieser Arbeit verwendete Fachvokabular knapp erläutert; auf an anderer Stelle ausführlicher dargestellte Begriffe wird dabei lediglich verwiesen.

Begriff, Synonyme	**Erklärung**
Anonymität	Eigenschaft, nicht von anderen Benutzern eines Dienstes unterschieden werden zu können, vgl. Abschnitt 2.1.2.4 auf Seite 45.
Assertion, Bestätigung, Auskunft	In Anlehnung an SAML werden *authentication*, *authorization* und *attribute assertions* unterschieden, vgl. Abschnitt 2.1.2.2 auf Seite 39.
Attribut	Über eine Identität erfasstes Datenfeld, z. B. `Nachname`, vgl. Abschnitt 2.1.2.4 auf Seite 42.
Attribute Acceptance Policy	Spezifikation, welche allgemeinen Attributsauskünfte ein SP akzeptiert, in Form einer maschinell verarbeitbaren Policy.
Attribute Authority	Siehe Abschnitt 2.1.2.3 auf Seite 40.
Attribute Release Policy	Spezifikation, welche allgemeinen Attributsauskünfte über eine Identität von einem IDP bzw. einer AA gemacht werden dürfen, in Form einer maschinell verarbeitbaren Policy.
Federation, Identity Federation, Föderation	Menge von Organisationen, die sich zum Zweck des FIM-basierten Datenaustausches zusammengeschlossen haben.
Identity Provider, IDP	Siehe Abschnitt 2.1.2.3 auf Seite 40.
Policy Decision Point	An einer Autorisierungsarchitektur beteiligte Komponente, die auf Basis eines als Policy vorliegenden Regelwerks entscheidet, ob bzw. welche Aktion durchgeführt werden soll, z. B. ob ein Benutzer Zugriff auf einen bestimmten Dienst erhalten soll.
Policy Enforcement Point	Komponente einer Autorisierungsarchitektur, die die von einem PDP gefällte Entscheidung umsetzt und beispielsweise einem Benutzer den Zugang zu einem Dienst verwehrt.
Privacy	Aus Datenschutzperspektive das Recht jeder Person, darüber zu bestimmen, welche personenbezogenen Daten von anderen genutzt werden dürfen.
Privacy Enhancing Technologies	Forschungsgebiet, das sich mit der Entwicklung neuer bzw. verbesserter Technologien im Bereich Privacy beschäftigt.
Privilege Management Infrastructure	Oberbegriff für Autorisierungsarchitekturen, mindestens bestehend aus PDP und PEP; praktisch sind in der Regel weitere Komponenten wie Policy Administration und Information Points beteiligt.

Begriff, Synonyme	**Erklärung**
Public Key Infrastructure	Organisatorische und technische Infrastruktur für das Management digitaler Zertifikate. Zertifikate werden von einer Certificate Authority (CA) ausgestellt, deren Vertrauenswürdigkeit anerkannt werden muss, und können nur überprüft werden, wenn auch das Zertifikat der CA vorliegt; die Komplexität von Föderationen wächst deshalb mit der Anzahl beteiligter CAs.
Security Assertion Markup Language	FIM-Standard, der insbesondere die Syntax und Semantik von *Assertions* definiert, vgl. Abschnitt 3.2.1.
Service Provider, Dienstanbieter, SP	Siehe Abschnitt 2.1.2.3 auf Seite 40.
Single Log-Out	Möglichkeit, sich bei allen derzeit genutzten Diensten auf einmal abmelden zu können, ohne die Nutzung jedes Dienstes separat beenden zu müssen.
Single Sign-On	SSO ist erreicht, wenn es zur Nutzung mehrerer, u. U. mit unterschiedlichen Passwörtern geschützter Dienste ausreicht, sich bei einem davon zu authentifizieren und die anderen Dienste im Anschluss ohne erneute Authentifizierung genutzt werden können.
Trust Level t_{AB_i}	Angabe des Vertrauensgrads zwischen zwei Entitäten A und B bezüglich des mittels FIM zu übertragenden Datentyps i, vgl. Abschnitt 2.1.2.5 auf Seite 47.
Unified Login	Nutzung mehrerer IT-Dienste mit derselben Kombination aus Benutzername und Passwort; im Unterschied zum Single Sign-On muss der Benutzer von jedem Dienst explizit authentifiziert werden.
Uniform Resource Identifier	Zeichenkette zur Identifikation einer Ressource; dabei werden die nachfolgend erläuterten Unterarten URLs und URNs unterschieden.
Uniform Resource Locator	Angabe von Zugriffsmechanismus und Ort einer Ressource, beispielsweise `http://www.example.com/`.
Uniform Resource Name	Dauerhafter, ortsunabhängiger Bezeichner für eine Ressource, der mit dem Präfix `urn:` beginnt und über Doppelpunkte in Namensräume untergliedert ist, z. B. gibt `urn:mace:shibboleth:arp:1.0` die Version 1.0 der Policysprache für Shibboleth-ARPs an.
User Provisioning, Provisioning	Einspeisen von Benutzerinformationen in ein zur Diensterbringung notwendiges System, z. B. auf Basis von Provisioningsystemen oder Meta-Directories (vgl. Abschnitt 2.1.1.5 auf Seite 21).

Begriff, Synonyme	**Erklärung**
Web Service	Über eine URI eindeutig identifizierbare Schnittstelle einer Softwarekomponente, mit der über das TCP/IP- und XML-basierte Protokoll SOAP kommuniziert werden kann. Die Schnittstellenbeschreibung erfolgt in der Sprache WSDL (Web Service Description Language); eine Registry von Web Services kann mittels UDDI (Universal Description, Discovery and Integration) realisiert werden.
Web Services Stack	Protokollfamilie zur Realisierung verschiedener Aspekte von Web Services, beispielsweise WS-Trust und WS-Federation (siehe Kapitel 3).

Anhang B.

Literaturverzeichnis

[ABLY04] Annie I. Anton, Elisa Bertino, Ninghui Li und Ting Yu: *A Roadmap for comprehensive online Privacy Policy.* Technischer Bericht 2004-47, CERIAS Center for Education and Research in Information Assurance and Security, Perdue University, West Lafayette, IN 47907-2086, 2004.

[ADdV+05] C. Ardagna, E. Damiani, S. De Capitani di Vimercati, C. Fugazza und P. Samarati: *Offline Expansion of XACML Policies Based on P3P Metadata.* In: *Proceedings of the 5th International Conference on Web Engineering, ICWE 2005*, Seiten 363–374. Springer Verlag, 2005.

[ADdVS05] C. A. Ardagna, E. Damiani, S. De Capitani di Vimercati und P. Samarati: *Towards Privacy-Enhanced Authorization Policies and Languages.* In: *Proceedings of the 19th Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Seiten 16–27. Springer Verlag, 2005.

[AHKS02] Paul Ashley, Satoshi Hada, Günter Karjoth und Matthias Schunter: *E-P3P Privacy Policies and Privacy Authorization.* In: *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society (WPES 2002).* ACM Press, November 2002.

[AL04] Anne Anderson und Hal Lockhart: *SAML 2.0 Profile of XACML 2.0.* OASIS TC Committee draft, 11. November 2004, 2004.

[And04a] Anne Anderson: *XML Digital Signature profile of XACML 2.0.* OASIS TC Committee draft, 16. September 2004, 2004.

[And04b] Anne H. Anderson: *A Comparison of EPAL and XACML.* `http://research.sun.com/projects/xacml/CompareEPALandXACML.html`, 2004.

[And04c] Anne H. Anderson: *An Introduction to the Web Services Policy Language (WSPL).* In: *Proceedings of the 5th IEEE International Workshop on Policies for Distributed Systems and Networks.* IEEE Press, 2004.

[And04d] Anne H. Anderson: *The Relationship Between XACML and P3P Privacy Policies.* `http://research.sun.com/projects/xacml/`, 2004.

[And05] Anne Anderson: *Key Differences between XACML and EPAL.* Technischer Bericht, Sun Microsystems Lab, Burlington, MA, USA, 2005.

[Ange06] Wolfgang Anger: *Planning and implementing of user self services and master user services for the identity management portal of the Leibniz Supercomputing Center Munich.* Diplomarbeit an der Technischen Universität München, Fakultät für Informatik, 2006.

[APPEL] Marc Langheinrich (Hrsg.): *A P3P Preference Exchange Language — APPEL 1.0.* `http://www.w3.org/TR/P3P-preferences/`, 2002.

[BBAE] Birgit Pfitzmann und Michael Waidner: *BBAE — a general protocol for browser-based attribute exchange.* Technischer Bericht RZ 3455 (#93800), IBM Research, Zürich, 2002.

[BBAEPR] Birgit Pfitzmann: *Privacy in browser-based attribute exchange.* In: *Proceedings of the ACM Workshop on Privacy in Electronic Society (WPES 2002)*, Seiten 52–62. ACM Press, 2002.

[BBF+06] Tom Barton, Jim Basney, Tim Freeman, Tom Scavo, Frank Siebenlist, Von Welch, Rachana Ananthakrishnan, Bill Baker, Monte Goode und Kate Keahey: *Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy.* Technischer Bericht PKI-06, GridShib Technical Report, April 2006.

[BBG05] Rafae Bhatti, Elisa Bertino und Arif Ghafoor: *A policy framework for access management in federated information sharing.* In: *Proceedings of the 2005 IFIP Conference on Security Management, Integrity, and Internal Control in Information Systems.* Springer Verlag, Dezember 2005.

[BBKS04] Michael Backes, Walid Bagga, Günter Karjoth und Matthias Schunter: *Efficient Comparison of Enterprise Privacy Policies.* In: *Proceedings of SAC 2004*, Seiten 375–382. ACM Press, März 2004.

[BDS04] Michael Backes, Markus Dürmuth und Rainer Steinwandt: *An Algebra for Composing Enterprise Privacy Policies.* In: *Proceedings of ESORICS 2004*, Band 3193 der Reihe *LNCS*. Springer Verlag, September 2004.

[BJWW02a] Claudio Bettini, Sushil Jajodia, X. Sean Wang und Duminda Wijesekera: *Obligation Monitoring in Policy Management.* In: *Proceedings of the 3rd IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2002)*, Seiten 2–12. IEEE Press, 2002.

[BJWW02b] Claudio Bettini, Sushil Jajodia, X. Sean Wang und Duminda Wijesekera: *Provisions and Obligations in Policy Management and Security Applications.* In: *Proceedings of the 28th Very Large Databases Conference (VLDB 2002).* Morgan Kaufmann, August 2002.

[BJWW03] Claudio Bettini, Sushil Jajodia, X. Sean Wang und Duminda Wijesekera: *Provisions and Obligations in Policy Rule Management.* In: *Journal of Network and Systems Management*, Band 11, Seiten 351–372. Plenum Publishing Corporation, März 2003.

[BLN86] C. Batini, M. Lenzerini und S. Navathe: *A comparative analysis of methodologies for database schema integration.* In: *ACM Computing Surveys (CSUR) Volume 18, Issue 4*, Seiten 323–364, New York, NY, USA, 1986. ACM Press.

[BM05] Adam Barth und John C. Mitchell: *Enterprise privacy promises and enforcement.* In: *Proceedings of WITS 2005*, Seiten 58–66. ACM Press, Januar 2005.

[BMR+98] Frank Buschmann, Regine Meunier, Hans Rohnert, Peter Sommerlad und Michael Stal: *Pattern-orientierte Softwarearchitektur – Ein Pattern-System.* Addison-Wesley-Longman Verlag, 1998.

[BMR04] Adam Barth, John C. Mitchell und Justin Rosenstein: *Conflict and Combination in Privacy Policy Languages.* In: *Proceedings of WPES 2004*, Seiten 45–46. ACM Press, Oktober 2004.

[Bos00] Jan Bosch: *Design and Use of Software Architectures.* Addison-Wesley Verlag, 2000.

[BPS03] Michael Backes, Birgit Pfitzmann und Matthias Schunter: *A Toolkit for Managing Enterprise Privacy Policies.* In: *Proceedings of ESORICS 2003*, Nummer 2808 in *LNCS*, Seiten 162–180. Springer Verlag, Oktober 2003.

[BuiBl1] Johannes Meinecke, Martin Nussbaumer und Martin Gaedke: *Building Blocks for Identity Federations.* In: *Proceedings of International Conference on Web Engineering ICWE 2005*, LNCS. Springer, 2005.

[BuiBl2] Martin Gaedke, Johannes Meinecke und Martin Nussbaumer: *A Modeling Approach to Federated Identity and Access Management.* In: *Proceedings of WWW 2005.* ACM Press, Mai 2005.

[CARDEA] Rebekah Lepro: *Cardea: Dynamic Access Control in Distributed Systems.* Technischer Bericht TR NAS-03-020, NASA Advanced Supercomputing Division, Ames, 2003.

[CARDSP] David Chappell: *Introducing Windows CardSpace.* Microsoft Developer Network MSDN, http://msdn.microsoft.com/winfx/reference/infocard, 2006.

[CMP05] Stephen Crane, Marco Mont und Siani Pearson: *On Helping Individuals to Manage Privacy and Trust.* Technischer Bericht HPL-2005-53, HP Laboratories Bristol, März 2005.

[CPXCHG] Kathy Bohrer und Bobby Holland: *Customer Profile Exchange (CPexchange) Specification.* `http://www.cpexchange.org/`, 2000.

[CRE87] B. Czejdo, M. Rusinkiewicz und D. Embley: *An Approach to Schema Integration and Query Formulation in Federated Database Systems.* In: *Proceedings of the Third International Conference on Data Engineering*, Seiten 477–484, Washington, DC, USA, 1987. IEEE Computer Society.

[CYS+05] Hyang-Chang Choi, Yong-Hoon Yi, Jae-Hyun Seo, Bong-Nam Noh und Hyung-Hyo Lee: *A Privacy Protection Model in ID Management Using Access Control*. In: O. Gervasi (Herausgeber): *Proceedings of ICCSA 2005*, Band 3481 der Reihe *LNCS*, Seiten 82–91. Springer, 2005.

[DEEP] Peter Gietz: *TERENA DEEP Project (Definition of a European EduPerson)*. `http://www.terena.org/activities/tf-lsd/projects/DEEPFinalReport.pdf`, 2002.

[DIX] J. Merrells, P. Rowley, J. Sermersheim und M. Pohlman: *DIX: Digital Identity Exchange Protocol*. IETF Spezifikation, IETF Network Working Group, Mai 2006.

[DIXUSE] J. Merrells: *Digital Identity Exchange – Use Cases*. Technischer Bericht, IETF Network Working Group, Mai 2006.

[DLC03] Timon Chih-Ting Du, Hsun-Ming Lee und Ane Chen: *Constructing federated databases in coordinated supply chains*. In: *Decision Support Systems, Volume 36, Issue 1*, Seiten 49–64, Amsterdam, 2003. Elsevier Science Publishers.

[DN03] Péter Dornbach und Zoltán Németh: *Privacy Enhancing Profile Disclosure*. In: *Proceedings of Workshop on Privacy Enhancing Technologies (PET 2002)*, Band 2482 der Reihe *LNCS*. Springer Verlag, 2003.

[DXZ06] Jim Dowd, Shouhuai Xu und Weining Zhang: *Privacy-Preserving Decision Tree Mining Based on Random Substitutions*. In: *Proceedings of International Conference on Emerging Trends in Information and Communication Security*, Band 3995 der Reihe *Lecture Notes in Computer Science, LNCS 3995*, Seiten 145–159, Freiburg, Juni 2006. Springer.

[Eber06] Matthias Ebert: *Konzeption und Implementierung einer policy-basierten Privacy Management Architektur für föderierte Identitätsmanagementsysteme am Beispiel Shibboleth*. Diplomarbeit an der Ludwig-Maximilians-Universität München, Institut für Informatik, 2006.

[EbZu05] Matthias Ebert und Sebastian Zunhammer: *Implementation of a web single sign-on prototype for the Munich Scientific Network based on Shibboleth*. Fortgeschrittenen-Praktikum an der Ludwig-Maximilians-Universität München, Institut für Informatik, 2005.

[EDUPER] Keith Hazelton: *EduPerson Object Class Specification (200312)*. `http://www.educause.edu/eduperson/`, 2003.

[ELBA07] Christian Emig, Kim Langner, J. Biermann und Sebastian Abeck: *Semantic Integration of Identity Data Repositories*. In: *Proceedings der Konferenz Kommunikation in Verteilten Systemen (KiVS 2007)*. Springer Verlag, 2007.

[EP3P] Günther Karjoth, Matthias Schunter und Michael Waidner: *The Platform for Enterprise Privacy Practices — Privacy-enabled Management of Customer Data*. In: *Proceedings of the Workshop on Privacy Enhancing Technologies, PET 2002*. Springer Verlag, 2002.

[EPAL12] Calvin Powers und Matthias Schunter: *Enterprise Privacy Authorization Language — EPAL 1.2.* Technischer Bericht RZ 3485 (#93951), IBM Research, Zürich, 2003.

[EPALP3] Matthias Schunter, Els van Herreweghen und Michael Waidner: *Translating EPAL to P3P – How to keep enterprise privacy promises in sync with the actual practices.* IBM Research Positional Paper, 2003.

[EPALW3] Calvin Powers und Matthias Schunter: *Enterprise Privacy Authorization Language, W3C member submission.* `http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/`, 2003.

[EU-DSR] Europäische Gemeinschaft: *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.* Amtsblatt der EG Nr. L 281 vom 23. November 1995 S. 31, 1995.

[GRDSHB] Von Welch, Tom Barton, Kate Keahey und Frank Siebenlist: *Attributes, Anonymity, and Access: Shibboleth and Globus Integration to Facilitate Grid Collaboration.* In: *Proceedings of the Internet2 PKI R&D Workshop 2005*, 2005.

[GRIDSA] Erik Vullings, Markus Buchhorn und James Dalziel: *Secure Federated Access to GRID applications using SAML/XACML.* Technischer Bericht, Macquarie University, Sydney, 2005.

[Gro03] Thomas Gross: *Security Analysis of the SAML Single Sign-On Browser/Artifact Profile.* In: *19th Annual Computer Security Applications Conference (ACSAC 2003).* IEEE Press, 2003.

[HAN99] Heinz-Gerd Hegering, Sebastian Abeck und Bernhard Neumair: *Integriertes Management vernetzter Systeme — Konzepte, Architekturen und deren betrieblicher Einsatz.* dpunkt-Verlag, ISBN 3-932588-16-9, Januar 1999.

[HGMM05] Markus Hillenbrand, Joachim Götze, Jochen Müller und Paul Müller: *A Single Sign-On Framework for Web-Services-based Distributed Applications.* In: *Proccedings of 8th International Conference on Telecommunications – ConTEL 2005.* IEEE Press, Juni 2005.

[Hom05a] Wolfgang Hommel: *Using XACML for Privacy Control in SAML-based Identity Federations.* In: *Proceedings of the 9th Conference on Communications and Multimedia Security (CMS 2005)*, Salzburg, Austria, September 2005.

[Hom05b] Wolfgang Hommel: *An Architecture for Privacy-aware Inter-domain Identity Management.* In: *Proceedings of the 16th IFIP/IEEE Distributed Systems: Operations and Management (DSOM 2005)*, Barcelona, Spain, Oktober 2005.

[Hom06a] Wolfgang Hommel: *Policy-based Integration of User- and Provider-sided Identity Management.* In: *Proceedings of International Conference on Emerging Trends in Information and Communication Security (ETRICS 2006)*, Band 3995 der Reihe *Lecture Notes in Computer Science, LNCS 3995*, Heidelberg, Juni 2006. Springer Verlag.

[HoRe05a] Wolfgang Hommel und Helmut Reiser: *Federated Identity Management in B2B Outsourcing.* In: *Proceedings of the 12th Annual Workshop of the HP OpenView University Association (HPOVUA 2005)*, Porto, Portugal, Juli 2005. ISBN 972-9171-48-3.

[HoRe05b] Wolfgang Hommel und Helmut Reiser: *Federated Identity Management: Shortcomings of existing standards.* In: *Proceedings of the 9th IFIP/IEEE International Symposium on Integrated Management (IM 2005)*, Nice, France, Mai 2005.

[HSN05] Steffen M. Hansen, Jakob Skriver und Hanne Riis Nielson: *Using Static Analysis to Validate the SAML Single Sign-On Protocol.* In: *Proceedings of WITS'05.* ACM Press, Januar 2005.

[HURDER] Greg Wettstein: *The Hurderos Project – A Model for Identity Based Information Management and Delivery*, 2005. `http://www.hurderos.org/`.

[IDEMIXa] Jan Camenisch und Els Van Herreweghen: *Design and Implementation of the idemix Anonymous Credential System.* In: *Proceedings of CCS 2002*, Seiten 21–30. ACM Press, 2002.

[IDEMIXb] Jan Camenisch und Dieter Sommer: *Architecture for using the idemix Privacy Certificate System for Identity Federation, Draft 0.6.* Technischer Bericht, IBM Research, Zurich Research Laboratory, 2005.

[IM4EVR] Jan Camenisch, Abhi Shelat, Dieter Sommer, Simone Fischer-Hübner, Marit Hansen, Henry Krasemann, Gerard Lacoste, Ronald Leenes und Jimmy Tseng: *Privacy and Identity Management for Everyone.* In: *Proceedings on 1st conference on Digital Identity Management.* ACM Press, November 2005.

[IMSURV] Teruko Miyata, Yuzo Koga, Paul Madsen, Shin ichi Adachi, Yoshitsugu Tsuchiya, Yasuhisa Sakamoto und Kenji Takahashi: *A Survey on Identity Management Protocols and Standards.* In: *IEICE Transactions on Information and Systems, Vol. E89-D.* IEICE, 2006.

[INFREL] Piero A. Bonatti und Pierangela Samarati: *Regulating Service Access and Information Release on the Web.* In: *Proceedings of CCS '00, Athens.* ACM Press, 2000.

[IPPBAC] Kathy Bohrer, Stephan Levy, Xuan Liu und Edith Schonberg: *Individualized Privacy Policy Based Access Control.* In: *Proceedings 6th International Conference on Electronic Commerce Research*, ICECR, 2003.

[JHF03] Ken Jordan, Jan Hauser und Steven Foster: *The Augmented Social Network: Building Identity and Trust into the next-generation Internet.* Technischer Bericht, Planetwork, Conference on Networking A Sustainable Future, Juni 2003.

[KM05] Michael Koch und Kathrin Möslein: *Identities Management for E-Commerce and Collaboration Applications.* International Journal of Electronic Commerce (IJEC), 2005.

[Koch02] Michael Koch: *Global Identity Management to Boost Personalization.* In: P. Schubert und U. Leimstoll (Herausgeber): *Proceedings of 9th Research Symposium on Emerging Electronic Markets*, Seiten 137–147, September 2002.

[LAAUTH] Paul Madsen (Hrsg.): *Liberty ID-FF Authentication Context Specification.* Normative Liberty Alliance Specification, Draft, 2004.

[LABIND] Scott Cantor, John Kemp und Daryll Champagne (Hrsg.): *Liberty ID-FF Bindings and Profiles Specification v1.2.* Normative Liberty Alliance Specification, 2004.

[LACBS] Sampo Kellomäki (Hrsg.): *Liberty ID-SIS Contact Book Service Specification.* Normative Liberty Alliance Specification, 2005.

[LACONF] Eric Tiffany (Hrsg.): *Liberty ID-FF 1.2 Static Conformance Requirements.* Normative Liberty Alliance Specification, 2004.

[LADISC] John Beatty, Jeff Hodges und Jonathan Sergent (Hrsg.): *Liberty ID-WSF Discovery Service Specification.* Liberty Alliance Specification, 2004.

[LAEmpP] Sampo Kellomäki (Hrsg.): *Liberty ID-SIS Employee Profile Service Specification.* Normative Liberty Alliance Specification, 2003.

[LAEPGL] Sampo Kellomäki und Tom Wason (Hrsg.): *Liberty ID-SIS Employee Profile Service Implementation Guidelines.* Liberty Alliance Specification, 2003.

[LAEUAD] Robert Aarts (Hrsg.): *Liberty ID-WSF Profiles for Liberty enabled User Agents and Devices.* Liberty Alliance Specification, 2004.

[LAGLS] Jukka Kainulainen (Hrsg.): *Liberty ID-SIS Geolocation Service Specification.* Normative Liberty Alliance Specification, 2005.

[LAIDFF] Peter Thompson und Darryl Champagne (Hrsg.): *Liberty ID-FF Implementation Guidelines v1.2.* Liberty Alliance Specification, 2004.

[LAISS] Robert Aarts (Hrsg.): *Liberty ID-WSF Interaction Service Specification.* Liberty Alliance Specification, 2004.

[LAMETA] Peter Davis (Hrsg.): *Liberty Metadata Description and Discovery Specification.* Normative Liberty Alliance Specification, 2004.

[LAOVER] Thomas Wason (Hrsg.): *Liberty ID-FF Architecture Overview v1.2.* Liberty Alliance Specification, 2004.

[LAPerP] Sampo Kellomäki (Hrsg.): *Liberty ID-SIS Personal Profile Service Specification.* Normative Liberty Alliance Specification, 2003.

[LAPPGL] Sampo Kellomäki und Tom Wason (Hrsg.): *Liberty ID-SIS Personal Profile Service Implementation Guidelines.* Liberty Alliance Specification, 2003.

[LAPRES] Peter Saint-Andre (Hrsg.): *Liberty ID-SIS Presence Service Specification.* Normative Liberty Alliance Specification, 2005.

[LAPRIV] Christine Varney (Hrsg.): *Liberty Alliance: Privacy and Security Best Practices*. Liberty Alliance Specification, November 2003.

[LAPROT] Scott Cantor und John Kemp (Hrsg.): *Liberty ID-FF Protocols and Schema Specification v1.2*. Normative Liberty Alliance Specification, 2004.

[LAPSS] Yuzo Kofa und Paul Madsen (Hrsg.): *Liberty ID-WSF People Service Specification*. Liberty Alliance Specification, Januar 2006.

[LASUBS] Sampo Kellomäki (Hrsg.): *Liberty ID-WSF Subscriptions and Notifications*. Liberty Alliance Specification, 2006.

[LATRST] John Linn (Hrsg.): *Liberty Trust Models Guidelines*. Liberty Alliance Specification, 2003.

[LAWDS] Jukka Kainulainen und Aravindan Ranganathan (Hrsg.): *Liberty ID-WSF Data Services Template Specification*. Liberty Alliance Specification, 2005.

[LAWOVR] Jonathan Tourzan und Yuzo Koga (Hrsg.): *Liberty ID-WSF Web Services Framework Overview*. Liberty Alliance Specification, 2004.

[LAWS] Kim Cameron: *The Laws of Identity*. Microsoft Corporation, `http://www.identityblog.com/?page_id=354`, Dezember 2005.

[LAWSFC] Greg Whitehead (Hrsg.): *Liberty ID-WSF 1.0 Static Conformance Requirements*. Liberty Alliance Specification, 2004.

[LGMC05] Gabriel Lopez, Antonio Gomez, Rafael Marin und Oscar Canovas: *A Network Access Control Approach Based on the AAA Architecture and Authorization Attributes*. In: *Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium*. IEEE Press, 2005.

[LTB06] Adam Lee, Parisa Tabriz und Nikita Borisov: *A privacy-preserving interdomain audit framework*. In: *Proceedings of the 5th ACM workshop on Privacy in electronic society*, Alexandria, Virginia, USA, 2006. ACM Press.

[MAMS] J. R. Dalziel und Erik Vullings: *MAMS and middleware: The easily solved authentication, authorization, identity, single-sign-on, federation, trust, security, digital rights and automated access policy cluster of problems*. In: *Proceedings of EDUCAUSE 2005*, 2005.

[MCCP06] U. M. Mbanaso, G. S. Cooper, David Chadwick und Seth Proctor: *Privacy Preserving Trust Authorization Framework using XACML*. In: *Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia*. IEEE Press, 2006.

[MIDM] Stephen Downes: *mIDm – Self-Identification on the World Wide Web*. http://www.downes.ca/midm.htm, Mai 2005.

[MKT05] Paul Madsen, Yuzo Koga und Kenji Takahasi: *Federated Identity Management for Protecting Users from ID Theft*. In: *Proceedings of the Workshop on Digital Identity Management (DIM 2005)*, Seiten 77–83. ACM Press, November 2005.

[Mont04a] Marco Mont: *Dealing with Privacy Obligations: Important Aspects and Technical Approaches.* Technischer Bericht HPL-2004-34, HP Laboratories Bristol, 2004.

[Mont04b] Marco Mont: *Dealing with Privacy Obligations in Enterprises.* Technischer Bericht HPL-2004-109, HP Laboratories Bristol, 2004.

[Mont04c] Marco Mont: *Identity Management: On the "Identity = Data + Policies" Model.* Technischer Bericht HPL-2004-14, HP Laboratories Bristol, 2004.

[MTCB05] Marco Mont, Robert Thyne, Kwok Chan und Pete Bramhall: *Privacy Management Technology Improves Governance.* In: *Proceedings of the 12th Annual Workshop of the HP OpenView University Association (HPOVUA 2005)*, Porto, Portugal, Juli 2005. ISBN 972-9171-48-3.

[NYMITY] I. Goldberg: *A Pseudonymous Communications Infrastructure for the Internet.* Doktorarbeit, University of California, Berkeley, 2000.

[OpenID] D. Recordon und B. Fitzpatrick: *OpenID Authentication 1.1 Specification.* http://www.openid.net/specs/, Mai 2006.

[OWNCTL] Carrie Gates und Jacob Slonim: *Owner-Controlled Information.* In: *Proceedings of New Security Paradigms Workshop 2003*, Ascona, Switzerland, 2003. ACM Press.

[P3P] Joseph Reagle und Lorrie F. Cranor: *The Platform for Privacy Preferences.* In: *Communications of the ACM*, Band 42, Seiten 48–55. ACM Press, 1999.

[P3PIDM] Oliver Berthold und Marit Köhntopp: *Identity management based on P3P.* In: *International workshop on Designing privacy enhancing technologies*, Seiten 141–160, New York, NY, USA, 2001. Springer-Verlag New York, Inc.

[P3PSEM] E. Damiani, S. De Capitani di Vimercati, C. Fugazza und P. Samarati: *Semantics-aware Privacy and Access Control: Motivation and Preliminary Results.* In: *Proceedings of 1st Italian Semantic Web Workshop*, Dezember 2004.

[PAPL06] Ruoming Pang, Mark Allman, Vern Paxson und Jason Lee: *The devil and packet trace anonymization.* In: *ACM SIGCOMM Computer Communication Review, Vol. 36, Issue 1*, New York, USA, 2006. ACM Press.

[PARADI] Ernesto Damiani, Sabrina De Capitani di Vimercati und Pierangela Samarati: *New Paradigms for Access Control in Open Environments.* In: *Proceedings of the 5th IEEE International Symposium on Signal Processing and Information Technology.* IEEE Press, Dezember 2005.

[PERMIS] David Chadwick und Alexander Otenko: *The PERMIS X.509 Role Based Privilege Management Infrastructure.* In: *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies*, SACMAT, Seiten 135–140. ACM Press, 2002.

[PERSIM] Kathy Bohrer, Xuan Liu, Dogan Kesdogan, Edith Schonberg, Moninder Singh und Susan Spraragen: *Personal Information Management and Distribution*. In: *4th International Conference on Electronic Commerce Research ICECR-4*, 2001.

[PESA] Tero Alamäki, Margareta Björksten, Péter Dornbach, Casper Gripenberg, Norbert Györbiró, Gábor Márton, Zoltán Németh, Timo Skyttä und Mikko Tarkiainen: *Privacy Enhancing Service Architectures*. In: *Proceedings of Workshop on Privacy Enhancing Technologies (PET 2002)*, Band 2482 der Reihe *LNCS*. Springer Verlag, 2003.

[PfWa03] Birgit Pfitzmann und Michael Waidner: *Federated Identity Management Protocols — Where User Authentication Protocols May Go*. In: *11th Cambridge Workshop on Security Protocols*. Springer, 2003.

[PIMWAY] Chris Connolly: *Managing Privacy in Identity Management - The Way Forward*. `http://www.agimo.gov.au/publications/2004/05/egovt_challenges/privacy/identity`, Mai 2004.

[PKIFL] Javier Lopez, Rolf Opplinger und Günther Pernul: *Why have Public Key Infrastructures failed so far?* Emerald Internet Research, 15(5), Oktober 2005.

[PONDER] Nicodemos Damianou, Naranker Dulay, Emil Lupu und Morris Sloman: *The Ponder Policy Specification Language*. Lecture Notes in Computer Science, 1995, 2001.

[PP03] Ruoming Pang und Vern Paxson: *A high-level programming environment for packet trace anonymization and transformation*. In: *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, Karlsruhe, Germany, 2003. ACM Press.

[Pre05] Sören Preibusch: *Implementing Privacy Negotiation Techniques in E-Commerce*. In: *Proceedings of the 7th IEEE International Conference on E-Commerce Technology*. IEEE Press, 2005.

[PREP] Gail-Joon Ahn und John Lam: *Managing Privacy Preferences for Federated Identity Management*. In: *Proceedings of 1st Workshop on Digital Identity Management (DIM'05)*. ACM Press, November 2005.

[PRIMET] Louis-Francois Pau: *PRIME Requirements V1 Part 2 Privacy Metrics and Service Level Agreements*. Technischer Bericht D1.1.b part 2, PRIME Consortium, Juni 2005.

[PRIPOL] Günther Karjoth und Matthias Schunter: *A Privacy Policy Model for Enterprises*. In: *Proceedings of the 15th IEEE Computer Foundations Workshop*. IEEE Press, 2002.

[PRISER] Günther Karjoth, Matthias Schunter und Michael Waidner: *Privacy-enabled Services for Enterprises*. `http://www.research.ibm.com/privacy/`, 2002.

[PRIVEC] Bettina Berendt, Oliver Günther und Sarah Spiekermann: *Privacy in E-Commerce.* Communications of the ACM, 48(4), April 2005.

[PRUSAB] John Sören Pettersson, Simone Fischer-Hübner, Ninni Danielsson, Jenny Nilsson, Mike Bergmann, Sebastian Clauss, Thomas Kriegelstein und Henry Krasemann: *Making PRIME Usable.* In: *Proceedings of the Symposium on usable privacy and security (SOUPS).* ACM Press, Juli 2005.

[PW02] Birgit Pfitzmann und Michael Waidner: *Token-based Web Single Signon with Enabled Clients.* Technischer Bericht RZ 3458 (#93844), IBM Research, Zürich, 2002.

[QUALIN] Sebastian Clauss: *A Framework for Quantification of Linkability Within a Privacy-Enhancing Identity Management System.* In: *Proceedings of International Conference on Emerging Trends in Information and Communication Security*, Band 3995 der Reihe *Lecture Notes in Computer Science, LNCS 3995*, Seiten 191–205, Freiburg, Juni 2006. Springer.

[REIDEN] Sebastian Clauss, Dogan Kesdogan und Tobias Kölsch: *Privacy Enhancing Identity Management: Protection Against Re-identification and Profiling.* In: *Proceedings of 1st Workshop on Digital Identity Management (DIM'05).* ACM Press, November 2005.

[RFCAC] S. Farrell und R. Housley: *RFC 3821: An Internet Attribute Certificate Profile for Authorization.* Technischer Bericht RFC 3281, IETF, Network Working Group, 2002.

[RFCIOP] M. Smith: *Definition of the inetOrgPerson LDAP Object Class.* IETF Proposed Standard, RFC 2798, 2000.

[RFCPXA] L. Howard: *An Approach for Using LDAP as a Network Information Service.* IETF Proposed Standard, RFC 2307, 1998.

[Ric05] Brian Richardson: *An Architecture for Identity Management.* Diplomarbeit, University of Saskatchewan, Juni 2005.

[RL97] Ron Rivest und Butler Lampson: *S-Expressions for use in SDSI and SPKI.* `http://theory.lcs.mit.edu/~rivest/sexp.html`, 1997.

[ROLPOL] Marco-Casassa Mont, A. Baldwin und C. Goh: *Role of Policies in a Distributed Trust Framework.* Technischer Bericht HPL-1999-104, HP Laboratories Bristol, Bristol, September 1999.

[RS06] Dominik Raub und Rainer Steinwandt: *An Algebra for Enterprise Privacy Policies Closed Under Composition and Conjunction.* In: *Proceedings of International Conference on Emerging Trends in Information and Communication Security (ETRICS 2006)*, Band 3995 der Reihe *Lecture Notes in Computer Science, LNCS 3995*, Seiten 130–144, Heidelberg, Juni 2006. Springer Verlag.

[S2AUTH] John Kemp, Scott Cantor, Prateek Mishra, Rob Philpott und Eve Maler (Hrsg.): *Authentication Context for the OASIS Security Assertion*

Markup Language (SAML) V2.0. OASIS Security Services Technical Committee Standard, März 2005.

[S2BIND] Scott Cantor, Frederick Hirsch, John Kemp, Rob Philpott und Eve Maler (Hrsg.): *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Security Services Technical Committee Standard, März 2005.

[S2CONF] Prateek Mishra, Rob Philpott und Eve Maler (Hrsg.): *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Security Services Technical Committee Standard, März 2005.

[S2CORE] Scott Cantor, John Kemp, Rob Philpott und Eve Maler (Hrsg.): *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Security Services Technical Committee Standard, März 2005.

[S2META] Scott Cantor, Jahan Moreh, Rob Philpott und Eve Maler (Hrsg.): *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Security Services Technical Committee Standard, März 2005.

[S2OVER] John Hughes und Eve Maler (Hrsg.): *OASIS Security Assertion Markup Language (SAML) V2.0 Technical Overview*. OASIS Security Services Technical Committee Working Draft 7, Juli 2005.

[S2PRIV] Frederick Hirsch, Rob Philpott und Eve Maler (Hrsg.): *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Security Services Technical Committee Standard, März 2005.

[S2TRST] John Linn (Hrsg.): *OASIS Security Assertion Markup Language (SAML) V2.0 Trust Model Guidelines*. OASIS Security Services Technical Committee document, 2005.

[SBP05] Simon S. Y. Shim, Geetanjali Bhalla und Vishnu Pendyala: *Federated Identity Management*. In: *IEEE Computer Vol. 38, Issue 12*. IEEE Press, Dezember 2005.

[SCFDBM] J. Leon Zhao: *Schema coordination in federated database systems*. In: *Proceedings of the 4th Annual Workshop on Information Technologies and Systems (WITS94)*, 1994.

[SCHAC] Javi Masa and others: *TERENA SCHAC: SChema Harmonisation Committee*. `http://www.terena.org/activities/tf-emc2/schac.html`, 2006.

[SDSI] Ron Rivest und Butler Lampson: *SDSI — A Simple Distributed Security Infrastructure*. Presented at CRYPTO'96 Rumpsession, 1996.

[SECUPS] Katrin Borcea-Pfitzmann, Elke Franz und Andreas Pfitzmann: *Usable Presentation of Secure Pseudonyms*. In: *Proceedings of Workshop on Digital Identity Management 2005*. ACM Press, November 2006.

[SHARPS] Scott Cantor: *Shibboleth v1.2 Attribute Release Policies.* `http://shibboleth.internet2.edu/guides/deploy-guide-origin1.2.html#2.e.`, 2004.

[SHIBTR] David Chadwick, Sassa Otenko und Wensheng Xu: *Adding Distributed Trust Management to Shibboleth.* In: *Proceedings of the 4th annual PKI R&D Workshop*, Gaithersburg MD, April 2005. NIST.

[SNL05] Christopher Steel, Ramesh Nagappan und Ray Lai: *Core Security Patterns.* Prentice Hall, ISBN 978-0131463073, 2005.

[SOAPFW] Nils Gruschka und Norbert Luttenberger: *Protecting Web Services from DoS Attacks by SOAP Message Validation.* In: *Proceedings of 21st International Information Security Conference (SEC 2006).* Springer Verlag, 2006.

[SPADE] Sidharth Nazareth und Sean Smith: *Using SPKI/SDSI for Distributed Maintenance of Attribute Release Policies in Shibboleth.* Technischer Bericht TR2004-485, Department of Computer Science, Dartmouth College, Hanover, HN 03744 USA, 2004.

[SPARSE] Reginald Tewarson: *Sparse Matrices.* Academic Press Inc., 1973.

[SPKI] Carl Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian Thomas und Tatu Ylonen: *SPKI Certificate Theory.* IETF Proposed Standard, RFC 2693, 1999.

[SPML20] Gary Cole (Hrsg.): *Service Provisioning Markup Language (SPML) Version 2.0.* OASIS Committee Specification, 2006.

[SRS+05] Ludwig Seitz, Erik Rissanen, Thomas Sandholm, Babak Sadighi Firozabadi und Olle Mulmo: *Policy Administration Control and Delegation using XACML and Delegent.* In: *Proceedings of IEEE Grid Computing Workshop 2005.* IEEE Press, 2005.

[SS05] Ingo Schmitt und Gunter Saake: *A comprehensive database schema integration method based on the theory of formal concepts.* In: *Acta Informatica, Volume 41, Numbers 7–8*, Seiten 475–524, Heidelberg, 2005. Springer Verlag.

[SSB05] Abhilasha Spantzel, Anna Squicciarini und Elisa Bertino: *Integrating Federated Digital Identity Management and Trust Negotiation.* Technischer Bericht 46, Purdue University, 2005.

[SSOTAX] Andreas Pashalidis und Chris Mitchell: *A Taxonomy of Single Sign-On Systems.* In: *LNCS Vol. 2727.* Springer, 2003.

[STICKY] Marco Mont, Siani Pearson und Pete Bramhall: *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services.* Technischer Bericht HPL-2003-49, HP Laboratories Bristol, 2003.

[SUNXAC] Seth Proctor: *Sun's XACML implementation.* `http://sunxacml.sf.net/`, 2004.

[SXIP20] Sxip Identity Corporation: *SXIP 2.0 Protocol Specification.* Technischer Bericht, SXIP Networks, 2006.

[SXIPIN] Sxip Identity Corporation: *How SXIP 2.0 works.* Technischer Bericht, SXIP Networks, 2006.

[SXIPOV] Sxip Identity Corporation: *SXIP 2.0 Overview.* Technischer Bericht, SXIP Networks, 2006.

[TEQILA] Claude Lecommandeur: *Tequila – A distributed Web authentication and access control tool.* In: *Proceedings of EUNIS 2005*, 2005.

[TERMPR] Andreas Pfitzmann und Marit Köhntopp: *Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology.* In: *LNCS Vol. 2009*, Seiten 1–9. Springer, 2000.

[TK06] Michael Carl Tschantz und Shriram Krishnamurthi: *Towards Reasonability Properties for Access-Control Policy Languages.* In: *Proceedings of SACMAT 2006.* ACM Press, Juni 2006.

[TM03] Kerry Taylor und James Murty: *Implementing Role Based Access Control for Federated information Systems on the Web.* In: *Proceedings of the Australasian Information Security Workshop 2003 (AISW2003).* Australian Computer Socienty, Inc., 2003.

[WALDEN] Beth Kirschner, Thomas Hacker, William Adamson und Brian Athey: *Walden: A Scalable Solution for Grid Account Management.* In: *Proceedings of 5th IEEE/ACM Workshop on Grid Computing*, November 2004.

[WBS+05] Benjamin Weyl, Pedro Brandao, Antonio Skarmeta, Rafael Lopez, Parijat Mishra, Christian Hauser und Holger Ziemek: *Protecting Privacy of Identities in Federated Operator Environments.* In: *Proceedings of 14th IST Mobile & Wireless Communications Summit*, Februar 2005.

[WEK05] Martin Wimmer, Pia Ehrnlechner und Alfons Kemper: *Flexible Autorisierung in Web Service-Föderationen.* In: *Proceedings der 11. GI-Fachtagung für Datenbanken in Business, Technologie und Web (BTW2005)*, LNI. Springer, März 2005.

[WP05] Jake Wu und Panos Periorellis: *Authorization-Authentication Using XACML and SAML.* Technischer Bericht CS-TR-907, School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Road, NE1 7RU, UK, Mai 2005.

[WS-FAR] Chris Kaler und Anthony Nadalin (Hrsg.): *WS-Federation: Active Requestor Profile.* Web Services Specification Document, BEA, IBM, Microsoft, RSA Security, Verisign, Juli 2003.

[WS-Fed] Chris Kaler und Anthony Nadalin (Hrsg.): *Web Services Federation Language (WS-Federation).* Web Services Specification Document, BEA, IBM, Microsoft, Verisign, RSA Security, 2003.

[WS-FPR] Chris Kaler und Anthony Nadalin (Hrsg.): *WS-Federation: Passive Requestor Profile.* Web Services Specification Document, BEA, IBM, Microsoft, RSA Security, Verisign, Juli 2003.

[WS-Ker] Giovanni Della-Libera, Brendan Dixon, Praerit Garg, Maryann Hondo, Chris Kaler, Hiroshi Maruyama, Anthony Nadalin und Nataraj Nagaratnam: *Web Services Security Kerberos Binding.* Web Services Specification Document, IBM, Microsoft, Dezember 2003.

[WS-MDX] Francisco Curbera und Jeffrey Schlimmer (Hrsg.): *Web Services Metadata Exchange (WS-MetadataExchange).* Web Services Specification Document, BEA, IBM, Microsoft, SAP, Februar 2004.

[WS-PAs] Anthony Nadalin (Hrsg.): *Web Services Policy Assertions Language (WS-PolicyAssertions).* Web Services Specification Document, BEA, IBM, Microsoft, SAP, Juni 2003.

[WS-PoA] Chris Kaler und Maryann Hondo (Hrsg.): *Web Services Policy Attachment (WS-PolicyAttachment).* Web Services Specification Document, BEA, IBM, Microsoft, SAP, Juni 2003.

[WS-Pol] Maryann Hondo und Chris Kaler (Hrsg.): *Web Services Policy Framework (WS-Policy).* Web Services Specification Document, BEA, IBM, Microsoft, SAP, Juni 2003.

[WS-Pro] Gearard Woods und Tony Gullotta: *Web Services Provisioning (WS-Provisioning).* Web Services Specification Document, IBM, Oktober 2003.

[WS-Sec] Chris Kaler (Hrsg.): *Web Services Security (WS-Security).* Web Services Specification Document, IBM, Microsoft, VeriSign, April 2002.

[WS-Tru] Chris Kaler und Antohony Nadalin (Hrsg.): *Web Services Trust Language (WS-Trust).* Web Services Specification Document, IBM, Microsoft, RSA Security, VeriSign, Dezember 2002.

[WSPL] Tim Moses, Anne H. Anderson, Seth Proctor und Simon Godik: *XACML Profile for Web Services (aka Web Services Policy Language).* OASIS TC Working Draft, September 29th, 2003.

[X2PRIV] Tim Moses: *Privacy Policy Profile of XACML 2.0.* OASIS TC Committee draft, 16. September 2004, 2004.

[XACML] Tim Moses (Hrsg.): *OASIS eXtensible Access Control Markup Language 2.0, core specification.* OASIS XACML Technical Committee Standard, 2005.

[XACMLD] Markus Lorch, Seth Proctor, Rebekah Lepro, Dennis Kafura und Sumit Shah: *First Experiences Using XACML for Access Control in Distributed Systems.* In: *Proceedings of the ACM Workshop on XML Security.* ACM Press, 2003.

[XALAN] Apache Software Foundation: *Xalan XSLT Processor.* `http://xml.apache.org/xalan-j/`, 2005.

[XCO05] Wensheng Xu, David Chadwick und Sassa Otenko: *Development of a Flexible PERMIS Authorisation Module for Shibboleth and Apache Server.* In: *Proceedings of 2nd European PKI Workshop*, Nummer 3545 in *LNCS*. Springer Verlag, 2005.

[XDAC] Paul Mazzuca: *Access Control in a Distributed Decentralized Network: An XML Approach to Network Security.* Honors Thesis, Dartmouth College, 2004.

[XDI] Andy Dale, Steven Churchill, Barry Beechinor und Justine Hirsch: *OASIS XRI Data Interchange (XDI).* Technischer Bericht, OASIS Technical Committee, 2006.

[XPOLA] Liang Fang, Dennis Gannon und Frank Siebenlist: *XPOLA – An Extensible Capability-based Authorization Infrastructure for Grids.* In: *Proceedings of the Internet2 PKI R&D Workshop 2005*, 2005.

[XPREF] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant und Yirong Xu: *An XPath-based Preference Language for P3P.* In: *Proceedings of WWW 2003.* ACM Press, Mai 2003.

[XSLT] James Clark: *XSL Transformations (XSLT), Version 1.0.* W3C Recommendation, `http://www.w3.org/TR/xslt/`, 1999.

[YADIS] Joaquin Miller: *Yadis Specification 1.0.* http://www.yadis.org/, 2006.

[ZRF05] Thomas Zwahr, Pierre Rossel und Matthias Finger: *Towards Electronic Governance - Gaining evidence for a paradigm shift in Governance from Federated Identity Management.* In: *Proceedings of 5th European Conference on E-Government*, Juni 2005.

Index

A

Lebenslauf

Persönliche Angaben

Name:	Wolfgang Hommel
Geburtsdatum:	28.06.1978
Geburtsort:	Gräfelfing bei München
Staatsangehörigkeit:	Deutsch

Ausbildung

1984–1988	Grundschule Penzing
1988–1997	Rhabanus-Maurus-Gymnasium Sankt Ottilien (Abschluss: Allgemeine Hochschulreife, 06/1997)
11/1998–10/2003	Studium an der Technischen Universität München (Abschluss: Diplom-Informatiker)

Beruflicher Werdegang

07/1997–04/1998	Grundwehrdienst
05/1998–10/1998	Deutsches Zentrum für Luft- und Raumfahrt, Oberpfaffenhofen
seit 11/2003	Leibniz-Rechenzentrum (Wissenschaftlicher Mitarbeiter von Prof. Dr. Hegering)