DISSERTATION AN DER

FAKULTÄT FÜR MATHEMATIK,
INFORMATIK UND STATISTIK

DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Konzepte zur Authentication Assurance und Multi-Faktor-Authentifizierung im föderierten Identitätsmanagement

eingereicht von

Jule Anna Ziegler

am 22. Februar 2022

1. Gutachter: **Prof. Dr. Helmut Reiser,** Ludwig–Maximilians–Universität München
2. Gutachter: **Prof. Dr. Wolfgang Hommel,** Universität der Bundeswehr München

Tag der mündlichen Prüfung: 4. April 2022

Eidesstattliche Versicherung
(Siehe Promotionsordnung vom 12.07.11, §8, Abs. 2 Pkt. 5)

Hiermit erkläre ich an Eides statt, dass die Dissertation von mir selbstständig, ohne unerlaubte Beihilfe angefertigt ist.

München, den 22. Februar 2022 Jule Anna Ziegler

.....
Jule Anna Ziegler

Danksagung

Die vorliegende Dissertation entstand im Rahmen meiner wissenschaftlichen Tätigkeit am Leibniz-Rechenzentrum (LRZ). Zur selben Zeit war ich ebenfalls Mitglied im europäischen Forschungsprojekt GÉANT sowie im Munich Network Management Team (MNM).

Da eine Dissertation nur selten die isolierte Anstrengung eines einzelnen ist, sondern vielmehr von Unterstützung und Föderung mehrerer Personen auf unterschiedliche Art und Weise geprägt ist, möchte ich an dieser Stelle meine Dankbarkeit zum Ausdruck bringen.

Ein ganz besonderer Dank gilt meinem Doktorvater Prof. Dr. Helmut Reiser, der diese Arbeit stets unterstützt hat und mir durch seine Expertise und sein Engagement verholfen hat meine Ergebnisse kritisch zu hinterfragen, um diese Arbeit zu verbessern.

Mein Dank gilt außerdem Prof Dr. Wolfgang Hommel, der die Rolle des Zweitgutachters übernommen hat und sich bereit erklärt hat diese Arbeit zu lesen.

Ferner möchte ich auch die beiden Kollegen Dr. David Schmitz und Tobias Appel namentlich nennen und ihnen danken. Dr. David Schmitz danke ich für die wertvollen Diskussionen, seinem Rat in technischen Angelegenheiten sowie für die gemeinsam geschriebenen Paper. Es hat Spaß gemacht! Tobias Appel danke ich für die gegenseitige Motivation und Inspiration.

Außerdem danke ich allen weiteren LRZ- und MNM- Kolleg:innen, die bei Diskussionen oder auf andere Art und Weise involviert waren.

Da meine Idee zu diesem Dissertationsthema aus dem GÉANT-Projekt hervorgegangen ist, gilt ein ebenso großes Dankeschön meinen GÉANT-Projektkolleg:innen. Ich bekam die Chance, die REFEDS Assurance Working Group zu leiten und konnte so maßgeblich zum Thema Assurance beitragen.

Zu guter Letzt danke ich von Herzen meiner Familie und meinem Freund Robert sowie allen Freunden. Ihr habt mir stets Rückhalt gegeben und ein offenes Ohr für meine Anliegen gehabt! Robert, du hast mich tagtäglich beim Disserations-Marathon unterstützt, alle Höhen und Tiefen mit mir durchlaufen und mich auch noch auf der Zielgeraden motiviert. Mein Dank dafür ist nicht in Worte zu fassen.

Zusammenfassung

Föderiertes Identitätsmanagement (FIM) ermöglicht anhand einer delegierten Benutzerverwaltung die Entkopplung zwischen zu nutzendem Dienst und dem Management von Identitäten. Die Vorteile, die aus Benutzerperspektive entstehen, sind neben einer verbesserten Benutzerfreundlichkeit - aufgrund der Tatsache, dass ein Benutzer nur noch eine digitale Identität zum Zugriff auf zahlreiche Dienste benötigt - zusätzlich die Möglichkeit einer Einmalanmeldung (*engl. Single Sign On*), sodass sich ein Benutzer bei den jeweiligen Diensten nicht zusätzlich erneut anmelden muss. Derartige Konstrukte kennen wir bereits von den großen Technologie-Unternehmen, subsumiert unter dem Begriff GAFAM,[1] und werden auch in Zukunft aufgrund der zunehmenden Digitalisierung eine immer größere Rolle spielen. Die in diesem Kontext als *Service Provider (SP)* bezeichneten Dienstanbieter müssen demnach keine eigene Benutzerverwaltung mehr implementieren, sondern kontaktieren den sogenannten *Identity Provider (IDP)* eines Benutzers. Auch in der Forschung und Lehre haben sich hochverteilte Föderationen zwischen IDPs und SPs (z.B. Universitäten, Forschungsinstitute) sowie Benutzern etabliert und verknüpfen diese weltweit. Ein wichtiger Aspekt stellt in diesem Zusammenhang das Vertrauen (*engl. Trust Management*) dar, da ein Service Provider nur Zugriff auf seinen Dienst bzw. seine Ressourcen gewähren wird, wenn sich dieser sicher sein kann, dass ein Benutzer mit einer bestimmten Qualität identifiziert und authentifiziert wurde. Der Schwerpunkt dieser Arbeit ist die Authentifizierung, d.h. die Überprüfung der Echtheit einer Entität bzw. Subjekts, weswegen im Rahmen dieser Arbeit Konzepte zur *Authentication Assurance* und *Multi-Faktor-Authentifizierung (MFA)* in FIM entwickelt werden. Die Authentication Assurance beschreibt dabei die Verlässlichkeit bzw. den Grad des Vertrauens durchgeführter Authentifizierungen, während mit Hilfe einer Multi-Faktor-Authentifizierung vorhandene Authentifizierungsmechanismen gegen unrechtmäßige Nutzung stärker geschützt werden können. Die beiden Konzepte stehen somit in engem Zusammenhang. Im Rahmen dieser Arbeit wird eine Architektur erarbeitet, die neben einem übergreifenden Authentication-Assurance-Konzept zum Informations- und Wissensaustausch ebenfalls einen MFA-Workflow spezifiziert, um Identity Provider, die keine eigene MFA-Lösung betreiben können, zu unterstützen. Durch die Spezifikation unterstützender Konzepte ist die Arbeit ebenfalls von hoher Praxisrelevanz, da Anleitungen und Hilfestellungen in diesem Zusammenhang bereitgestellt werden. Zu Beginn der Arbeit werden zunächst repräsentative Szenarien betrachtet und auf Basis einer umfassenden Analyse Anforderungen abgeleitet, klassifiziert und gewichtet. Darauf aufbauend werden mittels einer Architektur erforderliche Komponenten und Konzepte eingeordnet und aufgezeigt, wie diese aufeinander abgestimmt verwendet werden können. Nach einer Evaluation und prototypischen Implementierung ausgewählter Konzepte schließt die Arbeit mit einer methodischen Anwendung innerhalb eines realen Authentifizierungsszenarios ab.

[1] Google (Alphabet), Amazon, Facebook, Apple und Microsoft

Abstract

Federated Identity Management (FIM) decouples the management of identities and the access to services by means of a delegated identity management. The benefits that arise from a user perspective are reflected in an improved ease-of-use given that there is only one digital identity needed to access several services but also the ability to log on once (i.e. Single Sign On) to prevent users having to authenticate to each and every service individually. The big five technology players which are subsumed under GAFAM[2] have already set an example for us and the usage of such technologies will also play an increasingly important role in the future. Hence, in lieu of *Service Providers (SPs)* implementing their own identity management they approach the so called *Identity Provider (IDP)* of the user. In a similar way, highly distributed federations comprising IDPs and SPs (e.g. universities, research institutes) and users have been established in research and education which operate on a global scale. In this context, *Trust* and *Trust Management* are important aspects as Service Providers will only let users access their services or resources if the user's identity and authentication has sufficiently been proofed or performed, respectively. The main focus in this thesis lies in authentications, i.e. the verification of the authenticity of an entity or subject, and thus leads to the specification of concepts dealing with authentication assurance and multi factor authentications in FIM. *Authentication assurance* represents the quality, or more precisely, the degree of confidence of authentications performed, while *multi factor authentication* (MFA), in turn, enables the strengthening of existing authentication mechanisms by introducing multiple authentication factors. Thus, both concepts are closely linked. In this thesis, a holistic architecture is developed which comprises an authentication assurance concept for the purpose of information and knowledge exchange as well as an MFA workflow to support IDPs which cannot operate their own MFA solution. Additionally, by specifying auxiliary concepts this thesis also contributes to a high level of practical relevance. After investigating representative FIM scenarios, a comprehensive requirements analysis is carried out which results in classified and weighted requirements aggregated in a requirements catalogue. Based on that, modular concepts are specified as part of an architecture and demonstrated how they can be used in a coordinated manner. The thesis continues with an evaluation and prototypical implementation of selected concepts and concludes with a transfer of concepts to a real-world authentication scenario.

[2]Google (Alphabet), Amazon, Facebook, Apple and Microsoft

Inhaltsverzeichnis

Kapitel 1

Einleitung

Inhalt dieses Kapitels

„*Authenticate locally, authorize globally.*“

Ken Klingenstein (o.J.)[1]

Identitäten stellen nicht nur in der Informationstechnologie (IT), sondern auch unter anderem im juristischen und psychologischen Kontext ein grundlegendes Konzept bei der Interaktion mit der Umgebung dar. Im Bereich der IT spielen Identitäten vor allem dann eine Rolle, sobald es um die Verifikation der Echtheit einer Identität (**Authentifizierung**) und um die Zugriffsentscheidung basierend auf der Vergabe von Rechten (**Autorisierung**) einer Identität auf einen Dienst oder eine Ressource geht. Einhergehend mit der Digitalisierung und der ständig wachsenden Vernetzung entstehen somit auch neue Anforderungen an das Management von Identitäten, deren Authentifizierung und Autorisierung.

Während eine Person mittels Personalausweis oder Reisepass und den darauf enthaltenen Identitätsattributen wie Name, Geburtsdatum, Größe oder Fingerabdruck eindeutig identifiziert werden kann, sind aus der digitalen Perspektive identifizierende Attribute [Win05] wie eine E-Mail-Adresse oder die Zugehörigkeit (*engl. Affiliation*) zu einer Institution geläufiger. Jedoch existiert im Internet, oder der IT generell, keine einzigartige global gültige digitale Identität pro Person, sodass eine Person in der Regel mehrere verschiedene digitale Identitäten zum Zugriff auf diverse Dienste besitzt. Auch im beruflichen Werdegang erhält eine Person meist eine auf organisationsinterne Dienste maßgeschneiderte digitale Identität.

Als momentaner De-facto-Standard in Organisationen werden zur Verwaltung digitaler Identitäten und deren Zugriffsberechtigungen sogenannte **Identity & Access Management**

[1] http://www.bx.psu.edu/~schwartz/quotes.html

Systeme (IAM-Systeme) herangezogen. IAM-Systeme ermöglichen, dass Identitäten und deren Zugriffsberechtigungen an zentraler Stelle verwaltet werden, sodass mittels einer (einzigen) Benutzerkennung auf dedizierte Dienste oder Ressourcen innerhalb einer Domäne zugegriffen werden kann. Durch die Entkopplung der Benutzerverwaltung von den eigentlichen Diensten muss somit nicht jeder organisationsinterne Dienst eine eigene Benutzerverwaltung implementieren. Das führt zum einen zu einer konsistenten Benutzerverwaltung, zum anderen muss sich der Anwender nicht mehrere Benutzerkennungen merken. In Bezug auf die technische Realisierung greifen IAM-Systeme üblicherweise auf einen Verzeichnisdienst, z.B. Lightweight Directory Access Protocol, LDAP-basiert, zurück und stellen Schnittstellen zur Verfügung mittels derer Dienste Anfragen an die Benutzerdatenbasis stellen können.

Traditionelle IAM-Systeme stoßen jedoch an ihre Grenzen, sobald eine Person aus Organisation A, z.B. aufgrund eines gemeinsamen Projektes, auf Dienste von Organisation B zugreifen soll. Da die Organisation B in der Regel ein eigenes IAM betreibt, kann die digitale Identität der Person aus Heimatorganisation A nicht herangezogen werden, sodass stattdessen Ad-hoc-Lösungen wie die Erstellung eines lokalen Benutzerkontos bei Organisation B und ggf. vice versa erforderlich sind. Während dies bei bilateraler Kommunikation Abhilfe schafft, skaliert diese statische, manuelle Herangehensweise bei Projekten mit mehreren Teilnehmern jedoch nicht mehr, was folglich in einem zusätzlichen Pflegeaufwand sowie dem Merken mehrerer Zugangsdaten seitens der Benutzer resultiert. [Pöh16]

Folglich ist im IT-Sektor eine ausschließlich isolierte, domäneninterne Betrachtung digitaler Identitäten langfristig nicht anwendbar. Ein Lösungsansatz stellt das **Föderierte Identitätsmanagement** dar; im Folgenden durch **FIM** abgekürzt. FIM basiert auf dem Konzept einer delegierten Benutzerverwaltung, sodass Nutzer auch auf Dienste außerhalb der eigenen Organisation zugreifen können. FIM setzt dazu auf dem bereits existierenden IAM der jeweiligen Organisation auf. Dabei kommen Standards bzw. Protokolle wie die **Security Assertion Markup Language (SAML)** oder **OpenID Connect (OIDC)** zum Einsatz. Deren Grundprinzipien sehen vor, dass ein Nutzer mindestens einer Heimatorganisation (**Identity Provider**, kurz: **IDP**) zugeordnet ist, die dessen Benutzerverwaltung einschließlich Authentifizierung übernimmt. Die Autorisierung ist davon entkoppelt und wird von dem jeweiligen (externen) Dienstbetreiber bzw. **Service Provider (SP)** durchgeführt.

In Abbildung 1.1 sind die drei zentralen FIM-Rollen und deren Abhängigkeiten grafisch verdeutlicht. Durch das Bilden einer **Föderation**, an der sowohl Benutzer, Identity Provider als auch Service Provider teilnehmen, wird eine gegenseitige Dienstnutzung ermöglicht.

Im Bereich der Forschung und Lehre (*engl.* ***Research & Education***, kurz: **R&E**) haben sich bereits ebenjene (Identitäts-) Föderationen auf nationaler Ebene etabliert. Sie umfassen in der Regel die jeweiligen teilnehmenden wissenschaftlichen Einrichtungen (z.B. Universitäten, Rechenzentren, Forschungsinstitute) eines Landes und werden äquivalent auch als **Authentifizierungs- und Autorisierungs-Infrastrukturen (AAI)** bezeichnet. In Deutschland ist das beispielsweise die Authentifikations- und Autorisierungs-Infrastruktur des Deutschen Forschungsnetzes (DFN-AAI) [DFN10a]. Innerhalb der DFN-AAI können dann Forscher und Studenten aus Deutschland mit der Nutzerkennung ihrer Heimatorganisation (z.B. Universitätskennung) auf föderierte Dienste anderer deutscher wissenschaftlicher Einrichtungen zugreifen.

Durch das Entstehen von länderübergreifenden Forschungsprojekten, wie sie zum Beispiel durch die Europäische Union[2] gefördert werden, stößt auch FIM bei globaler Interaktion an dessen Grenzen. Gemäß [Hom07] wäre es utopisch ein föderationsübergreifendes Datenmodell aufzuspannen, insbesondere auch unter dem Gesichtspunkt, dass bereits zahlreiche nationale Identitätsföderationen, die auf unterschiedlichen Anforderungen basieren, existieren. Zu diesem Zweck wurde im Rahmen des europäischen Forschungsprojekts GÉANT der Dienst *eduGAIN* [GÉ18] entwickelt, der teilnehmende nationale Identitätsföderationen weltweit vernetzt und dazu auf das Konzept des **Interföderierten Identitätsmanagements (Inter-FIM)** zurückgreift.

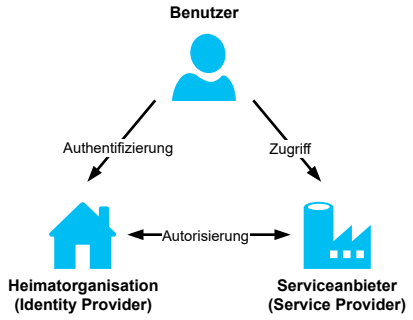


Abbildung 1.1: Dreiecksbeziehung in Föderationen

Inter-FIM basiert, wie der Name bereits indiziert, auf dem Konzept einer Interföderation, oder *engl. umbrella federation*. Eine **Inter-Föderation** ist eine Föderation, deren Teilnehmer wiederum selbst Föderationen sind, d.h. eine Föderation von Föderationen. Sowohl FIM als auch dessen Spezialisierung Inter-FIM sind in dieser Dissertation von Relevanz und werden in Kapitel 2 anhand repräsentativer Szenarien detailliert beleuchtet.

Somit kann beispielsweise in R&E unter Verwendung der Heimatorganisationskennung weltweit auf wissenschaftliche Dienste zugegriffen werden. Dies hat den Vorteil, dass die Anzahl der Benutzerkennungen, die sich ein Nutzer merken muss, reduziert wird und gleichzeitig durch den erweiterten Anwendungsbereich und Technologien wie Single Sign On (SSO) eine verbesserte User Experience entsteht [Cha09].

Gegenüber den Chancen, die durch eine (inter-) föderierte Identität gegeben sind, stehen auch Risiken, die aus Perspektive der Informationssicherheit eine zentrale Rolle spielen. Wird eine derartige Identität kompromittiert, im Besonderen unter Betrachtung der Aspekte der *Vertraulichkeit* und *Integrität*, ist ein Angreifer in der Lage auf sämtliche Dienste und Ressourcen zuzugreifen. Dienstbetreiber werden dementsprechend ihre Dienste zur interorganisationalen Nutzung nur dann zur Verfügung stellen, wenn ein einheitliches und durchgehendes Trust- und Sicherheitsmanagement vorhanden ist [Rei08].

Während für Identity Provider in diesem Zusammenhang ein kritischer Aspekt der angemessene Umgang mit denen von ihnen bereitgestellten, personenbezogenen Benutzerdaten ist, stellt ein zentraler Aspekt zur Etablierung gegenseitigen Vertrauens seitens der Service Provider eine **verlässliche Authentifizierung** dar, da sich in FIM-Szenarien Service Provider auf die durch die Heimatorganisation eines Benutzers durchgeführten Authentifizierungen verlassen. Der Fokus dieser Dissertation sind Maßnahmen in Bezug auf die Authentifizierung, wobei zwei zentrale Aspekte zu berücksichtigen sind:

[2] https://ec.europa.eu/info/research-and-innovation_de

- Die Zusicherung und Kommunikation seitens der Identity Provider, dass ihre zugehörigen Benutzer qualitative Authentifizierungsfaktoren, wie zum Beispiel Passwörter, verwenden.

- Die Etablierung einer Authentifizierung basierend auf mehreren Faktoren beziehungsweise Nachweisen, die im Allgemeinen als Multi-Faktor-Authentifizierung bezeichnet wird, zum Zugriff auf besonders schützenswerte Dienste.

In Bezug auf den ersten Punkt existieren in R&E zwar bereits bei einer Vielzahl von Organisationen Richtlinien oder Verfahrensbeschreibungen zum Umgang mit beispielsweise Passwörtern, die die Verwendung von Initialpasswörtern oder leicht zu erratenden Passwörtern verbieten, jedoch ist dies aufgrund der Autonomie der teilnehmenden Organisationen weder übergreifend verpflichtend noch wird es einheitlich kommuniziert. Darüber hinaus sind vorhandene Ansätze und deren Anforderungen zum Austausch von Vertrauensinformation, wie zum Beispiel zur Authentifizierungsstärke bzw. -qualität, zwischen Entitäten, subsumiert unter dem Begriff **Level of (Authentication) Assurance (LoA)**, oftmals zu umfangreich und strikt und ermöglichen nur eine geringe Handlungsfreiheit hinsichtlich der Implementierung. Es wird folglich ein übergreifender, d.h. für alle Entitäten bzw. Teilnehmende anwendbarer, und zugleich leichtgewichtiger[3] Ansatz benötigt, sodass Dienstbetreiber Rückschlüsse über die Qualität einer stattgefundenen Authentifizierung ziehen können. Dies schließt sowohl Authentifizierungen mit einem Faktor, d.h. **Ein-Faktor-Authentifizierungen (1FA)**, als auch **Multi-Faktor-Authentifizierungen (MFA)** mit ein. Die Definition von Kriterien zur Ein-Faktor-Authentifizierung ist in FIM vor allem unter der Tatsache relevant, da die einzelnen Faktoren einer Multi-Faktor-Authentifizierung gegebenenfalls von verschiedenen, vertrauenswürdigen Entitäten verifiziert und dann zusammengeführt werden, d.h. MFA resultiert aus einer Summe mehrerer 1FAs.

Den ersten Punkt zusammenfassend ist folglich ein einheitliches und sicherheitsbezogenes Grundverständnis für die Teilnehmende einer (Inter-) Föderation bezüglich Authentifizierungen notwendig. Dabei gilt es auch zu untersuchen, wie Service Provider hinsichtlich der Auswahl einer für ihren Dienst geeigneten Authentifizierungsstärke, im Sinne einer Ein-Faktor- oder Multi-Faktor-Authentifizierung, unterstützt werden können.

Um kritische Dienste vor unrechtmäßiger Nutzung durch Einführung einer **Multi-Faktor-Authentifizierung** stärker zu schützen (vgl. Punkt 2) müssen folglich die gemäß Punkt 1 zu spezifizierenden Kriterien für 1FA und MFA entsprechend kommuniziert und zusätzlich die vorhandene 1FA-Infrastruktur für MFA erweitert werden. Dabei stellt idealerweise jeder Identity Provider MFA für die ihm zugehörigen Nutzer zur Verfügung, was jedoch mit einem erheblichen Ressourcenaufwand seitens der Identity Provider verbunden ist. In R&E zeigt sich, dass eine Vielzahl von Identity Providern MFA für ihre Nutzer (noch) nicht zur Verfügung stellen oder eine MFA-Implementierung nicht für FIM Zwecke genutzt wird. Dies kann zu einem Ausschluss von Nutzern führen, deren Heimatorganisation über keine FIM-fähige MFA-Implementierung verfügt.

[3] *Leichtgewichtig* im Sinne der gestellten Anforderungen, unter anderem hinsichtlich der Quantität der Anforderungen.

Es ist daher zu untersuchen, wie Identity Provider durch Einführung eines, z.B. extern betriebenen, Dienstangebots für MFA unterstützt werden können. Dabei soll die durch die Heimatorganisation zur Verfügung gestellte Ein-Faktor-Authentifizierungsmethode, z.B. Benutzername-Passwort-Kombination, wiederverwendet werden. Damit möglichst viele Teilnehmende einer (Inter-) Föderation von einem derartigen Dienstangebot profitieren, ist daher ein **MFA-Workflow** zu erarbeiten, der Identity Provider, Service Provider sowie einen oder mehrere externe MFA-Provider verbindet, sodass kritische Dienste in (Inter-) FIM-Szenarien auch für Nutzer eines betroffenen Identity Providers ohne eigene MFA-Kapabilität zugreifbar bleiben.

Da die Etablierung der zwei aufgeführten Punkte eine Anpassung vorhandener und die Einführung neuer Komponenten und Konzepte erfordert, stellt dies eine große Herausforderung für die involvierten Entitäten dar. Aus diesem Grund wird daher als Teil der Dissertation ebenfalls ein **Beschreibungsmodell für Authentifizierungsszenarien** erarbeitet, das von Entitäten, wie beispielsweise Infrastrukturbetreibern, zur Abbildung einer existierenden Umgebung verwendet werden kann, um diese darauf aufbauend auf eine strukturierte Art und Weise zu erweitern.

Zusammenfassend sind **Konzepte zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM** notwendig, um diese Herausforderungen und Problemstellungen zu adressieren.

1.1 Zielsetzung und Fragestellung

Gemäß der zuvor erläuterten Problemstellung und zur Eingrenzung der Aufgabenstellung ergibt sich die folgende **Fragestellung**, die im Rahmen dieser Arbeit beantwortet wird:

Wie sieht eine Architektur für föderiertes Identitätsmanagement aus, die Komponenten und Konzepte zur Authentication Assurance und Multi-Faktor-Authentifizierung liefert?

Das **Ziel dieser Arbeit** ist somit der Entwurf modularer Konzepte zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM.

Modular bezeichnet in diesem Kontext die Konzeption klar voneinander abgegrenzter, durch Schnittstellen miteinander verbundener (Teil-) Lösungen[4] die in einer Architektur subsumiert sind und steht im Gegensatz zu einer monolithischen Konzeption. Die Konzeption einer Architektur orientiert sich dabei an den vier zentralen Teilmodellen von Managementarchitekturen [HAN99] und sorgt somit für eine Klassifikation und Eingliederung der in die Konzepte involvierten Komponenten.[5]

[4] Die Begriffe *(Teil-) Lösung* und *Konzept* werden an dieser Stelle synonym verwendet.

[5] Der Begriff *Komponente* wird in dieser Arbeit als Sammelbegriff verwendet und bezeichnet einen Bestandteil (zum Beispiel ein Informationsobjekt, eine Rolle, eine Funktion, eine Interaktion et cetera) einer übergeordneten Einheit; hier eines Konzepts.

Der Begriff beziehungsweise die Abkürzung *FIM* wird in dieser Arbeit als Oberbegriff verwendet und bezieht auch die in der Einleitung motivierte Spezialisierung Inter-FIM mit ein.

Die Herausforderung aus wissenschaftlicher Perspektive besteht darin, dass die zu entwickelnde Architektur bereits existierende FIM-Teillösungen berücksichtigt, um somit eine *Integrierbarkeit*, d.h. eine Eingliederung beziehungsweise Anwendung der neu entwickelten Konzepte gemäß der in Kapitel 2 skizzierten, föderierten Authentifizierungsszenarien, sicherzustellen. Darüber hinaus ist die Fragestellung auch von hoher Praxisrelevanz, da die Architektur Konzepte zur Umsetzungshilfe liefert, um Föderations- und Dienstbetreiber bei der Etablierung zu unterstützen.

Zur Erreichung dieses Ziels sind die folgenden Sub-Fragestellungen zu beantworten:

- Wie können Entitäten, Dienste sowie Abhängigkeiten innerhalb eines Authentifizierungsszenarios *universell*, d.h. unabhängig von zugrundeliegenden Protokollen, Standards, Technologien und Rahmenwerken sowie *ganzheitlich* und *service-orientiert*[6] beschrieben und abgebildet werden?
- Welchen Kriterien müssen Ein-Faktor- und Multi-Faktor-Authentifizierungen mindestens genügen und wie können diese in einem Authentication-Assurance-Konzept abgebildet werden? Was ist die minimale Qualität?
- Wie können Dienstbetreiber bei der Auswahl eines angemessenen Authentication-Assurance-Levels bzw. -Profils unterstützt werden?
- Wie kann ein existierender Ein-Faktor-Authentifizierungsworkflow um die Bereitstellung eines zweiten bzw. zusätzlichen Faktors erweitert werden?

Nicht im Fokus dieser Arbeit ist die Autorisierung und Zugriffskontrolle, die auf Basis unterschiedlicher Modelle erfolgen kann (z.B. Attribute-based Access Control, Role-based Access Control) [Ben06, FSG+01, HFCK17]. Ferner werden auch die Identity Assurance und die damit verbundenen Verfahren zur Feststellung der Identität nur oberflächlich betrachtet und erläutert, da dieser Bereich ein eigenes, umfassendes Forschungsthema darstellt.

Im nächsten Abschnitt wird die zur Lösung der Fragestellungen notwendige Vorgehensweise präsentiert.

1.2 Vorgehensmodell

Abbildung 1.2 zeigt die gewählte Vorgehensweise und den Aufbau der vorliegenden Arbeit im Detail. Innerhalb der Kapitelstruktur repräsentieren weiß eingefärbte Rechtecke die erarbeiteten wissenschaftlichen Beiträge und Ergebnisse. Die dazu relevanten Kapitel sind blau umrahmt dargestellt.

[6] *Service-Orientierung* bezeichnet in diesem Kontext den Bezug zum IT Service Management, das Prozesse zum Management von Services während des gesamten Lebenszyklus eines Services (i.S.v. *ganzheitlich*, d.h. vom Design bis hin zur Deprovisionierung) definiert.

Kapitel 1 – *Einleitung*

Dieses Kapitel hat die vorliegende Arbeit motiviert und die daraus resultierende, zentrale Fragestellung sowie die Zielsetzung hervorgehoben. Nach der hier vorliegenden Skizzierung der Vorgehensweise werden nachfolgend die vorab publizierten Teile der Arbeit aufgelistet sowie eine Abgrenzung zu verwandten Forschungsarbeiten gegeben.

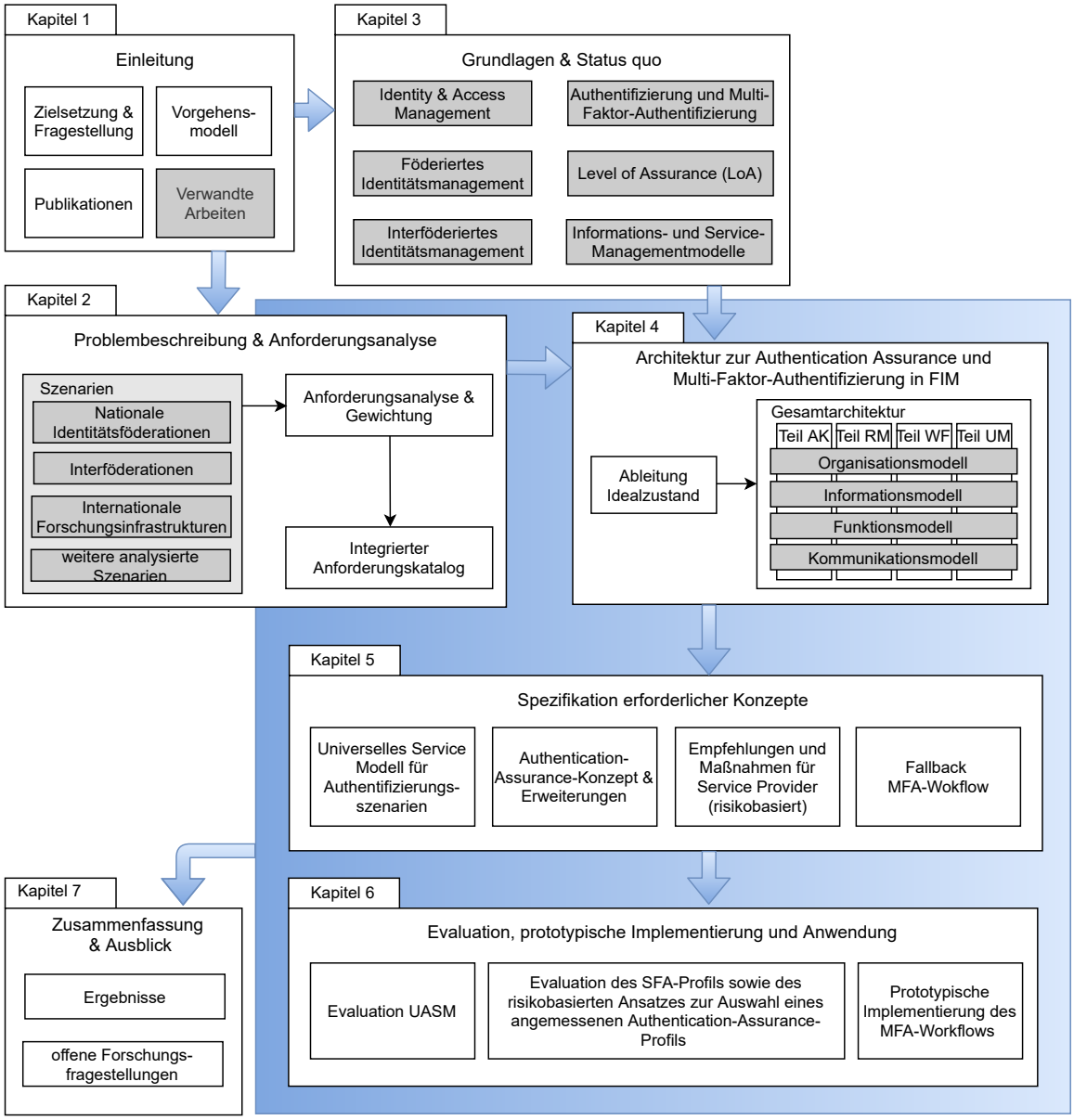


Abbildung 1.2: Vorgehensmodell der Arbeit

Kapitel 2 – *Problemstellung und Anforderungsanalyse*

In diesem Kapitel werden verschiedene Szenarien betrachtet, um den Anwendungsbereich detailliert zu beleuchten und Anforderungen abzuleiten. Anschließend werden die erarbeiteten Anforderungen einer Gewichtung unterzogen und in einem integrierten Anforderungskatalog übersichtlich zusammengefasst.

Kapitel 3 – *Grundlagen und Status quo*

In diesem Kapitel werden die Grundlagen und der Status quo des Identity&Access Managements sowie des föderierten und interföderierten Identitätsmanagements dargelegt. Darauf aufbauend werden Aspekte der Benutzerauthentifizierung erläutert sowie ein Einblick in das Konzept der Level of Assurance und der Informations- und Service-Managementmodelle gegeben. Zuletzt werden die Perspektiven und Dimensionen des Problemraums zusammengefasst und die Arbeit in den Forschungsstand eingegliedert.

Kapitel 4 – *Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM*

In diesem Kapitel wird eine Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM spezifiziert. Dazu werden die Teilmodelle für Managementarchitekturen [HAN99] herangezogen und auf Basis dessen vier aufeinander aufbauende Architekturteile systematisch erarbeitet.

Kapitel 5 – *Spezifikation erforderlicher Konzepte*

In diesem Kapitel werden die aus der Architektur resultierenden, erforderlichen Konzepte detailliert erarbeitet bzw. referenziert. Dies umfasst ein universelles Modell für Authentifizierungsszenarien, ein leichtgewichtiges Authentication-Assurance-Konzept sowie, aufbauend auf dem Authentication-Assurance-Konzept, Empfehlungen und Maßnahmen für Service Provider unter Verwendung eines risikobasieren Ansatzes. Zuletzt wird ein MFA-Workflow spezifiziert.

Kapitel 6 – *Evaluation, prototypische Implementierung und Anwendung*

In diesem Kapitel werden die Konzepte evaluiert oder prototypisch implementiert. Es wird unter anderem eine Testumgebung aufgebaut und aufgezeigt, wie die spezifizierten Komponenten und Konzepte eingesetzt und miteinander interagieren können. Anhand einer methodischen Anwendung wird aufgezeigt, wie der MFA-Workflow in realen Szenarien eingesetzt werden kann.

Kapitel 7 – *Zusammenfassung und Ausblick*

Im letzten Kapitel wird nochmals eine Zusammenfassung der Arbeit und der Ergebnisse bereitgestellt. Die Arbeit schließt mit einem Ausblick auf potentielle Folgearbeiten ab.

1.3 Publikationen

Im Rahmen der hier vorliegenden Arbeit wurden Teile der Arbeit bereits vorab in Form von wissenschaftlichen Veröffentlichungen publiziert. Der Abschnitt listet diese in chronologischer Reihenfolge auf und gibt eine kurze Zusammenfassung zu der jeweiligen Publikation.

- *Jule A. Ziegler und David Schmitz, Establishing a Universal Model for Authentication Scenarios based on MNM Service Model, In 11. DFN-Forum Kommunikationstechnologien, Seiten 81–91, Gesellschaft für Informatik e.V., 2018.*: In [ZS18] wird ein *Universal Authentication Service Model* (UASM) basierend auf dem MNM Service Modell dargestellt, mit dem Ziel Authentifizierungsszenarien in generischer, service-orientierter Art und Weise zu beschreiben. Die Idee zur Erweiterung des MNM Service Model zur Beschreibung und Modellierung von Authentifizierungsszenarien stammt von der Erstautorin. David Schmitz agierte an dieser Stelle als Sparringspartner, um die erarbeiteten Ergebnisse kritisch und lösungsorientiert zu diskutieren. Von ihm stammt u.a. der Vorschlag zur Einführung einer $\text{UASM}_{\text{service}}$ Basic View und $\text{UASM}_{\text{subject}}$ Basic View. Als Work in Progress werden in [ZS18] zunächst grundlegende Begriffe und Konzepte eingeführt, die in der vorliegenden Dissertation in Abschnitt 5.1 aufgegriffen werden. Darüber hinaus erweitert und detailliert der Abschnitt 5.1 das in [ZS18] eingeführte Universal Authentication Service Model, insbesondere durch Einführung der UASM Service View, der UASM Realization View sowie der UASM Templates.
- *Jule A. Ziegler, Michael Schmidt und Mikael Linden, Improving Identity and Authentication Assurance in Research & Education Federations, In Security and Trust Management, 15th International Workshop, STM 2019, Seiten 1–18, Springer, 2019.*: Kern von [ZSL19] ist ein leichtgewichtiges Assurance-Rahmenwerk, die REFEDS Assurance Suite. Es wird gezeigt, dass aufgrund umfassender und strikter Kriterien existierende Rahmenwerke in Forschung und Lehre nicht ohne Weiteres anwendbar sind und wie auf Basis einer Anforderungsanalyse ein leichtgewichtiger Ansatz abgeleitet wird. Ferner werden die Ergebnisse der durchgeführten Evaluation sowie die des technischen Piloten präsentiert. Augenmerk sind hier vor allem zwei der drei in der REFEDS Assurance Suite aggregierten Spezifikationen: das REFEDS Single Factor Authentication Profile[7] sowie das (Identity) Assurance Framework. Um eine internationale Anwendbarkeit zu erreichen, können derartige Spezifikationen nicht Isolation entstehen, sondern müssen die verschiedenen Sichten der (Identitätsföderations-) Teilnehmer einbeziehen, weswegen die beiden Spezifikationen im Rahmen der REFEDS Assurance Working Group, zu diesem Zeitpunkt unter Leitung von M. Linden, entstanden. Maßgeblich an der Entwicklung und Evaluation des Single Factor Authentication Profiles beteiligt waren die Autorin der vorliegenden Dissertation sowie M. Schmidt. In der vorliegenden Dissertation wird das Single Factor Authentication Profile sowie dessen Evaluationsergebnisse im Besonderen in den Abschnitten 5.2 und 6.2 aufgegriffen und zum Zwecke der Unterstützung eines Fallback MFA-Workflows erweitert.

[7] Das Single Factor Authentication Profile wurde ebenfalls in Form von nicht-wissenschaftlichen Publikationen, vgl. hierzu [Zie18] und [REF18c], über das Internet zur Verfügung gestellt. Diese werden neben der hier aufgelisteten Publikation [ZSL19] in der vorliegenden Dissertation gleichermaßen referenziert.

- *Jule A. Ziegler, Uros Stevanovic, David Groep, Ian Neilson, David P. Kelsey und Maarten Kremers, Making Identity Assurance and Authentication Strength Work for Federated Infrastructures, In International Symposium on Grids & Clouds 2021, Proceedings of Science, 2021.*:[8] In [ZSG+21a] wird die REFEDS Assurance Suite - die das REFEDS Assurance Framework (RAF), das Single Factor Authentication Profile (SFA) sowie das Multi Factor Authentication Profile (MFA) umfasst - aufgegriffen, und Umsetzungsempfehlungen bzw. -hilfestellungen unter Einbezug repräsentativer Use Cases erarbeitet, um Identity Provider und Service Provider hinsichtlich der Verwendung von Assurance-Komponenten zu unterstützen. Der Hauptteil der Publikation, d.h. das in den Sektionen 5 und 6 beschriebene Vorgehen, wurde nach Abstimmung des Autorenteams über mögliche Inhalte durch die Erstautorin im Detail ausgearbeitet und verfasst. Die Anwendungsbeispiele der Sektion 6, die das Vorgehen exemplarisch veranschaulichen, wurden hauptsächlich durch U. Stevanovic erläutert. Während Sektion 5 in der vorliegenden Dissertation in Abschnitt 5.3 nur kurz referenziert wird, stimmen hingegen die Inhalte der Sektion 6 mit dem Abschnitt 5.3 der Dissertation im Wesentlichen überein. In Ergänzung zu Sektion 6 in [ZSG+21a] visualisiert die vorliegende Dissertation das ganzheitliche risikobasierte Vorgehen grafisch und liefert darüber hinaus erste Ansätze zur Konzeption eines Risk Decision Paths.

1.4 Abgrenzung zu verwandten Forschungsarbeiten

In diesem Abschnitt wird kurz auf verwandte Forschungsarbeiten Bezug genommen und deren Abgrenzung zu dieser Arbeit hervorgehoben.

- Helmut Reiser beschreibt im Rahmen seiner Habilitation „*Ein Framework für föderiertes Sicherheitsmanagement*“ [Rei08] wie ein organisationsübergreifendes Sicherheitsmanagement innerhalb einer Föderation bzw. virtuellen Organisation (VO) etabliert werden kann. Es wird ein Kriterienkatalog zur Bewertung von Sicherheitsmechanismen entwickelt, der auf verschiedene Middleware-Technologien angewendet wird und dessen Defizit- und Schwachstellenanalyse verbesserungswürdige Sicherheitsdienstklassen identifiziert. Als Teil der Arbeit wird ein rekursiver Trust Algorithmus spezifiziert, der den Wert des Vertrauens gemäß einer Skala von 1 bis 4 quantifiziert und diesen an Teilnehmende einer Grid-Infrastruktur überträgt. Während in [Rei08] der Fokus auf der technischen Abbildbarkeit durch Verwendung von Trust-Graphen liegt, ist ein Teilziel der hier vorliegenden Arbeit, das Vertrauen durch Kommunikation von spezifizierten Authentifizierungsinformationen und -leveln zwischen Identity Providern und Service Providern in föderierten Szenarien zu stärken.
- In der Dissertation „*Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management*“ [Hom07] von Wolfgang Hommel wird ein ganzheitliches Architekturkonzept zur strukturierten Integration von FIM-Komponenten mit bereits vorhandenen I&AM-Systemen sowohl auf Seiten der Identity Provider als auch der Service Provider entwi-

[8] Ein Preprint [ZSG+21b] dieser Veröffentlichung ist unter dem folgenden Link verfügbar: `https://doi.org/10.5281/zenodo.4916049`

ckelt. Die Arbeit spezifiziert dazu notwendige technische Schnittstellen und betrachtet die ITIL-Prozesse Security Management und Change Management. Es werden neue FIM-Komponenten zur Verbesserung der Interoperabilität von teilnehmenden Organisationen einer Identitätsföderation erarbeitet; mit der Abgrenzung, dass in der hier vorliegenden Arbeit der Fokus auf der Interoperabilität im Sinne einer Multi-Faktor-Authentifizierung liegt.

- Daniela Pöhn beschreibt in ihrer Dissertation „*Architektur und Werkzeuge für dynamisches Identitätsmanagement in Föderationen*“ [Pöh16] eine Managementplattform für dynamisches FIM, deren Fokus auf einem orchestrierten, technischen Metadatenaustausch zwischen den involvierten Entitäten liegt. Analog zu [Hom07] werden die IT-Service-Prozesse Security Management und Change Management betrachtet sowie, darüber hinaus, Werkzeuge mit dem Ziel der Automatisierung und der Skalierbarkeit existierender FIM-Abläufe spezifiziert. Als Teilziel der Arbeit wird ein Mechanismus zum dynamischen Metadatenaustausch erarbeitet, wohingegen die hier vorliegende Arbeit den Austausch von Metadaten als Chance nutzt, ein Subset von Authentifizierungsinformationen vorab zwischen Teilnehmenden einer Identitätsföderation zu kommunizieren.
- Latifa Boursas stellt in ihrer Dissertation „*Trust-Based Access Control in Federated Environments*“ [Bou09] eine Zugriffslösung basierend auf Vertrauen (TBAC-Lösung) für föderierte Umgebungen vor. Es wird ein Vertrauensprozessmodell bestehend aus verschiedenen Phasen - beginnend bei der Initialisierung über das Management bis hin zur abschließenden Prüfung - entwickelt, das anschließend in einem TBAC-Rahmenwerk umgesetzt und prototypisch implementiert wird. Während in [Bou09] der Fokus auf einer vertrauensbasierten Access Control liegt, ist der Fokus der hier vorliegenden Arbeit die Authentifizierung, deren Qualität, basierend auf Assurance Leveln, ein wichtige Rolle bei der Zugriffsentscheidung spielen.
- In der Dissertation „*Organisational and Cross-Organisational Identity Management*“ [Lin09] analysiert Mikael Linden sowohl das Identity Management als auch FIM und berücksichtigt als Teil der Arbeit, wie eine aggregierte Sicht auf Benutzeridentitäten innerhalb einer Organisation erzielt werden kann. Darüber hinaus betrachtet er die Verbindung zwischen Identity Management sowie einer verlässlicheren Authentifizierungsmethode und schlägt vor, was bei einem Single Sign On (SSO) und Public Key Infrastructure (PKI) Deployment berücksichtigt werden muss. Die Arbeit kann daher als logische Ausgangsbasis für die hier vorliegende Arbeit angesehen werden.

Kapitel 2

Problemstellung und Anforderungsanalyse

Inhalt dieses Kapitels

Ziel dieses Kapitels ist die systematische Ableitung von Anforderungen auf Basis repräsentativer Szenarien. Als Motivation dieses Kapitels werden in Abschnitt 2.1 zunächst **Kollaborationen** und **Kooperationen** betrachtet und gezeigt, warum sich insbesondere internationale Kollaborationen in der Forschung und Lehre (R&E) etabliert haben. Dazu wird im Besonderen das europäische Forschungsprojekt GÉANT referenziert.

In Abschnitt 2.2 wird das erste Szenario betrachtet. Es werden **nationale Identitätsföderationen in R&E**, oftmals auch synonym als National Research and Education Networks

(NRENs) bezeichnet, vorgestellt sowie Problemstellungen und Defizite bezüglich der Authentication Assurance und Multi-Faktor-Authentifizierung aufgezeigt. Das erste Szenario wird im Fortlauf der Arbeit abkürzend als **nationales FIM** bezeichnet. Das zweite Szenario in Abschnitt 2.3 baut auf den Gegebenheiten des ersten Szenarios auf und zeigt, wie in diesem Rahmen eine internationale Kollaboration im Sinne einer **Interföderation** ermöglicht wird (vgl. Kapitel 1). Das dritte vorgestellte Szenario, siehe Abschnitt 2.4, beschäftigt sich mit **Forschungsinfrastrukturen** (engl. *research infrastructures*) und verdeutlicht, dass ähnliche Problemstellungen auch in Forschungsinfrastrukturen existieren. Darauf folgend werden in Abschnitt 2.5 verschiedene Szenarien aus dem kommerziellen Sektor betrachtet, die zeigen, dass ähnliche Herausforderungen auch außerhalb von R&E von Relevanz sind. Ferner werden Problemstellungen und Defizite aggregiert aufgelistet und darauf basierend Hauptanforderungen abgeleitet, die in den Abschnitten 2.6.2 bis 2.6.5 zu konkreten Anforderungen verfeinert werden. Ein entsprechendes Schema zur Gewichtung der Anforderungen wird in Abschnitt 2.7 eingeführt. In Abschnitt 2.8 werden alle identifizierten Anforderungen gemäß des Gewichtungsschemas in einem integrierten Anforderungskatalog übersichtlich und zusammenfassend dargestellt. Abschnitt 2.9 schließt mit einer Bewertung und einer Überleitung in das nächste Kapitel ab.

2.1 Interorganisationale Kollaborationen versus Kooperationen

Langanhaltende Entwicklungen wie insbesondere die Globalisierung und die damit verbundene Verflechtung in der Wirtschaft und vielen weiteren Bereichen hat dazu geführt, dass interorganisationale Kollaborationen und Kooperationen aus der heutigen Welt nicht mehr wegzudenken sind. Wesentliche Gründe für einen Zusammenschluss stellen dabei neben der Zielerreichung unter anderem die Gewinnmaximierung, die Optimierung von Prozessen sowie die Steigerung der Effizienz im Sinne einer ressourcenschonenden Produktion oder Bereitstellung von Dienstleistungen und Gütern dar. Dazu wird bspw. auf Bereitstellungsstrategien wie just-in-time oder just-in-sequence, d.h. einer bedarfsbasierten, zeitlich abgestimmten Bereitstellung von Materialien entlang einer Lieferkette zurückgegriffen, sodass benötigte Materialien zum richtigen Zeitpunkt (*engl. time*) als auch in der richtigen Reihenfolge (*engl. sequence*) der Lieferkette zur Verfügung stehen. Das Konzept stammt ursprünglich aus dem Bereich der Automobilindustrie und soll an dieser Stelle verdeutlichen, dass eine enge Zusammenarbeit und Abstimmung zwischen verschiedenen - sowohl internen als auch externen - organisatorischen Einheiten einen kritischen Erfolgsfaktor bei der Bereitstellung von Dienstleistungen darstellt. Dies verdeutlicht auch das Konzept des *Outsourcing*, wobei (Sub-) Dienstleistungen oder -Prozesse an externe Dienstleister ausgelagert werden.

Eine wichtige Unterscheidung stellt in diesem Zusammenhang die Differenzierung zwischen einer **Kooperation** und einer **Kollaboration** dar. In dem oben exemplarisch motivierten Automobilindustrie-Beispiel handelt es sich um ein **Kooperations**-Szenario, wobei verschiedene Dienstleister zusammenarbeiten, um jeweils *eigene Ziele* zu erreichen. Kooperationen dienen hier insbesondere dazu Arbeitsabläufe zu standardisieren und Verantwortlichkeiten klar zu trennen (*engl. separation of duties*). [AXE20]

Dem gegenüber stehen **Kollaborationen**. Hier ist der Zweck einer Zusammenarbeit die Erreichung *gemeinsamer Ziele*. Kollaborations-Modelle finden dabei nicht nur im kommerziellen Sektor Anwendung, sondern kommen auch in der Forschung und Lehre (R&E) zum Einsatz.

Charakteristisch unterscheiden sich R&E Kollaborationen im Vergleich zu denjenigen des kommerziellen Sektors in der Hinsicht, dass neben der Erreichung eines gemeinsamen Ziels nicht die Gewinnmaximierung maßgeblich ist, sondern die Tatsache, dass es sich größtenteils um Non-Profit Organisationen mit dem Fokus der Gemeinnützigkeit handelt. Ein Beispiel stellt hier das Grid-Computing dar, wobei durch verteilte Rechenleistung rechenintensive, wissenschaftliche Probleme gemeinschaftlich in einem Verbund gelöst werden [Rei08].

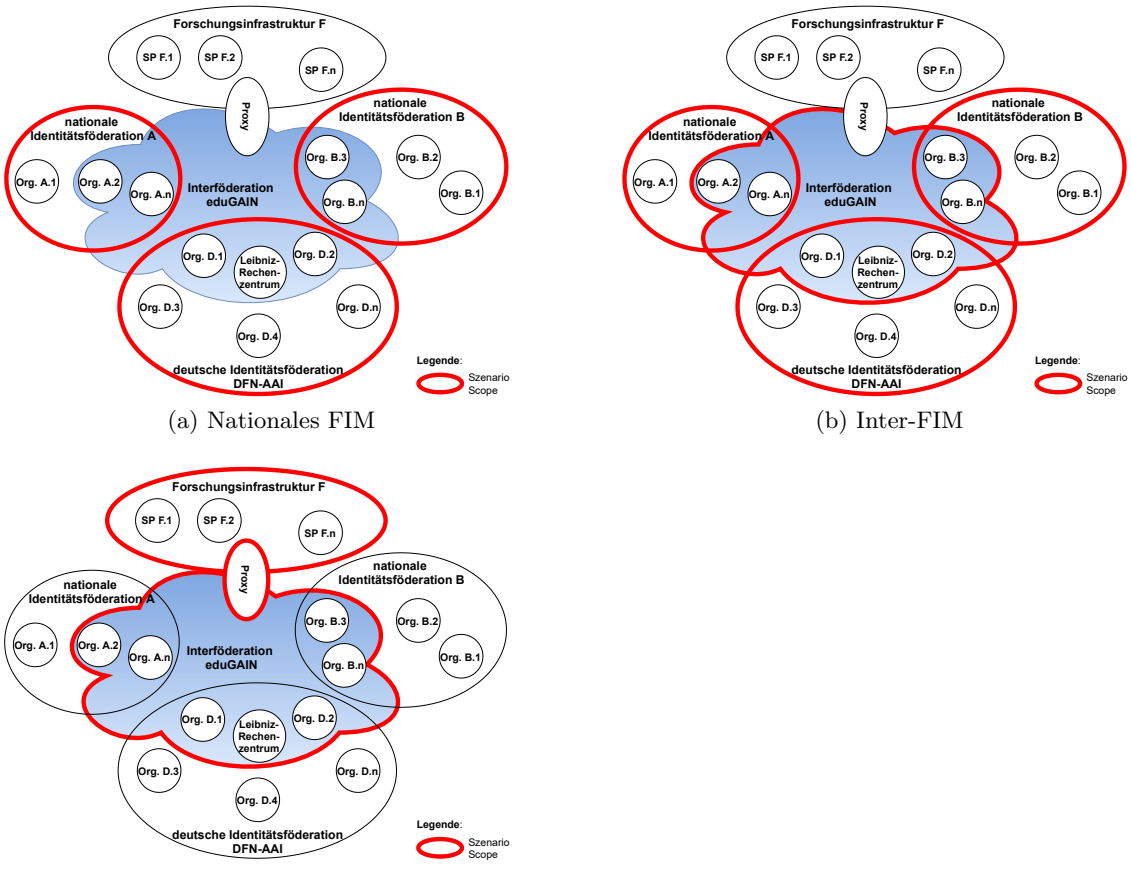
Interorganisationale Kollaborationen (hier i.S.v. Föderationen bzw. Inter-Föderationen) mit dem Anwendungsbereich in Forschung und Lehre stellen zugleich das Hauptaugenmerk der drei Szenarien dar. Da die drei Szenarien, die in den Abschnitten 2.2 bis 2.4 detailliert erläutert werden, auf realen Herausforderungen im Zusammenhang bzw. unmittelbarer Nähe zu dem Forschungsprojekt GÉANT stehen, wird anhand eines kleinen Exkurses das Forschungsprojekt GÉANT kurz vorgestellt.

Exkurs: Forschungsprojekt GÉANT

Das GÉANT Projekt, finanziert durch das European Union Horizon 2020 Programm, startete ursprünglich in seiner ersten Iteration unter dem Namen GN1 im Jahr 2000; seit Januar 2019 läuft die vierte Iteration GN4 in der dritten Phase (GN4-3). In GN4-3 sind inzwischen mehr als 30 Projektpartner mit über 500 Teilnehmern involviert. [GÉ22a]

In der zweiten Iteration GN2 startete die Entwicklung des Interföderations-Services eduGAIN [GÉ18] - als Teil des *Trust & Identity* Bereiches - welcher im Szenario Inter-FIM in Abschnitt 2.3 detailliert beleuchtet wird. eduGAIN verknüpft nationale Authentifizierungs- und Autorisierungs-Infrastrukturen (vgl. Szenario nationales FIM in Abschnitt 2.2) und vereinfacht dadurch den weltweiten Zugriff auf zahlreiche wissenschaftliche Dienste unter Verwendung einer einzigen digitalen Identität. Die digitale Identität wird dabei von der Heimatorganisation eines Benutzers (z.B. Universität) - also entkoppelt von den zu nutzenden Diensten - verwaltet. Zu den über eduGAIN erreichbaren Diensten zählen u.a.: Cloud-/Speicher-Dienste, E-Publishing, Kollaborationsdienste wie Wikis, E-Learning oder Studien-Dienste zur bspw. Studienfinanzierung [GÉ21b]. Im Jahr 2011 wurde eduGAIN zum operativen Dienst und der Betrieb sowie die stetige Weiterentwicklung hält bis in die aktuelle Phase an. Ende des Jahres 2021 nutzen etwa 4600 Identity Provider und 3500 Service Provider aus Forschung und Lehre den Dienst [GÉ21b]. Davon stammen allein über 400 Entitäten aus Deutschland [GÉ21b]. Dazu zählen vielzählige deutsche Universitäten und Hochschulen aber auch wissenschaftliche Einrichtungen wie das Leibniz-Rechenzentrum [Lei21]. Hier verdeutlicht schon allein die internationale Quantität an Identity Providern und Service Providern die Relevanz dieses Dienstes für Forschung und Lehre.

Der Dienst eduGAIN ist primär für nationale Identitätsföderationen konzipiert, weswegen im Szenario nationales FIM (vgl. Abschnitt 2.2) zunächst nationale Identitätsföderationen unabhängig von eduGAIN betrachtet werden. Die erweiterte, internationale Kollaboration der im Szenario nationales FIM dargestellten nationalen Identitätsföderationen mittels eduGAIN, wird dann im Szenario Inter-FIM in Abschnitt 2.3 beleuchtet. Die beiden Szenarien sowie deren Reichweite bzw. Fokus werden ebenfalls in Abbildung 2.1a und 2.1b grafisch verdeutlicht. Die in den Grafiken abgebildeten Organisationen (mit „Org“ abgekürzt) können dabei entweder die Rolle eines Identity Providers und bzw. oder eines Service Providers annehmen. Von zunehmender Wichtigkeit werden auch Forschungsinfrastrukturen, die ihren Nutzern den Zugriff auf Ressourcen mittels den an eduGAIN teilnehmenden Identity Providern erleichtern wollen (siehe Abbildung 2.1c). Dieses Szenario wird in Abschnitt 2.4 weiter konkretisiert. Alle drei Szenarien repräsentieren somit reale Anwendungsfälle in R&E. Der Unterschied dieser Szenarien besteht dabei hauptsächlich in deren technischer Realisierung. Die daraus resultierenden Problemstellungen und Defizite im Zusammenhang mit Authentifizierungen werden im Folgenden szenarioweise erarbeitet.



(a) Nationales FIM

(b) Inter-FIM

(c) Forschungsinfrastrukturen

Abbildung 2.1: Übersicht der skizzierten Szenarien. Grafiken in Anlehnung an [GÉ17a]

2.2 Szenario 1: FIM in nationalen Identitätsföderationen

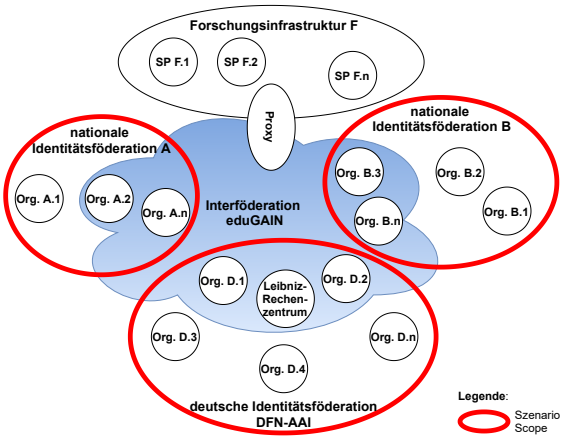


Abbildung 2.2: Nationales FIM

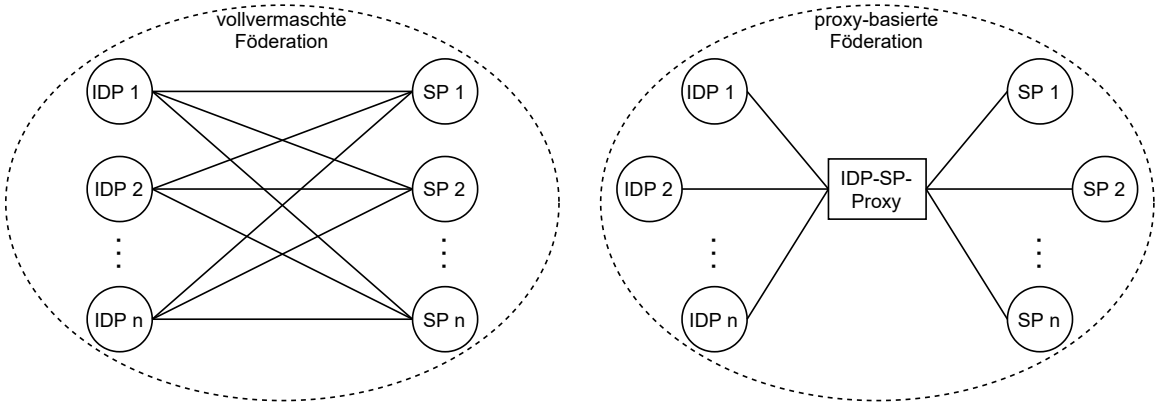
Im Bereich der nationalen Forschung und Lehre spannen eine Vielzahl von Ländern ein Wissenschaftsnetz auf, welches wissenschaftliche Institutionen und Einrichtungen, wie bspw. Universitäten und Forschungszentren, miteinander verknüpft. Organisatorisch gesehen ist jede dieser teilnehmenden wissenschaftlichen Organisationen eine autonome Instanz, die jedoch zum Zwecke der Forschung und Lehre miteinander kollaborieren. Abschnitt 2.1 hat dazu bereits die Abgrenzung zu einer Kooperation dargestellt und gezeigt, dass eine interorganisationale Kollaboration aufgrund des Bezuges dieser Arbeit zum föderierten Identitätsmanagement als **(Identitäts-) Föderation** bezeichnet wird. In diesem Anwendungsszenario spricht man von einer **nationalen Föderation** (vgl. auch Abbildung 2.2), da die Teilnehmer einer Föderation i.A. aus einem spezifischen Land stammen. Im Englischen hat sich weiter präzisierend der Begriff **National Research and Education Network**, kurz NREN, etabliert. Als „NREN“ wird einerseits das Netzwerk selbst bezeichnet, im allgemeinen Sprachgebrauch verkörpert der Begriff „NREN“ jedoch auch den *Provider* des entsprechenden Netzwerks.

Der Provider des Deutschen Forschungsnetzes (DFN) ist der gemeinnützige DFN-Verein [DFN10b], der das Netz betreibt und fortlaufend verbessert. Dazu zählen verschiedene Dienste. Die Kernkomponente des DFN stellt das Wissenschaftsnetz X-WiN dar, das mittels Glasfaserplattform wissenschaftliche Einrichtungen verbindet und mit entsprechender Bandbreite versorgt. Das Leibniz-Rechenzentrum (LRZ) ist bspw. aktuell mit 4x100 Gbit/s (technische Schnittstelle) am X-WiN angebunden. Das DFN agiert auch als Direktverbindung zu einigen Nachbarländern sowie als zentraler Knotenpunkt in das europäische Forschungsnetz GÉANT. Neben dem X-WiN bietet das DFN für R&E weitere relevante, maßgeschneiderte Dienste an, wie bspw. die Unterstützung der deutschen eduroam WLAN-Infrastruktur [GÉ20a] durch Bereitstellung eines deutschen eduroam Föderationsservers oder aber auch die Bereitstellung einer Authentifizierungs- und Autorisierungs-Infrastruktur (in Deutschland: DFN-AAI) [DFN10b]. Beide Dienste werden i.d.R. in den meisten europäischen und z.T. auch in internationalen NRENs angeboten bzw. unterstützt.

Fokus dieses Szenarios und dieser Arbeit stellt die **Authentifizierungs- und Autorisierungs-Infrastruktur (AAI)** dar, durch die Endnutzer auf webbasierte Dienste zugreifen können. FIM bietet die Chance, die Authentifizierung der Nutzer an die jeweilige Heimatorganisation des Nutzers auszulagern, sodass ein Dienst selbst keine Benutzerverwaltung implementieren muss und sich der Nutzer nur noch eine Benutzerkennung merken muss (i.S.v. *user centric design*). Im wissenschaftlichen Bereich wird dazu momentan überwiegend auf

die **Security Assertion Markup Language (SAML)** [CKPM05] zurückgegriffen. Auch **OpenID Connect** [SBJ+14b] rückt zunehmend in den Vordergrund.

Ferner haben sich zur Realisierung einer nationalen Identitätsföderation verschiedene Föderationsarchitekturen herauskristallisiert (vgl. exemplarisch und stark vereinfacht in Abbildung 2.3a und 2.3b). Die DFN-AAI basiert bspw. auf einem **vollvermaschten Konzept** (*engl. Full Mesh*) [GÉ17b], wobei jeder SAML Identity Provider über eine zentrale Metadaten-Datei mit jedem SAML Service Provider verknüpft ist. Dem gegenüber stehen Architekturen auf Basis eines Proxies. Eine detaillierte Übersicht über die verschiedenen FIM-Architekturmodelle ist in Abschnitt 3.2.4 zu finden. Der Verständlichkeit dienend, beschränkt sich das hier skizzierte Szenario zunächst auf **nationale Identitätsföderationen**, die auf einem **vollvermaschten Konzept** basieren. Ein FIM-Szenario in Kombination mit einem zentralen Proxy bzw. Hub wird im Szenario Forschungsinfrastrukturen adressiert.



(a) Vollvermaschte Föderation

(b) Proxy-basierte Föderation

Abbildung 2.3: Architekturmuster in Identitätsföderationen

Zur Verdeutlichung des Authentifizierungsworkflows, den ein Nutzer zum Zugriff auf einen föderierten Dienst durchläuft, wird im Folgenden auf ein Beispiel zurückgegriffen, bei dem sich ein Student (hier: Bob) bei einem FIM-fähigen Online-Lexikon anmelden möchte (vgl. auch SAML Workflow in Abbildung 3.2).

Da eine Vielzahl von Organisationen bzw. Föderationen noch keine Multi-Faktor-Authentifizierung, d.h. eine Authentifizierung mit mehr als einem Faktor, für ihre Nutzer anbieten, werden im Folgenden die Schritte eines Ein-Faktor-Authentifizierungsworkflows mit einer Kombination aus Benutzername und Passwort skizziert. Aus Sicht des Nutzers ist der Workflow über die bisher skizzierten Architekturmodelle hinweg grundsätzlich analog.

1. Der Student Bob möchte ein Online-Lexikon nutzen, das in seiner nationalen Föderation registriert ist. Dazu klickt Bob auf der Webseite des entsprechenden Dienstes auf den Login-Button, um sich zu authentifizieren. Dieser Anwendungsfall wird als *SP-initiated* [RHP+08] bezeichnet und stellt den inzwischen am häufigsten verwendeten Anwendungsfall dar.

2. Bob wählt den „Login mit föderierter Identität“ aus und bekommt eine Liste möglicher Identity Provider präsentiert. Er wählt seine Heimatorganisation aus, um sich dort zu authentifizieren. (Sollte seine Heimatorganisation dort nicht aufgelistet sein, kann das eine Vielzahl von Gründen haben. Z.B. die Heimatorganisation nimmt nicht an der Föderation teil oder die Liste möglicher Identity Provider wurde vorab anhand verschiedener Kriterien gefiltert. In diesem Fall kann Bob das Online-Lexikon nicht nutzen.)

3. Nach Auswahl seiner Heimatorganisation wird Bob zum Login-Interface seiner Heimatorganisation weitergeleitet. Dort gibt er seinen Benutzernamen, den er von seiner Heimatorganisation erhalten hat, zusammen mit seinem Passwort ein. Ist die Benutzername-Passwort-Kombination korrekt, wird Bob zurück zum Online-Lexikon geleitet. Im Hintergrund werden notwendige (Meta-) Informationen und Attribute zwischen Heimatorganisation und Service Provider ausgetauscht, die einerseits verwendet werden, um zu überprüfen, ob Bob berechtigt ist den Dienst zu nutzen und andererseits ggf. zur Personalisierung und Individualisierung des Dienstes dienen. Das von Bob eingegebene Passwort gelangt dabei zu keiner Zeit zu dem Service Provider und wird ausschließlich von Bobs Heimatorganisation geprüft. Die Heimatorganisation bestätigt dem Service Provider lediglich in Form einer Response, dass die Authentifizierung erfolgreich war und übermittelt entsprechende Benutzerattribute (z.B. Identifier, Affiliation). Zusätzlich kommen kryptographische Mittel, wie Zertifikate, zum Einsatz, um die Kommunikation zwischen Identity Provider und Service Provider abzusichern.

4. Nach positiver Zugriffsentscheidung durch den Service Provider kann Bob das Online-Lexikon entsprechend seiner Berechtigungen nutzen. Durch die Möglichkeit des Web Single Sign On (SSO) kann Bob nun auch Dienste anderer Service Provider nutzen ohne sich erneut bei seiner Heimatorganisation authentifizieren zu müssen.

Wie bereits in der Einleitung motiviert, wird folglich ein Betreiber eines Dienstes, v.a. wenn es sich um einen besonders schützenswerten Dienst handelt, seine Ressourcen nur dann zur Verfügung stellen, wenn sich dieser sicher sein kann, dass eine durchgeführte Benutzerauthentifizierung einer gewissen Qualität bzw. Stärke genügt. Da die für FIM-Services verwendete digitale Identität typischerweise derjenigen für IDP-interne Dienste entspricht, sollte es daher in beider Interesse sein entsprechende Maßnahmen, bspw. für sichere Passwörter, zu implementieren.

In einem vollvermaschten Szenario wäre der Idealzustand demzufolge, dass jeder Identity Provider einer nationalen Föderation eine eigene Lösung zur Multi-Faktor-Authentifizierung implementiert, die dann sowohl für kritische organisationsinterne Dienste als auch für kritische (inter-) föderierte Dienste herangezogen werden kann. Zugleich wird anhand eines standardisierten Assurance-Konzepts Vertrauensinformation zwischen den Teilnehmern einer (Inter-) Föderation ausgetauscht. Die Realität ist jedoch oft anders, da das Thema Multi-Faktor-Authentifizierung und Authentication Assurance ein sehr komplexes Themengebiet darstellt, welches nur mit ausreichenden Ressourcen und Kenntnissen gehandhabt werden kann. Der Wunsch, den ersten Faktor durch weitere Faktoren in Form eines Dienstangebots zu ergänzen, rückt daher zunehmend in den Vordergrund.

Aus dem hier skizzierten FIM-Szenario leiten sich somit die folgenden **Problemstellungen und Defizite** ab:

- Eine Vielzahl von **Identity Providern** betreibt (noch) keine Multi-Faktor-Authentifizierung oder diese ist nicht für (inter-) föderierte Zwecke nutzbar. Ein betroffener Nutzer kann somit diejenigen (inter-) föderierten MFA-Dienste, die MFA erfordern, nicht nutzen.

- Zwar stellen z.T. die **Betreiber einer Föderation** eine auf ihre Föderation zugeschnittene MFA-Lösung bereit, jedoch zeigt sich v.a. in vollvermaschten Föderationen, dass seitens der Betreiber oftmals keine für alle Teilnehmer nutzbare MFA-Lösung angeboten wird. Die Herausforderung in vollvermaschten Szenarien ist, dass im Gegensatz zu proxy-basierten Föderationen (vgl. Abbildung 2.3b oder Abschnitt 3.2.4) keine zentrale technische Instanz, im Sinne eines Proxies oder Hubs, vorhanden ist, die die Teilnehmer einer Föderation verknüpft und an die eine für alle Teilnehmer nutzbare MFA-Lösung angegliedert werden könnte (siehe Abbildung 2.4). Die vollvermaschte U.S. amerikanische Föderation InCommon ist bspw. eine der wenigen Föderationen, die einen Vertrag mit einem kommerziellen Anbieter ausgehandelt hat, anhand dessen teilnehmenden Identity Providern ein Third Party MFA-Dienst zu vergünstigten Konditionen an die Hand gegeben wird [Int21]. Die Integration dieses Dienstes hat nichtsdestotrotz pro IDP zu erfolgen.

- Ein Defizit in vollvermaschten Föderationen ist folglich, dass sobald IDP-seitig keine MFA-Lösung implementiert ist, betroffene Nutzer die durch MFA abgesicherten Dienste nicht nutzen können. In proxy-basierten Szenarien würde in einem solchen Fall (sofern vorhanden) ein Nutzer an einen an den Proxy angeschlossenen MFA-Dienst weitergeleitet werden, der die Überprüfung eines zweiten bzw. weiteren Authentifizierungsfaktors übernimmt, dann die Ergebnisse aller Überprüfungen aggregiert (d.h. sowohl erster Faktor als auch zweiter bzw. weitere Faktoren) und das Ergebnis an den Service Provider weiterleitet. Siehe hierzu Abbildung 2.4, die die fünf Ablaufschritte des Workflows visualisiert. Für vollvermaschte Föderationen ist ein analoger **Fallback-Workflow für MFA** wünschenswert.

- Folglich ist die Integration eines MFA-Dienstes bzw. -Systems auf Identity Provider Seite kein Teilziel dieser Arbeit, auch aufgrund der Tatsache, dass bereits eine Vielzahl dedizierter Lösungen auf dem Markt vorhanden sind [Jor17, Miz19]. Durch die Definition eines Fallback MFA-Workflows sollen jedoch existierende IDP-seitige MFA-Lösungen nach wie vor nutzbar bleiben. Da der Fokus dieser Arbeit auf dem (inter-) föderierten Identitätsmanagement liegt, wird eine Bereitstellung von MFA für organisationsinterne Dienste (z.B. Desktoparbeitsplätze, VPN) ebenfalls nicht angestrebt.

- Darüber hinaus ist FIM in R&E von zunehmendem Wachstum geprägt, sowohl seitens der Teilnehmer als auch bzgl. neuer Technologien. Es existiert jedoch kein technologieagnostisches Modell, um Authentifizierungsszenarien (d.h. Entitäten, Rollen, Dienste, Abhängigkeiten) strukturiert abzubilden. Eine derartige Beschreibungs- und Modellierungsfähigkeit ist aber in vielerlei Hinsicht sinnvoll:

- Zur Durchführung diverser Analysen (z.B. GAP- oder Security Analyse)
- Dem Design zukünftiger Architektur (-muster)
- Der Einführung neuer Technologien
- Der Identifikation von Nutzern, Kunden und Providern (dabei kann z.B. festgestellt werden, dass durch Nutzer, Kunden oder Provider verwendete Komponenten nicht mehr benötigt werden)
- Zur generischen Abstraktion aus der dann verschiedene Implementierungen abgeleitet werden können
- Der Ableitung wiederverwendbarer Schablonen

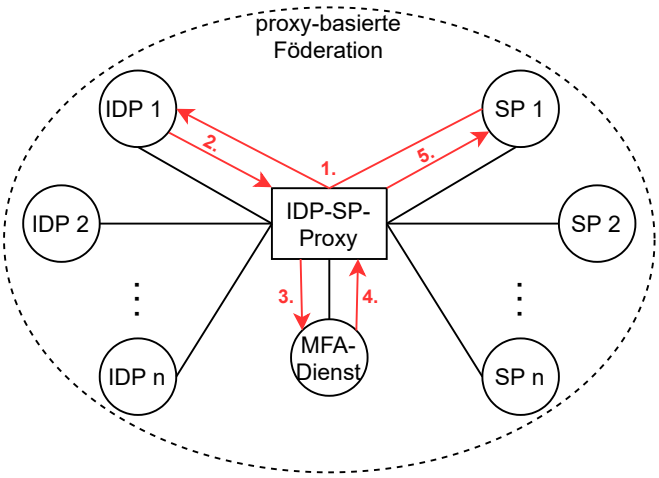


Abbildung 2.4: Schematische Darstellung einer Multi-Faktor-Authentifizierung unter Verwendung eines zentralen Proxies

2.3 Szenario 2: Inter-FIM in eduGAIN

Inter-FIM erweitert FIM um den Aspekt der *föderationsübergreifenden* Dienstnutzung. Damit kann ein Nutzer aus (nationaler) Föderation A mittels Authentifizierung bei seiner Heimatorganisation auf einen Dienst, der in (nationaler) Föderation B angeboten wird, zugreifen (vgl. Abbildung 2.5), wodurch bspw. Studierende eines Auslandssemesters profitieren können. In R&E ist dieser Interföderations-Service unter dem Namen *eduGAIN* bekannt und wird von dem GÉANT Projekt betrieben und stetig weiterentwickelt (vgl. Abschnitt 2.1). Ende des Jahres 2021 nehmen weltweit 73 NRENs an der Identitätsinterföderation eduGAIN teil [GÉ21b]. eduGAIN *erleichtert* somit die Dienstnutzung in skizziertem Szenario durch Bereitstellung einer Infrastruktur, ob ein Nutzer jedoch zur Dienstnutzung berechtigt ist, muss nach wie vor bilateral zwischen den involvierten Entitäten ausgehandelt werden. Dazu zählen u.a. auch die auszutauschenden, erforderlichen Attribute. Wie auch im Szenario nationales FIM zählen hier zu den interföderierten Diensten Dienste, die *über das Web* erreichbar sind.

Das Szenario Inter-FIM erweitert somit das in Abschnitt 2.2 skizzierte Szenario nationaler Identitätsföderationen. Hierbei werden die auf unterschiedlichen Architekturmustern basierenden nationalen Identitätsföderationen (z.B. vollvermascht, proxy-basiert) gemäß eines vollvermaschten Prinzips verknüpft. Technisch bedeutet das, dass alle SAML Identity Provider und SAML Service Provider, die an der Interföderation eduGAIN teilnehmen, in einer zentralen Metadaten-Datei aggregiert sind, die dann von allen Entitäten konsumiert wird.[1] Die Abbildung 2.6 stellt dies schematisch dar. Ein Nutzer bekommt dabei i.d.R. von der zugrundeliegenden technischen Realisierung nichts mit und der in Abschnitt 2.2 beschriebene 1FA-Workflow ist in diesem Szenario analog.

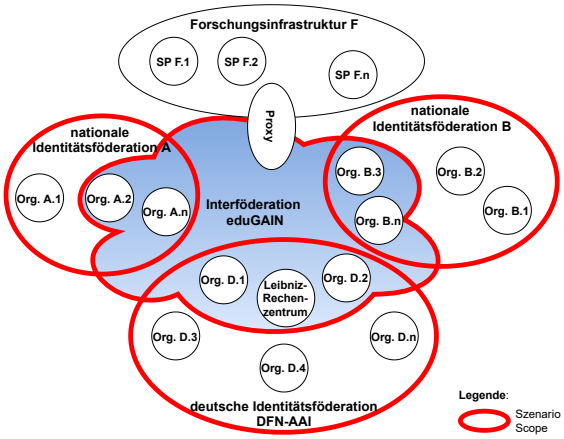


Abbildung 2.5: Inter-FIM

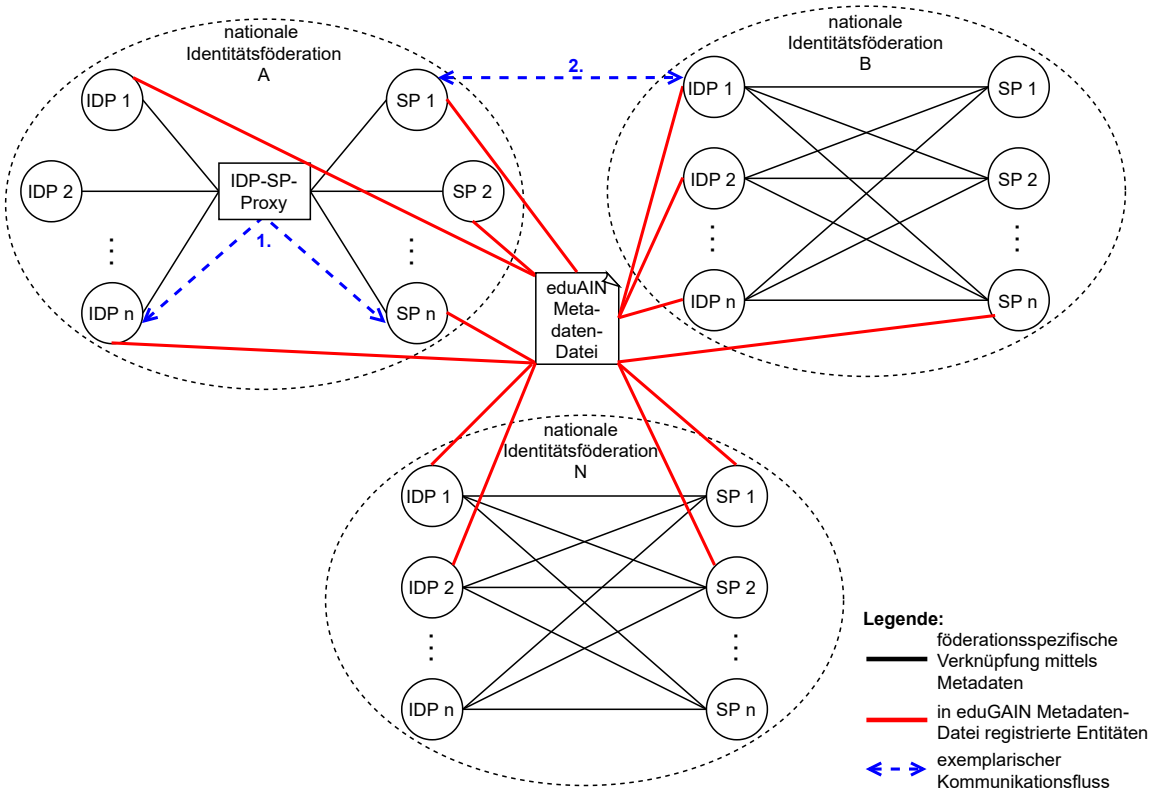


Abbildung 2.6: Schematische Darstellung der Interföderation eduGAIN

[1] Im Vergleich, in proxy-basierten Architekturen, kennen jeweils SAML IDPs und SAML SPs nur die Metadaten des Proxies, während der Proxy die Metadaten aller Teilnehmer kennt.

Abbildung 2.6 verdeutlicht ebenfalls, dass bspw. eine Kommunikation innerhalb einer proxybasierten Föderation über den entsprechenden Proxy stattfindet (vgl. Kommunikationsfluss 1, der blau eingefärbt ist), wohingegen bei einem föderationsübergreifenden Authentifizierungsworkflow (siehe Kommunikationsfluss 2) ein Proxy, abhängig von der Implementierung des Proxies, nicht zwangsweise in den Authentifizierungsworkflow involviert sein muss. Dies kann zur Folge haben, dass ein an den Föderationsproxy angeschlossener MFA-Dienst u.U. nicht nutzbar ist oder Nutzer sich bei mehreren MFA-Diensten registrieren müssten.

Die Herausforderungen spitzen sich in diesem Szenario, in Ergänzung zum Szenario nationales FIM, also aufgrund des enormen Skalierungsfaktors und der Heterogenität der Umgebung bzw. Architektur weiter zu. Dementsprechend kommen, wie in Abschnitt 2.6 ersichtlich werden wird, auch neue Anforderungen hinzu. Hier ist u.a. zu berücksichtigen, dass die involvierten Entitäten (i.S.v. Identity Provider, Service Provider) als auch die involvierten Föderationen ihre eigenen Modelle hinsichtlich Richtlinien, Verfahren und Teilnahme implementieren und somit bspw. föderationsübergreifende Kriterien zur Authentication Assurance aufgrund des autonomen Charakters kaum forcierbar sind und daher derart zu spezifizieren sind, dass konfliktäre Kriterien vermieden werden.

Aus dem Szenario Inter-FIM leiten sich folgende **Problemstellungen und Defizite** ab:

- In Ergänzung zum Szenario nationales FIM existiert auch in dem skizzierten Inter-FIM Szenario, z.B. bereitgestellt als Subservice von eduGAIN, zum Zeitpunkt der Recherche kein föderationsübergreifender Fallback-Workflow zur Multi-Faktor-Authentifizierung, um Identity Provider ohne MFA-Implementierung zu unterstützen.
- Ferner ist in eduGAIN die Verwendung und der Einsatz einer Multi-Faktor-Authentifizierung sowie der damit verbundene Austausch der Authentifizierungsqualität, auch Ein-Faktor-Authentifizierungen betreffend, nicht ausreichend standardisiert. Jedoch sind aufgrund des autonomen Charakters zwingende Vorgaben, bspw. zur Passwortsicherheit oder der Verpflichtung zur Implementierung von MFA, kaum realisierbar. Neue Lösungsansätze müssen folglich derart entworfen werden, dass sie freiwillig angenommen werden und nicht konfliktär zu vorhandenen organisations-/föderationsspezifischen Richtlinien stehen.
  - Dazu zählt, wie bereits erläutert, der Austausch zur Qualität einer Authentifizierung (Assurance-Information). Hier gibt es föderationsspezifische Konzepte, die jedoch von anderen Föderationen nicht interpretiert werden (können). Es wird daher ein möglichst **sinnvoller gemeinsamer Nenner** benötigt, auf den sich Teilnehmer einer Interfödertion einigen. Dieser könnte dann auch von (nationalen) Föderationen (siehe Abschnitt 2.2), die aktuell gar kein Assurance-Konzept verwenden, herangezogen werden.[2]
  - Aktuell müssen Service Provider den wenig konkreten Aussagen über stattgefundene Authentifizierungen vertrauen und erhalten kaum Informationen über durchgeführte Authentifizierungen (z.B. garantierte Passwortstärke).

[2] Wird kein dediziertes Assurance-Konzept verwendet, werden bspw. die von SAML definierten Standard-Authentifizierungskontexte [KCM+05] wie *PasswordProtectedTransport* ohne weitere Qualitätskriterien herangezogen.

- Identity Provider und Service Provider werden bei dem Thema Authentication Assurance und auch Assurance im Allgemeinen kaum unterstützt.
  - Identity Provider benötigen Hilfestellung bei der (schrittweisen) Einführung eines föderationsübergreifenden Konzeptes zur Authentifizierungsqualität (vgl. vorheriger Listenpunkt).
  - Service Provider müssen aktuell selbst entscheiden, ob MFA für ihren angebotenen Dienst bzw. Dienste sinnvoll ist oder nicht. Hilfestellungen und Referenzdokumente über vorhandene Anwendungsfälle und Risikobewertungen sind wünschenswert.

2.4 Szenario 3: Internationale Forschungsinfrastrukturen

Eine Forschungsinfrastruktur (engl. *research infrastructure*), in kurz: R-Infrastruktur bzw. R-Infra, ist eine von nationalen Identitätsföderationen unabhängige Infrastruktur für Forscher und teilnehmende Einrichtungen. Sie unterscheiden sich dahingehend von nationalen Identitätsföderationen, dass sie typischerweise nicht auf ein einziges Land beschränkt sind, sondern Forscher aus diversen Ländern, meist mit dem Interesse an einem gemeinsamen, spezifischen Forschungsbereich vernetzen [ZSL19]. Eine R-Infrastruktur ist dabei üblicherweise Teil einer übergreifenden, fach-spezifischen *Research Community*, die die Gesamtheit aller Forschenden in dem jeweiligen Fach darstellt. Exemplarisch wird an dieser Stelle die Research Community der Lebenswissenschaften (*engl. Life Sciences*) genannt, die wiederum mehrere R-Infrastrukturen umfasst. Ein Beispiel ist die auf biologische Daten spezialisierte R-Infrastruktur ELIXIR [ELI21], deren über 180 teilnehmende Forschungseinrichtungen über ganz Europa verteilt sind. ELIXIR beschäftigt sich mit menschlichen (Genom-) Daten und ermöglicht Zugriff auf sensible Daten.

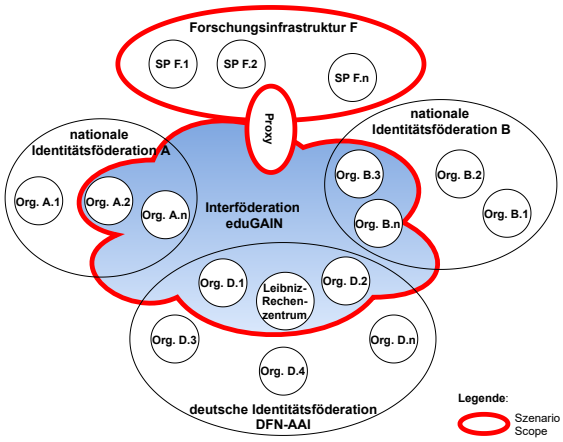


Abbildung 2.7: Forschungsinfrastrukturen

Die Gruppe FIM4R (Federated Identity Management for Research), die mit Interessensvertretern zahlreicher Research Communities und Infrastructures zur Etablierung von FIM zur Authentifizierung und Autorisierung in Research Communities und Infrastructures kollaboriert, hat im Paper FIM4Rv2 [ABB+18] eine Liste beitragender Communities publiziert. Im Vergleich zur vorhergehenden FIM4R Version 1 [BJK+13] zeigt sich, dass auch hier das Interesse an FIM gestiegen ist. Zur Verdeutlichung der Relevanz zeigt die folgende Auflistung die aktuell beitragenden Communities (in Englisch aufgelistet) [ABB+18]:

- *Arts and Humanities*
- *Climate Science*

- *Earth Observation (EO)*
- *European Neutron and Photon Facilities (umbrellaID)*
- *Gamma-Ray Astronomy*
- *Gravitational Wave Astronomy*
- *High Energy Physics*
- *Ionospheric and Atmospheric Science*
- *Infectious Disease Research*
- *Life Sciences*
- *Linguistics*
- *Nuclear Physics*
- *Radio Astronomy*
- *Virtual Atomic and Molecular Data Centre*

Als Teil des o.g. FIM4Rv2 Papers und der darin referenzierten Research Communities wurden ebenfalls Anforderungen erfasst und innerhalb einer Matrix kategorisiert. Die Kategorie „*Assurance & Multi Factor Authentication (MFA)*“ [ABB+18] verdeutlicht hierbei die Notwendigkeit das Vertrauen in Identitäten und Authentifizierungen (bspw. durch Einführung von MFA) zu steigern und zu kommunizieren. In [ABB+18] wird auf zwei high-level Anforderungen verwiesen, nämlich das Fortführen der Arbeiten am Assurance Framework zur Bewertung und zum Austausch von Identitäts- und Authentifizierungsinformation sowie die Unterstützung von MFA und die Aufnahme von MFA-Information in Authentifizierungstokens und Metadaten. Nach Befragung geeigneter „Ecosystem Constituents“ hat sich gezeigt, dass beide Anforderungen in skizziertem Umfeld von Relevanz sind, die Anforderung an ein Assurance Framework gegenüber der Anforderung an MFA jedoch stärker priorisiert wurde.

Ferner wurden zu einem früheren Zeitpunkt in [LGP+15] im Rahmen eines Interviews mehrere Infrastrukturen hinsichtlich eines minimalen Assurance Levels befragt, woraus insgesamt sechs high-level Anforderungen entstanden sind. Davon beschäftigen sich vier dieser Anforderungen mit der Identity Assurance, die in dieser Arbeit ausgeklammert wird, und auf Basis ebenjener Anforderungen inzwischen ein Identity Assurance Framework entstanden ist.[3] Die Anforderung zur Authentication Assurance „*Password authentication (with some good practices)*“ [LGP+15] stellt klar, dass Authentifizierungen auf Basis von Passwörtern für Anwendungsfälle mit geringem Risiko ausreichend sind, jedoch anerkannte Qualitätskriterien wie bspw. Passwortlänge und -komplexität festzulegen sind. Die Letzte der sechs

[3] Die Recherche zu dieser Arbeit startete Anfang 2017 als das oben genannte Identity Assurance Framework noch nicht existierte. Dieses wurde erst im Jahr 2018 zusammen mit hier referenzierten Teilen zur Authentication Assurance veröffentlicht [ZSL19, Zie18, REF18c]. Aus diesem Grund werden diese Aspekte in dem hier vorliegenden Kapitel 2 (Anforderungsanalyse) und Kapitel 3 (Grundlagen) noch nicht als gegeben angesehen, sondern sind Teil der späteren Konzeption (Kapitel 4) und Spezifikation (Kapitel 5).

high-level Anforderungen in [ABB+18] nimmt Bezug auf die Überprüfung der Konformität und beschreibt, dass eine regelmäßige Selbsteinschätzung (*engl. self-assessment*), anstatt kostenintensiver Audits, ausreichend ist.

Um internationale Forschungskollaborationen auf dem Weg zur Etablierung von FIM zu unterstützen, wurde im Rahmen des europäischen Forschungsprojekts AARC, ein Software-Baukasten, die *AARC Blueprint Architecture* (AARC-BPA), entwickelt. Das AARC-BPA-Modell greift auf die Verwendung eines Proxies zurück, der als zentrale Vermittlungsstelle zwischen Benutzerverwaltungsdiensten und den zu nutzenden Diensten agiert (vgl. IDP-SP-Proxy in Abbildung 2.8) und gleichzeitig die Integration von Systemen zur Benutzerregistrierung und Gruppenmanagement ermöglicht. Gleichzeitig fügt AARC-BPA Funktionalität zum Zugriff auf Non-Web Services hinzu. AARC-BPA ermöglicht die Integration mit eduGAIN, sodass der Proxy als Integrationspunkt für R-Infrastruktur Services verwendet werden kann. Damit muss nicht jeder Service separat mit nationalen Identitätsföderationen bzw. eduGAIN verknüpft werden. [AAR19]

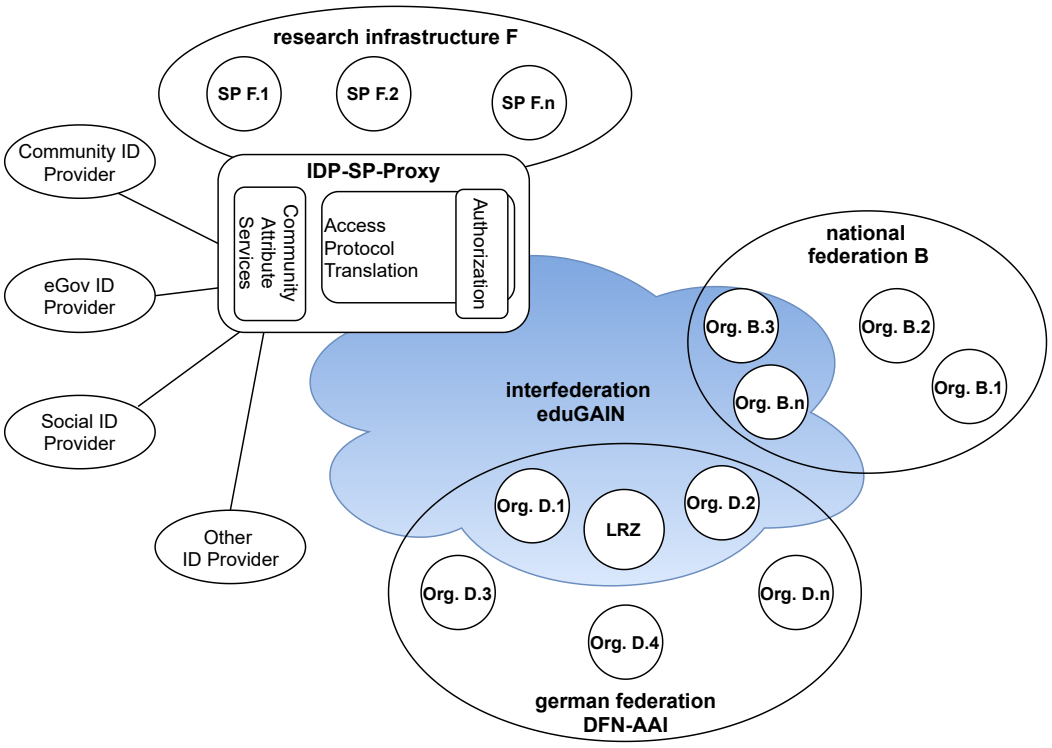


Abbildung 2.8: Schematische Darstellung einer Forschungsinfrastruktur auf Basis des AARC-BPA Modells [AAR19]

Abbildung 2.8 verdeutlicht auch, dass sich Forschungskollaborationen dahingehend von den Szenarien nationales FIM und Inter-FIM abgrenzen, dass hier typischerweise auf mehrere Arten externer Identity Provider zurückgegriffen wird[4] und das Konzept des **Identity**

[4]Nutzeridentitäten aus eduGAIN stellen dabei nur eine mögliche Quelle dar, zum Einsatz kommen u.a. auch *Social Accounts* oder *Governmental Accounts*.

Linking zur Authentifizierung von Nutzern herangezogen wird. Dabei erhält ein Nutzer zu Beginn eine sogenannte „Infrastruktur Identität“, die häufig mit Hilfe o.g. externer Identity Provider initiiert wird und dann mit entsprechender Gruppenzugehörigkeit und Rolleninformation versehen wird [VELL+18]. Werden mehrere externe Identitäten mit der Infrastruktur Identität verlinkt, resultieren daraus auch mehrere Authentifizierungsoptionen mit potentiell unterschiedlicher Authentication Assurance. Daher wird auch hier strukturierte Assurance-Information seitens der Identity Provider benötigt, damit diese dann zusammengeführt werden kann, um das Assurance Level eines Nutzers zu erhöhen.

Bezüglich eines Fallback MFA-Workflows existierte während der initialen Recherchearbeit für proxy-basierte Authentifizierungsszenarien in Forschungskollaborationen - im Falle, dass die Heimatorganisation bzw. der Identity Provider kein MFA liefern kann - noch kein derartiger Workflow als Teil der AARC-BPA; dieser wurde aber inzwischen in [SLV+18] erarbeitet und publiziert. Ferner wurden im Rahmen von eduTEAMs, eine auf *Virtual Organizations* (VOs) basierende Implementierung der AARC-BPA, verschiedene bereits existierende MFA-Proxy-Lösungen untersucht [ZvD18] und anhand einer zentralen, proxy-seitigen MFA-Implementierung gelöst. Folglich ist für proxy-basierte Umgebungen ein entsprechender Fallback MFA-Workflow bereits vorhanden, wohingegen dies für vollvermaschte Szenarien nicht der Fall ist. Die Arbeit knüpft daher an dieser Stelle an.

Bei Betrachtung aller drei Szenarien zeigt sich somit, dass, obwohl es sich um jeweils unterschiedliche bzw. eigenständige Szenarien handelt, ähnliche Herausforderungen existieren. Aus diesem Grund werden anhand eines modularen Architekturkonzepts entsprechende Lösungsansätze entwickelt, die die Anforderungen der Szenarien, die in Abschnitt 2.6 abgebildet sind, berücksichtigen.

Nach der Skizzierung der Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen in den Abschnitten 2.2 bis 2.4, werden im Folgenden, basierend auf den Problemstellungen und Defiziten aller Szenarien, modulare Lösungsansätze bzw. Konzepte abgeleitet.[5] Hierbei wird nach der Analyse o.g. Punkte deutlich, dass **Lösungsansätze für drei zentrale Themenkomplexe** benötigt werden, die wiederum die Basis für die in Abschnitt 2.5 erarbeiteten Hauptanforderungen bilden.[6]

- **Konzeption eines Fallback MFA-Workflows**
  - Erarbeiten eines Fallback MFA-Workflows für vollvermaschte Authentifizierungsszenarien in FIM
  - Berücksichtigung vorhandener 1FA-Implementierungen
  - Unterstützung verschiedener Zweitfaktor-Provider und dynamische Auswahl der Provider

[5] Die Begriffe *Lösungsansatz*, *(Teil-) Lösung* bzw. *Konzept* werden in dieser Arbeit synonym verwendet.

[6] Die drei zentralen Themenkomplexe werden in Abschnitt 2.5 durch vier Hauptanforderungen widergespiegelt. Dies lässt sich darauf zurückführen, dass in Bezug auf das Authentication-Assuance-Konzept zwischen der Definition des Konzeptes und der Umsetzungsunterstützung des Konzeptes differenziert wird.

- **Authentication-Assurance-Konzept**
  - Erarbeiten eines sinnvollen gemeinsamen Nenners unter Berücksichtigung vorhandener LoA-Konzepte; Vordergründig sind leichtgewichtige Kriterien zur Unterstützung der freiwilligen Annahme durch die Teilnehmer
  - Getrennte Betrachtung der Authentication Assurance und der Identity Assurance, um verschiedene Anwendungsfälle bzw. Assurance-Anforderungen abzudecken
  - Berücksichtigung verschiedener Typen von Authentifizierungsfaktoren (vgl. Abschnitt 3.4.1)
  - Definition von Kriterien unabhängig von nationalen Gegebenheiten (wie z.B. Gesetze)
  - Umsetzungsunterstützung zur Implementierung des Authentication-Assurance-Konzepts
- **Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien**
  - Beschreibung und Modellierung unabhängig von zugrundeliegenden Authentifizierungsprotokollen, -standards, -technologien und -rahmenwerken
  - Berücksichtigung des gesamten Lebenszyklus eines Services
  - Erzeugung von Schablonen (*engl. Templates*)

Um die verschiedenen Herausforderungen und Defizite der drei aufgelisteten, zentralen Themenkomplexe zu adressieren, ist eine modulare Architektur einer monolithischen Architektur vorzuziehen. Zur Verbildlichung kann dies mit einem Werkzeugkasten mit verschiedenen Werkzeugen gleichgesetzt werden, die je nach Szenario individuell kombiniert bzw. angewendet werden können.

2.5 Fazit: Notwendigkeit modularer Konzepte zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM

Neben den in den Abschnitten 2.2 bis 2.4 skizzierten Szenarien aus der Forschung und Lehre wurde zusätzlich untersucht, ob weitere Szenarien zu FIM,[7] u.a. in Kombination mit starker Authentifizierung, in anderen Bereichen existieren. Dabei zeigt sich, dass FIM bzw. die Verwendung föderierter Standards und Protokolle auch im kommerziellen Sektor Anwendung findet. Ein Beispiel stellt hierbei Odette SESAM [Jod08] dar, eine sektorspezifische Föderation auf Basis des Protokolls SAML 2.0 aus der Automobilbranche. Hier wurden im Rahmen der Odette Working Group, die u.a. aus namhaften Automobilherstellern besteht, technische Empfehlungen zur Implementierung in der Automobilbranche erarbeitet.

[7] Aus Gründen der besseren Lesbarkeit subsumiert im Folgenden der Begriff bzw. die Abkürzung „FIM“ das föderierte Identitätsmanagement sowie dessen Spezialisierung des interföderierten Identitätsmanagements. Ist explizit von Inter-FIM die Rede wird dies entsprechend referenziert.

Ein weiteres Beispiel zu Identitätsföderationen mit Bezug zum Cloud-Computing stellt Amazon Webservices (kurz: AWS) dar. AWS beschreibt eine Föderation als einen Ansatz zum Aufbau eines Zugriffskontrollsystems, bei dem Nutzer anhand eines zentralen IDPs verwaltet werden, um Zugriff auf mehrere Applikationen bzw. Services zu erhalten [Ama21]. AWS unterstützt dabei die gängigen, offenen Standards SAML 2.0 [CKPM05], OpenID Connect [SBJ+14b] und OAuth 2.0 [Har12]; inwieweit AWS komplexe, multilaterale Föderationsstrukturen unterstützt (vgl. R&E Szenarien), geht jedoch nicht hervor.

Ein weiterer, repräsentativer Anwendungsfall stammt aus dem Finanzsektor. Unter Verwendung föderierter Standards bzw. Protokolle werden hier im Bereich Fintech (kurz für *engl. financial technology*), das i.A. mit der Digitalisierung von Finanzdienstleistungen assoziiert wird, Schnittstellen zwischen Banken und Third Party Providern etabliert bzw. geöffnet, um die bisherigen Dienstleistungen der Banken zu digitalisieren als auch um neue, kundenorientierte und potentiell disruptive Banking-Geschäftsmodelle bereitzustellen. Die Öffnung der Banken bzw. der Zugriff auf Kundendaten für Third Parties wird in diesem Zusammenhang als *Open Banking* bezeichnet und unterliegt in der EU der *Payment Service Directive* (PSD2) [Eur15b], die eine Zahlungsdienstrichtlinie der Europäischen Kommission darstellt. Hierbei zeigt sich, dass die Anforderungen denjenigen aus den Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen ähnlich sind. Neben dem Consent Management, das die ausdrückliche Zustimmung des Verbrauchers bzw. des Kunden erfordert, um einen Zahlungsvorgang auszulösen, wird mit PSD2 auch die Verpflichtung einer starken Kundenauthentifizierung eingeführt [Deu21a]. Ferner spielt auch die Assurance im Finanzsektor eine Rolle. So wird u.a. getrieben durch gesetzliche Bestimmungen (wie z.B. Anti-Money Laundering Directive V (AMLD V) [Eur18]) innerhalb einer Working Group der OpenID Foundation [Ope21a] die Kommunikation von Identity-Assurance-Information standardisiert. Zusätzlich wird deutlich, dass die länderübergreifende Verteilung der Entitäten in Bezug auf einheitliche Verfahren auch hier eine Herausforderung darstellt.

Beim Vergleich der Herausforderungen und Defizite mit den Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen zeigt sich, dass auf high-level Ebene zwar Ähnlichkeiten hinsichtlich der Anforderungen vorhanden sind, diese jedoch bei genauerer Betrachtung nicht 1:1 abbildbar sind. Während in R&E Anforderungen, z.B. an die Implementierung von MFA, kaum übergreifend und verpflichtend durchsetzbar sind, unterliegt z.B. der Finanzsektor hingegen starken gesetzlichen Regulierungen, die in der EU bspw. durch Richtlinien der Europäischen Kommission festgeschrieben sind, wodurch auch Anforderungen an die minimale Qualität von Passwörtern oder Authentifizierungstoken auf eine andere Art und Weise forcierbar sind. Auch hinsichtlich der Überprüfung der Konformität kann im kommerziellen Sektor auf strengere Maßnahmen zurückgegriffen werden als in R&E. Ferner wird deutlich, dass R&E Identitätsföderationen häufig komplexere Ausprägungen aufweisen als bspw. im kommerziellen Sektor. Zu den Standardfällen im kommerziellen Sektor zählen meist 1:n oder n:1 Föderationen, d.h. ein Identity Provider kann zum Login bei mehreren Services verwendet werden oder ein Service Provider erlaubt Logins von diversen Identity Providern. Weniger verbreitet sind multilaterale bzw. vollvermaschte Föderationen (n:m) wie in R&E.

Insgesamt zeigt sich, dass die resultierenden Anforderungen nicht ausreichend deckungsgleich sind, als dass diese in einer gemeinsamen Architektur aggregiert werden könnten, weswegen

diese Arbeit in Abschnitt 2.6 verfeinerte Anforderungen im Hinblick auf die Authentication Assurance und die Multi-Faktor-Authentifizierung auf Basis der Szenarien des nationalen FIM, des Inter-FIM und der Forschungsinfrastrukturen ableitet. Zu den Herausforderungen zählen hier insbesondere:

- Das Vorhandensein unterschiedlicher Föderationsarchitekturen (wie z.B. vollvermascht, proxy-basiert) sowie verschiedene Ansätze zur Multi-Faktor-Authentifizierung und deren Integrierbarkeit
- Die Diversität verwendeter Technologien und Protokolle
- Die starke Autonomie involvierter Entitäten hinsichtlich der Durchsetzung verbindlicher Vorgaben sowie die z.T. vorhandene Ressourcenknappheit
- Das Herstellen und Vermitteln von Vertrauen bei Authentifizierungen zwischen Entitäten

Aus den identifizierten Problemstellungen und Defiziten der Szenarien aus den Abschnitten 2.2 bis 2.4 werden im Folgenden **Hauptanforderungen an Teillösungen bzw. Konzepte für eine Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM** abgeleitet. Die Identifikation von Hauptanforderungen dient zunächst nur zur übergeordneten Gruppierung, welche dann im Rahmen einer umfangreichen Anforderungsanalyse in Abschnitt 2.6 weiter konkretisiert werden. Die Klassifikation, Eingliederung und das Zusammenspiel der zu erarbeitenden Teillösungen bzw. Konzepte sowie den dabei involvierten Komponenten findet dann in Kapitel 4 im Rahmen der Konzeption einer Architektur statt.

Die Ableitung feingranularer Anforderungen in Abschnitt 2.6 basiert zum Einen auf den gewonnenen Erkenntnissen aus dem Tätigkeits- und Projektumfeld der Autorin sowie zum Anderen auf den z.T. zu dieser Thematik veröffentlichten Dokumenten. Die Dokumente werden dazu in den Abschnitten 2.6.2 bis 2.6.5 an den entsprechenden Stellen referenziert. Durch die Involvierung der Autorin in verschiedene Working Groups zum Thema Trust und Assurance in R&E konnten einerseits Anforderungen identifiziert als auch diskutiert und verifiziert werden. Da sich das Projektumfeld und die erwähnten Working Groups neben Forschenden größtenteils aus Betreibern - wie Interföderations-, Föderations-, R-Infra-, Identity Providern und Service Providern - zusammensetzt, welche wiederum die entsprechenden Nutzergruppen repräsentieren, fand während der Entstehung dieser Arbeit ein umfassender und andauernder Austausch der Autorin mit zentralen Interessensgruppen statt, um zur Vollständigkeit der Anforderungen beizutragen.

- **Hauptanforderung AK: Definition eines leichtgewichtigen Authentication-Assurance-Konzepts zum Austausch der Qualität durchgeführter Authentifizierungen**

  (*AK abgeleitet von Authentication-Assurance-Konzept*)

  Damit Service Provider Rückschlüsse über die Stärke einer durchgeführten Authentifizierung ziehen können, muss Vertrauen durch den Austausch von Authentifizierungsinformation hergestellt werden. Da z.T. bereits spezifische Konzepte vorhanden sind,

muss ein organisations- bzw. föderationsübergreifendes gemeinsames Verständnis erarbeitet werden. Dies kann nur, auch unter den Aspekten der Ressourcenknappheit und Konfliktfreiheit, mit Hilfe eines leichtgewichtigen Ansatzes erfolgen.

- **Hauptanforderung RM: Umsetzungsunterstützung für Service Provider[8] zur Auswahl eines angemessenen Authentication-Assurance-Profils**

  (*RM abgeleitet von risikobasierten Maßnahmen*)

  Da nicht jeder Dienst eines föderierten Szenarios zwangsweise ein höheres Assurance Level benötigt, sollten Service Provider, basierend auf der Kritikalität und der dem Dienst ausgesetzten Risiken, eine Bewertung des für sie passenden Assurance Levels durchführen. Es kann jedoch nicht davon ausgegangen werden, dass jeder Service Provider einen Risikomanagement-Prozess (bspw. im Sinne der ISO 27001 [ISO13a]) etabliert hat, weswegen Service Provider in ihrer Bewertung und Entscheidungsfindung zu unterstützen sind.

- **Hauptanforderung WF: Analyse existierender MFA-Realisierungsoptionen und Konzeption eines Fallback MFA-Workflows für vollvermaschte Authentifizierungsszenarien**

  (*WF abgeleitet von (MFA-)Workflow*)

  Nutzer, deren Heimatorganisation bzw. Identity Provider aufgrund verschiedener Gründe (u.a. Ressourcenknappheit, Fachwissen-Mangel) keine eigene MFA-Lösung implementieren können, sollen die Möglichkeit besitzen auf einen Fallback MFA-Workflow mit externem Zweitfaktorprüfer zurückgreifen zu können, um somit nicht von einem SP, der MFA erfordert, abgewiesen zu werden. Da bereits verschiedene MFA-Implementierungen (vgl. Abschnitt 3.5) existieren, ist zu überprüfen inwieweit diese geeignet sind und inwiefern alternative Modelle bzw. Workflows für vollvermaschte Szenarien verwendet werden können. Dabei soll möglichst sparsam mit Anpassungen auf IDP-Seite umgegangen werden und, wenn möglich, für Benutzer bereits bekannte Mechanismen wiederverwendet werden.

- **Hauptanforderung UM: Service-orientierte und ganzheitliche Beschreib- und Modellierbarkeit von Entitäten und Diensten eines Authentifizierungsszenarios unabhängig von zugrundeliegendem Protokoll, Standard, Technologie oder Framework**

  (*UM abgeleitet von Universelles Modell*)

  Bevor ein existierendes Ein-Faktor-Authentifizierungsszenario um Konzepte zur Multi-Faktor-Authentifizierung erweitert wird, sollten zuerst alle (i.S.v. Ganzheitlichkeit) involvierten Entitäten, Dienste sowie deren Abhängigkeiten identifiziert und abgebildet

[8] Um seitens des Identity Providers ein entsprechendes Authentication Assurance Level bzw. Profil signalisieren zu können, sind organisationsinterne Prozesse und Verfahren gegen die entsprechenden Kriterien zu evaluieren, was bspw. durch Maßnahmen wie Schulungen, Workshops oder (gegenseitige) Überprüfung bzw. Audits unterstützt werden kann. Der Aufbau eines derartigen Programms für Identity Provider wird in dieser Arbeit jedoch nicht weiter untersucht, sondern als gegeben vorausgesetzt.

werden, sodass neue Komponenten auf eine koordinierte Art und Weise in ein bestehendes Szenario integriert werden können. Bei Betrachtung der Ganzheitlichkeit in Bezug auf die Service-Orientierung sollten ebenfalls die verschiedenen Phasen eines Service-Lifecycles berücksichtigt werden, sodass das zu spezifizierende Modell sowohl bspw. in der Design-Phase von Software-Architekten oder während des Betriebs von Pentestern herangezogen werden kann. Da föderierte Szenarien zudem eine hohe Diversität an eingesetzten Protokollen, Standards, Technologien und Frameworks aufweisen können, ist ebenfalls eine uniforme Beschreib- und Modellierbarkeit vorteilhaft.

2.6 Anforderungsanalyse

Da es sich bei Identity Providern im Allgemeinen (vgl. z.B. Finanzsektor) als auch denjenigen aus Forschung und Lehre (z.B. Universitäten oder Hochschulen) häufig um Organisationen handelt, deren primärer Fokus nicht der Betrieb, die Wartung und die Weiterentwicklung von technischen Komponenten zur (inter-) föderierten Nutzung darstellen, rücken Dienstangebote (*engl. offered services* oder *as-a-service*) zur Multi-Faktor-Authentifizierung zunehmend in den Vordergrund. Neben der reinen Quantität an Identity Providern in R&E, fehlen R&E Identity Providern häufig auch die notwendigen Ressourcen oder die Expertise, um MFA bereitzustellen. Zwar werden z.T. in wissenschaftlichen Einrichtungen bereits Zweitfaktoren bereitgestellt, jedoch sind diese oft rollen-gebunden (z.B. für Mitarbeiter, nicht aber Studenten) und lediglich für den Zugriff auf organisationsinterne Systeme gedacht. Dazu kommt, dass abhängig von der jeweiligen MFA-Lösung diese womöglich nicht ohne Weiteres mit einem FIM-Protokoll für organisationsübergreifende Dienste kompatibel ist. Das Ziel dieser Arbeit ist daher, ein Architekturkonzept auf Basis der vier Hauptanforderungen zu entwickeln, das neben einem zu spezifizierenden Fallback MFA-Workflow für vollvermaschte Authentifizierungsszenarien (vgl. Hauptanforderung WF) ebenfalls ein universelles Modell zur Beschreib- und Modellierbarkeit von Authentifizierungsszenarien (vgl. Hauptanforderung UM) sowie ein leichtgewichtiges Authentication-Assurance-Konzept mit Hilfestellungen für Anwender (vgl. Hauptanforderungen AK und RM) spezifiziert.

2.6.1 Verschiedene Anforderungstypen

Zur vollständigen und zweckmäßigen Erfassung sowie aus Strukturierungsgründen findet die Anforderungsanalyse Top-Down auf Basis der vier Hauptanforderungen statt. Die Anforderungen der Infrastrukturbetreiber, der Identity Provider bzw. Service Provider Rollen sowie der Benutzer sind dabei unter der entsprechenden Hauptanforderung subsumiert.

Zugleich werden Anforderungen während der Anforderungsanalyse gemäß ihres Typs klassifiziert. Dazu wird zwischen den folgenden **Anforderungstypen** unterschieden:

- **Funktionale Anforderung (FA)**: Funktionale Anforderungen beziehen sich auf die Funktionalität oder den Zweck eines Systems.

- **Nicht-funktionale Anforderung (NFA)**: Nicht-funktionale Anforderungen hingegen beziehen sich auf übergreifende Aspekte eines Systems (z.B. Antwortzeiten, Wartbarkeit) und sind im Gegensatz zu funktionalen Anforderungen eher produkt-unspezifisch. Die Abgrenzung zwischen funktionalen Anforderungen und nicht-funktionalen Anforderungen ist daher nicht immer trennscharf.
- **Sicherheitsanforderung (SIA)**: Bezieht sich auf die Sicherheit eines Systems oder Umgebung. Hier werden Anforderungen zum Schutz vor Angriffen und unrechtmäßigem Zugriff erarbeitet.
- **Datenschutzanforderung (DSA)**: Da in Authentifizierungsszenarien personenbezogene Daten verarbeitet und kommuniziert werden, werden hier Anforderungen definiert, um diese bestmöglich zu schützen.

2.6.2 Top-Down Analyse der Hauptanforderung AK

Da die Einführung einer Multi-Faktor-Authentifizierung auf einer existierenden Ein-Faktor-Infrastruktur aufbaut und somit in einer Erweiterung der vorhandenen Ein-Faktor-Authentifizierungskonzepte resultiert, werden im Folgenden zunächst Anforderungen definiert, um ein gemeinsames Verständnis hinsichtlich der Qualität durchgeführter Authentifizierungen zu etablieren.

Zwar existieren bereits verschiedene LoA-Standards, -Normen und Rahmenwerke (vgl. Abschnitt 3.6), wie bspw. die Digital Identity Guidelines vom National Institute of Standards and Technology (NIST) [GGF17b, GFL+17, GFN+17, GRS+17], jedoch sind die auf rund 250 Seiten enthaltenen Anforderungen viel zu umfassend und enthalten eine Vielzahl von Anforderungen, die in R&E Föderationen nicht umsetzbar sind. Im Folgenden werden daher Anforderungen definiert, um existierende LoA-Rahmenwerke[9] zu evaluieren und anhand derer Ergebnisse bewertet werden kann, inwieweit ein maßgeschneidertes Authentication-Assurance-Konzept für R&E benötigt wird.

Aufgrund des high-level Charakters der aufgeführten Anforderungen in [LGP+15] (vgl. Abschnitt 2.4) werden die Anforderungen an ein leichtgewichtiges Authentication-Assurance-Konzept, das in föderierte AAIs integrierbar ist, im Folgenden erneut aufgegriffen und weiter konkretisiert:

> [FA_LoA_1FA]: Ein Authentication-Assurance-Konzept muss dedizierte Anforderungen an die Qualität von Authentifizierungen mit einem Faktor stellen (z.B. minimale Passwortlänge) und zwischen verschiedenen, typisch genutzten Faktortypen unterscheiden.
>
> [FA_LoA_MFA]: Ein Authentication-Assurance-Konzept muss ebenfalls Anforderungen an die Qualität von Authentifizierungen mit zwei oder mehreren Faktoren definieren.

[9] Im Folgenden werden existierende LoA-Standards, LoA-Normen o.ä. unter dem Begriff „LoA-Rahmenwerk“ subsumiert.

Wie bereits erläutert, soll ein Authentication-Assurance-Konzept für föderierte Infrastrukturen so minimal wie möglich hinsichtlich der darin definierten Kriterien gehalten sein. Aus diesem Grund ist die folgende Anforderung zu berücksichtigen:

> [NFA_LoA_Minimalität]: Ein entsprechendes Authentication-Assurance-Konzept soll einen leichtgewichtigen Ansatz verfolgen und der Fokus der Kriterien auf Kernanforderungen gerichtet sein. Als Kernanforderungen werden jene Anforderungen erachtet, die Authentifizierungen direkt adressieren. Nicht essentielle Kriterien, die nicht unmittelbar im Zusammenhang mit durchgeführten Authentifizierungen stehen, wie bspw. Kriterien zu Audit- und Awarenessprogrammen, werden daher als vernachlässigbar erachtet. Diese können im Rahmen eines spezifischeren Trust Frameworks, welches z.B. den Kontext und legale Aspekte regelt, definiert werden. Darüber hinaus sollen Kernanforderungen nicht zu strikt definiert sein und einen Umsetzungsspielraum gewähren, um Konflikte mit organisations-/föderationsspezifischen Anforderungen zu vermeiden.

Neben der Minimalität stellt eine weitere Anforderung die Modularität bzw. die Verwendung eines orthogonalen Ansatzes dar, sodass die jeweiligen Assurance-Komponenten individuell behauptbar sind. Orthogonale Komponenten sind dabei gemäß [RJ18] gegeben, wenn eine größtmögliche Überlappungsfreiheit der Komponenten gewährleistet ist. Hierzu zählt bspw. die Überlappungsfreiheit von Anforderungen der Authentication Assurance mit der Identity Assurance und aber auch von Anforderungen untereinander.

> [NFA_LoA_Modularität]: Um verschiedene Anwendungsfälle abzudecken, soll ein modularer bzw. orthogonaler Ansatz verfolgt werden, sodass die Komponenten der Authentication Assurance unabhängig von der Identity Assurance behauptet werden können.

Darüber hinaus stellt ein grundlegendes Ziel die Protokoll-Kompatibilität dar:

> [FA_LoA_Protokollkompatibilität]: Ein Authentication-Assurance-Konzept muss mit aktuellen Protokollen des föderierten Identitätsmanagements kommunizierbar sein.

Ferner ist ein Authentication-Assurance-Konzept unabhängig von nationalen Gegebenheiten erforderlich, damit dieses (föderations-) übergreifend und universell anwendbar ist. Zwar wird bspw. innerhalb einer EU-Verordnung die elektronische Identifizierung sowie Vertrauensdienste geregelt (vgl. *Electronic Identification, Authentication and Trust Services* [Eur14], kurz: eIDAS, siehe Abschnitt 3.6.1.3), jedoch wird dieses kaum Anwendung in Ländern bzw. nationalen Identitätsföderationen außerhalb der EU finden.

> [NFA_LoA_Unabhängigkeit]: Es wird ein Authentication-Assurance-Konzept unabhängig von nationalen Gegebenheiten bzw. Regulierungen benötigt.

In Bezug auf ein Authentication-Assurance-Konzept sind noch weitere, nicht-funktionale Anforderungen zu berücksichtigen, welche dann später auf Basis der Ergebnisse einer sogenannten *Community Consultation* (vgl. Abschnitt 6.2) überprüft werden. In [ZSL19] wurden hierzu bereits allgemeine Anforderungen an Assurance-Konzepte erarbeitet bzw. konkretisiert, die hier aufgegriffen werden:

[NFA_LoA_Umsetzbarkeit]: Da aufgrund des föderierten, autonomen Charakters übergreifende Standards in R&E nicht zwingend durchgesetzt werden können, muss ein Assurance-Konzept derart entworfen sein (vgl. v.a. [NFA_LoA_Minimalität]), dass es von einem Großteil der Organisationen leicht annehmbar ist.

[NFA_LoA_Implementierbarkeit]: Da Organisationen oft auf Standardsoftware zurückgreifen, muss die Implementierung des Assurance-Konzepts auch mit Standard-Software zur Benutzerdatenverwaltung möglich sein (Out-of-the-box).

[NFA_LoA_Verständlichkeit]: Anforderungen eines Assurance-Konzepts müssen auch für Personen einer Organisation ohne dediziertes Security-Fachwissen verständlich formuliert und umsetzbar sein.

[NFA_LoA_Eigenständigkeit]: Sofern möglich, sollen Anforderungen eines Assurance-Konzepts nicht auf weitere externe Referenzdokumente verweisen, da nicht davon ausgegangen werden kann, dass einer Organisation genügend Ressourcen und Fachwissen zur Verfügung stehen (vgl. Anforderung [NFA_LoA_Verständlichkeit]).

2.6.3 Top-Down Analyse zu Hauptanforderung RM

In Bezug auf die Hauptanforderung RM konnten keine konkreten Sub-Anforderungen im Projektkontext identifiziert werden, da der Fokus hier auf der *Unterstützung* und *Hilfestellung* bzw. *Empfehlung* hinsichtlich der Auswahl eines angemessenen Authentication-Assurance-Profils unter Verwendung eines risikobasierten Ansatzes liegt. Eine Klassifikation der Hauptanforderung RM als Sub-Anforderung ist hier jedoch nicht möglich, da der Hauptanforderung RM in den Kapiteln 4 und 5 eine umfassende Modellierung und Spezifikation zugrunde liegt. Aus diesem Grund wird direkt zur Top-Down Analyse der Hauptanforderung WF übergegangen.

2.6.4 Top-Down Analyse zu Hauptanforderung WF

Ein Teilziel dieser Arbeit stellt die Konzeption eines in eine vollvermaschte Infrastruktur integrierbaren Fallback MFA-Workflows dar, sodass Nutzer, deren Heimatorganisation oder Föderation über keine Multi-Faktor-Authentifizierung verfügt, sich trotzdem unter Verwendung eines externen Zweitfaktorprüfers bei einem (inter-) föderierten Dienst authentifizieren können, der MFA erfordert. Während in proxy-basierten Szenarien ein geeigneter Fallback Workflow bzw. Lösungsansatz bereits vorhanden ist (vgl. Abschnitt 2.4), ist bspw. in Szenarien wie eduGAIN, wo nationale Identitätsföderationen eine Mischung aus vollvermaschten als auch proxy-basierten Föderationsarchitekturen verfolgen, nicht existent. Eine Statistik [GÉ17b] zeigt auf, dass circa 80% der in eduGAIN teilnehmenden Föderationen eine vollvermaschte Architektur verfolgen, weswegen ein integrierbarer MFA-Workflow auch für vollvermaschte Szenarien dringend erforderlich ist. Die Interföderation eduGAIN (auch: *Umbrella-Föderation*) verfolgt dabei selbst ein vollvermaschtes Prinzip.

Auf Basis der hier definierten Anforderungen werden an späterer Stelle vorhandene Lösungsansätze hinsichtlich deren Eignung überprüft und analysiert inwiefern alternative Ansätze erforderlich sind, da zum Zeitpunkt der Recherche noch kein ausgereiftes Konzept für vollvermaschte Szenarien existiert.

Einen maßgeblichen Aspekt des Fallback MFA-Workflows stellt in diesem Zusammenhang die Integrierbarkeit in vorhandene Infrastrukturen dar. Da Föderationen, wie oben beschrieben, auf unterschiedlichen AAI-Architekturen basieren (vgl. Abbildung 2.3 und Abschnitt 3.2.4), ist ein Workflow erforderlich, der mit den verschiedenen Architekturmustern kompatibel ist.

Es ergibt sich die folgende Anforderung:

> [NFA_Integrierbarkeit]: Ein Fallback MFA-Workflow muss mit verschiedenen Föderationsarchitekturen kompatibel sein und soll keine Änderungen an der zugrundeliegenden Föderationsarchitektur erfordern.

Ferner ist zu berücksichtigen, dass Föderationen oder Organisationen z.T. bereits selbst eigene MFA-Lösungen implementieren.

> [FA_Koexistenz]: Individuelle MFA-Lösungen müssen dennoch nutzbar bleiben. MFA unter Verwendung eines Fallback MFA-Workflows, d.h. unter Verwendung eines externen Faktorprüfers, darf den Nachrichtenfluss vorhandener Implementierungen nicht stören.

Ein weiterer Aspekt stellt die Realisierung innerhalb der technischen Infrastruktur dar. Da ein Großteil der Föderationsbetreiber und -mitglieder auf Standardsoftware zurückgreifen, muss ein entsprechender Fallback MFA-Workflow auch von Standardsoftware unterstützt bzw. diese entsprechend erweitert werden können. Andernfalls würde dies einen tiefgehenden Eingriff erfordern, was die Wahrscheinlichkeit der Akzeptanz eines derartigen MFA-Workflows erheblich reduzieren würde.

> [NFA_Realisierbarkeit]: Der Lösungsansatz ist mit Standard-Software implementierbar oder diese kann entsprechend erweitert werden.

Darüber hinaus sind Anforderungen an die Skalierbarkeit und Unabhängigkeit zu berücksichtigen:

> [NFA_Skalierbarkeit]: Ein Lösungsansatz soll skalierbar und folglich auf verschiedenen Ebenen (d.h. Föderations-, Interföderations-Ebene) implementierbar sein.
>
> [NFA_Unabhängigkeit]: Ein Fallback MFA-Workflow unter Verwendung eines externen Faktorprüfers darf nicht für einen spezifischen IDP bzw. SP maßgeschneidert sein, sondern soll allgemein anwendbar sein. Es ist zu vermeiden, dass Benutzer pro Dienst einen dedizierten Zweitfaktor registrieren müssen.

Ferner ist aus Sicht von Infrastrukturbetreibern ein Mechanismus zur Messbarkeit und Statistik wünschenswert.

> [FA_Messbarkeit]: Anhand der im MFA-Workflow eingesetzten Mechanismen können Statistiken erzeugt werden. Es soll hervorgehen, welche IDPs MFA unterstützen

und welche nicht als auch, ob MFA bei einer Benutzerauthentifizierung stattgefunden hat oder nicht.

Speziell aus Sicht der Organisationen, d.h. seitens der teilnehmenden Identity Provider und Service Provider, sind ebenfalls Anforderungen zu berücksichtigen:

> [NFA_Einrichtungsauswand]: Identity Provider sollen durch einen entsprechenden Fallback MFA-Workflow mit externem Faktorprüfer entlastet werden. D.h. selbst ein Ansatz in Form eines as-a-Service Angebots soll kaum IDP-seitige Anpassungen erfordern. Da MFA zum Schutz der zugreifbaren Dienste eines Service Providers dient, kann hier ein moderater Einrichtungsaufwand, insbesondere hinsichtlich (initialer) Konfiguration, erwartet werden.

In [AAR18], in dem u.a. Anforderungen für MFA in einer proxy-basierten Architektur aufgelistet sind, zählt ebenfalls ein konformes Verhalten zu den Anforderungen:

> [FA_Konformität]: Ein externer Faktorprüfer soll sich aus der technischen Sicht eines SPs wie ein IDP verhalten.

Aus Perspektive der Nutzer soll diesen die Möglichkeit zur Verfügung stehen mehrere bzw. unterschiedliche Zweitfaktoren bei prinzipiell beliebig vielen Faktorprüfern registrieren zu können. Es reicht nicht aus, nur eine Realisierung eines zweiten Faktors bereitzustellen, da in der Organisation eines Nutzers spezielle Richtlinien vorhanden sein können. Z.B. könnte eine Richtlinie die Verwendung von USB-Schnittstellen unterbinden, sodass jegliche Zweitfaktoren, die via USB angeboten werden, für die Nutzer der entsprechenden Organisation u.U. nicht anwendbar wären.

> [FA_Dynamik]: Nutzer sollen die Möglichkeit besitzen, verschiedene (potentiell unterschiedlich starke) Zweitfaktoren bei prinzipiell beliebig vielen Faktorprüfern zu registrieren. Ferner soll ein Nutzer pro Dienst, der MFA erfordert, flexibel entscheiden können, welchen Zweitfaktor (-Prüfer) er für den Dienst nutzen möchte. Um dies zu gewährleisten, ist ein dynamischer Workflow gegenüber einem statischen Workflow zu bevorzugen.

Die zuvor genannte Fähigkeit dient zugleich auch als Fallback-Mechanismus, im Falle, dass einer der Faktorprüfer ausgefallen ist. Ferner können damit auch fortgeschrittenere Anwendungsfälle abgedeckt werden, sodass bspw. je nach gefordertem Assurance Level eine passende Kombination von Faktoren ausgewählt werden kann.

Zur Unterstützung der Benutzererfahrung sollten folgende Anforderungen berücksichtigt werden:

> [FA_Benutzbarkeit]: Ein MFA-Workflow baut auf vorhandenen Konzepten auf, um die Erwartbarkeit zu unterstützen und um eine intuitive Benutzererfahrung zu ermöglichen.
>
> [FA_Fehlerbehandlung]: Fehlermeldungen sollen verbessert werden, indem ein potentielles Scheitern einer Multi-Faktor-Authentifizierung aufgrund fehlender weiterer Faktoren frühzeitig kommuniziert wird.

Neben den bisher identifizierten funktionalen und nicht-funktionalen Anforderungen, sind Anforderungen zur Sicherheit des Lösungsansatzes bzw. Workflows zu berücksichtigen.

Multi-Faktor-Authentifizierungen zeichnen sich grundsätzlich dadurch aus, dass die Faktoren *unterschiedlichen Typs* sind. Im Allgemeinen ist hier die Unterscheidung zwischen *something you know*, *something you have* und *something you are* bekannt [GGF17b] (vgl. Abschnitt 3.4.1). D.h. es darf nicht möglich sein bspw. zwei verschiedene Passwörter für eine Multi-Faktor-Authentifizierung zu verwenden, da diese desselben Faktortyps entstammen. Es müssen immer zwei Faktoren *unterschiedlichen Typs* verwendet werden.

> [SIA_Faktorprüfung]: Es kann nicht davon ausgegangen werden, dass der erste verwendete Faktor stets eine Benutzername-Passwort-Kombination ist. Daher ist sicherzustellen, dass die Faktoren einer Multi-Faktor-Authentifizierung stets unterschiedlich sind, z.B. durch Implementieren einer Logik.
>
> [SIA_Vertraulichkeit]: Die Übertragung von Authentifizierungsinformation ist vor unautorisierter Offenlegung zu schützen.

Und letztlich, da durch einen MFA-Workflow unter Verwendung eines externen Faktorprüfers Informationen über Benutzer und deren Authentifizierungen verarbeitet werden, ist der Schutz personenbezogener Daten zu berücksichtigen:

> [DSA_Datenminimalisierung]: Bei der Benutzerauthentifizierung durch einen externen Faktorprüfer sollen so wenig personenbezogene Daten wie möglich gespeichert und verarbeitet werden.

2.6.5 Top-Down Analyse der Hauptanforderung UM

Zuletzt findet eine Top-Down Analyse der Hauptanforderung UM statt, die sich mit einem Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien befasst.

Bevor eine existierende Ein-Faktor AAI um Konzepte zur Authentifizierung (bspw. MFA) erweitert wird, sollten zunächst die vorhandenen Entitäten, Rollen, Dienste sowie deren Beziehungen und Abhängigkeiten identifiziert und abgebildet werden. Eine Herausforderung, die in föderierten Szenarien existiert, ist, dass eine Vielzahl unterschiedlicher Protokolle, Technologien, Rahmenwerke und Standards zum Einsatz kommen, die eng miteinander verflochten sind und dadurch eine unabhängige Beschreibung und Modellierung der vorhandenen Infrastruktur erschweren. Hinzu kommt, dass mit der Entstehung neuer Protokolle und Technologien auch neue *Terminologien* entstehen, die zum Teil parallel, zum Teil vermischt angewendet werden. Die Abgrenzung und das allgemeine Verständnis zwischen involvierten Entitäten und Rollen, Services, technischen Komponenten und deren Abhängigkeiten ist dadurch erschwert. Bevor also neue Komponenten in eine vorhandene, verteilte und heterogene Infrastruktur eingeführt werden, ist ein ganzheitliches Verständnis des Authentifizierungsszenarios sehr vorteilhaft. Abbildung 2.9 verdeutlicht dazu anhand drei exemplarischer Sichten (farbige Linien), in welchen Anwendungsfällen, neben der initialen Designphase, ein derartiges Modell noch hilfreich sein kann.

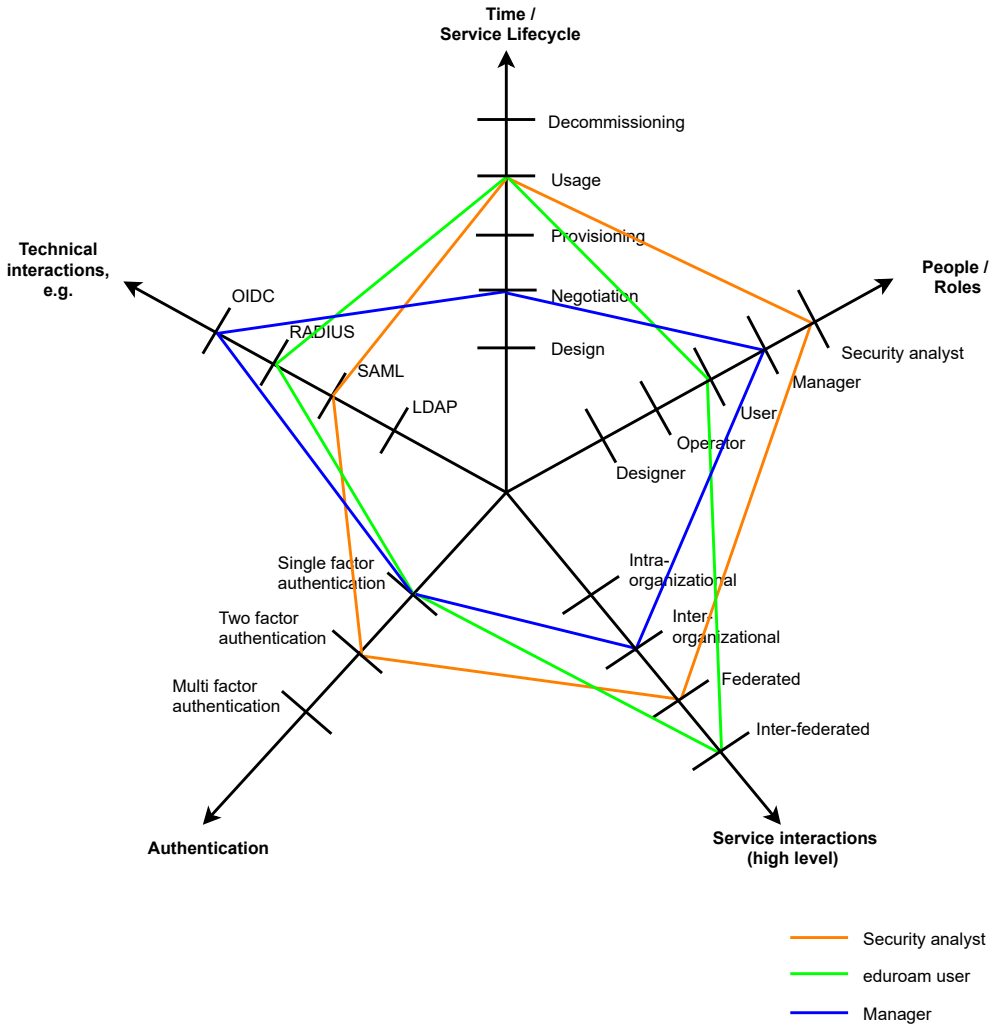


Abbildung 2.9: Exemplarische Sichten innerhalb von Authentifizierungsszenarien

Die orange-farbige Linie repräsentiert z.B. die Rolle eines Security Analysten, der bei einer Zwei-Faktor-Implementierung in einer SAML-basierten Föderation nach Schwachstellen sucht. Die grüne Linie visualisiert die Nutzungsphase der eduroam-Infrastruktur [GÉ20a] bei der sich ein Nutzer auf Basis von RADIUS [RRWS00] mit seinem Benutzername und Passwort authentifiziert, während die blaue Linie die Sicht eines Managers darstellt, der einen Vertrag für eine OIDC-basierte Ein-Faktor-Lösung mit einem externen Supplier aushandelt.

Um eine *vollständige* und *vergleichbare* Beschreibung für Authentifizierungsszenarien zu erzielen, wurden daher in [ZS18] Anforderungen erarbeitet, die an dieser Stelle referenziert werden. Vergleichbarkeit wird durch eine uniforme Terminologie erreicht, wohingegen Vollständigkeit durch eine ganzheitliche Beschreibung in einer Service (Lebenszyklus) orientierten Art und Weise erreicht wird [ZS18]:

[FA_Terminologie]: Zur Vergleichbarkeit sowie für ein besseres Verständnis soll ein entsprechendes Modell eine universelle und uniform anwendbare Terminologie und Rollenbeschreibung - unabhängig von zugrundeliegenden Protokollen, Standards, Technologien und Rahmenwerken - bereitstellen.

[FA_Service_Orientierung]: Authentifizierungsszenarien sollen auf eine Service (Lebenszyklus) orientierte Art und Weise abbildbar sein und verschiedene Sichten auf Services (z.B. Realisierungssicht) ermöglichen.

Darüber hinaus soll ein entsprechendes Modell verschiedene Funktionalitäten eines Authentifizierungsszenarios berücksichtigen und abbilden. Dazu zählen im Besonderen *Managementfunktionalitäten* sowie *Nutzungsfunktionalitäten* eines Dienstes. Als Managementfunktionalitäten werden im Allgemeinen Funktionen zum Management eines Dienstes durch den Kunden bezeichnet. In Bezug auf Authentifizierungsszenarien und MFA zählt dazu bspw. das Trust Management oder die Zweitfaktorbindung (bspw. unter Zuhilfenahme von Service Requests). Als Nutzungsaspekte werden im Allgemeinen Interaktionen durch den Nutzer bezeichnet, was im Fall von Authentifizierungen bspw. die Eingabe von Benutzername und Passwort auf der grafischen Benutzeroberfläche sein kann. [ZS18]

Gemäß [ZS18] sind die folgenden zwei Anforderungen ebenfalls von Relevanz:

[FA_Managementaspekte]: Berücksichtigung von Managementaspekten in Authentifizierungsszenarien.

[FA_Nutzungsaspekte]: Berücksichtigung von Aspekten hinsichtlich der Nutzung in Authentifizierungsszenarien (*engl. usage*).

Weitere, gemäß [ZS18] wichtige Kriterien sind:

[FA_Rekursion]: Um verschachtelte Hierarchien in Authentifizierungsszenarien abbilden zu können (bspw. MFA), muss ein entsprechendes Modell rekursionsfähig sein.

[FA_Schablonen]: Da Authentifizierungen oftmals bestimmten Mustern genügen, sollen szenario-unabhängige Templates für Authentifizierungen zur Verfügung gestellt werden.

Eine vollständige und vergleichbare Beschreibung eines existierenden Authentifizierungsszenarios mit Hilfe eines spezifizierten Konzepts dient somit einerseits als Hilfestellung, bevor neue Authentifizierungskomponenten in eine existierende Infrastruktur integriert werden. Es ist aber auch, wie oben in Abbildung 2.9 exemplarisch aufgezeigt, in weiteren Phasen abseits der Design-/Konzeptphase, z.B. in der Nutzungsphase für Security-Analysen, zweckdienlich.

2.7 Gewichtung der Anforderungen

Nach der Identifikation der Anforderungen werden alle Anforderungen einer Gewichtung gemäß den drei Stufen *essentiell*, *wichtig* und *wünschenswert* unterzogen. Die Gewichtung dient primär dazu, die Relevanz zur Erfüllung einer spezifischen Anforderung zu definieren,

sodass essentielle Anforderungen gegenüber wünschenswerten Anforderungen stärker priorisiert werden. Im Anschluss werden alle Anforderungen inklusive deren Gewichtung in einen integrierten Anforderungskatalog aufgenommen, der in Abschnitt 2.8 dargestellt ist.

Das Gewichtungsschema greift auf ein einfaches, intuitives, dreistufiges Modell zurück. Jedes Gewicht wird dabei zusätzlich mit einem Zahlenwert, der als Multiplikator dient, versehen (vgl. Tabelle 2.1).

Tabelle 2.1: Gewichtungsschema der Anforderungen

Gewichtung	**Multiplikator**
essentiell	4
wichtig	2
wünschenswert	1

In den folgenden Abschnitten 2.7.1 bis 2.7.4 werden die den Hauptanforderungen untergeordneten Sub-Anforderungen erneut aufgegriffen und gegen das in Tabelle 2.1 definierte Gewichtungsschema abgewägt.

2.7.1 Gewichtung der Sub-Anforderungen der Hauptanforderung AK

In der folgenden Tabelle 2.2 werden zunächst die Anforderungen an das Authentication-Assurance-Konzept priorisiert:

Tabelle 2.2: Gewichtete Anforderungen an das Authentication-Assurance-Konzept

Anforderung	**Gewichtung**	**Kurzbeschreibung und Begründung**
[FA_LoA_1FA]	**(2)**	**Zusammenfassung:** Kriterien zur Qualität von Ein-Faktor-Authentifizierungen
Begründung: Um ein gemeinsames, übergreifendes Verständnis zur Qualität durchgeführter Authentifizierungen zu etablieren, müssen sowohl Authentifizierungen mit einem als auch mit mehreren Faktoren berücksichtigt werden. Die Anforderung wird daher als *wichtig* klassifiziert.		
[FA_LoA_MFA]	**(2)**	**Zusammenfassung:** Kriterien zur Qualität von Multi-Faktor-Authentifizierungen
Begründung: Analog zu vorheriger Anforderung und Argumentation wird auch diese Anforderung als *wichtig* priorisiert.		
[NFA_LoA_Minimalität]	**(4)**	**Zusammenfassung:** Fokus auf Kernanforderungen mit Umsetzungsspielraum

Begründung: Da in föderierten Szenarien (organisations-/föderations-) spezifische Richtlinien und Maßnahmen bereits häufig existieren, sind minimale Anforderungen, sowohl hinsichtlich des Mindest-Erfüllungsgrades als auch der Quantität *essentiell*.

[NFA_LoA_Modularität] **(4)** **Zusammenfassung:** Verwendung eines modularen bzw. orthogonalen Ansatzes

Begründung: Die Anforderung wird als *essentiell* bewertet, da je nach Szenario und Kritikalität unterschiedliche Anwendungsfälle abzudecken sind.

[FA_LoA_Protokoll-kompatibilität] **(2)** **Zusammenfassung:** Kompatibilität mit FIM-Protokollen

Begründung: Es ist *wichtig*, dass ein Authentication-Assurance-Konzept mit FIM-Protokollen kommunizierbar ist, da das Authentication-Assurance-Konzept andernfalls für föderierte Szenarien wertlos ist.

[NFA_LoA_Unabhängigkeit] **(2)** **Zusammenfassung:** Unabhängigkeit von nationalen Gegebenheiten bzw. Regulierungen

Begründung: Es ist ebenfalls *wichtig*, dass ein Authentication-Assurance-Konzept unabhängig von nationalen Gegebenheiten konzeptioniert wird, um den Ausschluss von Teilnehmern zu vermeiden.

[NFA_LoA_Umsetzbarkeit] **(4)** **Zusammenfassung:** Sicherstellung der leichten Umsetzbarkeit durch einen Großteil der Organisationen

Begründung: Da der Umsetzbarkeit die Notwendigkeit eines leichtgewichtigen Ansatzes zugrunde liegt, d.h. Fokus auf Kernkriterien und deren Umsetzungsspielraum (vgl. Anforderung [NFA_LoA_Minimalität]), erhält diese Anforderung daher dieselbe Priorität.

[NFA_LoA_Implementierbarkeit] **(2)** **Zusammenfassung:** Standardsoftware unterstützt die Implementierung des Authentication-Assurance-Konzepts

Begründung: Ist mit Standardsoftware das entsprechende Konzept nicht implementierbar oder sind weitreichende Änderungen erforderlich, senkt dies die Annahme seitens der Teilnehmer. Die Anforderung wird daher als *wichtig* gewichtet.

[NFA_LoA_Verständlichkeit] **(2)** **Zusammenfassung:** Sicherstellung der Verständlichkeit für Personen ohne dediziertes Security-Fachwissen

Begründung: Diese Anforderung ist *wichtig*, da nicht davon ausgegangen werden kann, dass den Organisationen genügend Ressourcen zur Verfügung stehen.

[NFA_LoA_Eigenständigkeit]	**(1)**	**Zusammenfassung:** Verzicht auf Referenzdokumente

Begründung: Diese Anforderung wird als *wünschenswert* priorisiert, um die Verständlichkeit zu erhöhen und um Problemen hinsichtlich der Versionierung entgegnen zu können.

2.7.2 Gewichtung der Sub-Anforderungen der Hauptanforderung RM

Da der Hauptanforderung RM aufgrund ihres unterstützenden Charakters keine spezifischen Sub-Anforderungen zugeordnet wurden, kann direkt zur Gewichtung der Sub-Anforderungen der Hauptanforderung WF übergegangen werden.

2.7.3 Gewichtung der Sub-Anforderungen der Hauptanforderung WF

In Tabelle 2.3 sind die Anforderungen an einen Fallback MFA-Workflow aggregiert gesammelt und einer Gewichtung unterzogen:

Tabelle 2.3: Gewichtete Anforderungen an den/einen Fallback MFA-Workflow

Anforderung	**Gewichtung**	**Kurzbeschreibung und Begründung**
[NFA_Integrierbarkeit]	**(4)**	**Zusammenfassung:** Sicherstellung der Kompatibilität mit verschiedenen Föderationsarchitekturen ohne grundlegende Änderungen

Begründung: Die Kompatibilität mit verschiedenen Architekturmustern ohne grundlegende Änderungen stellt eine elementare Anforderung dar und wird daher als *essentiell* bewertet.

[FA_Koexistenz]	**(4)**	**Zusammenfassung:** Sicherstellung der Nutzbarkeit vorhandener, individueller MFA-Lösungen

Begründung: Das Vorhandensein einer beliebigen MFA-Implementierung auf Identity Provider Seite gilt nach wie vor als Idealzustand und muss daher auf jeden Fall unterstützt werden, weswegen die Anforderung als *essentiell* bewertet wird.

[NFA_Realisierbarkeit]	**(2)**	**Zusammenfassung:** Nutzbarkeit des Lösungsansatzes mit Standard-Software

Begründung: Da nicht garantiert werden kann, dass jedes (proprietäre) Software-Produkt unterstützt wird, sollten zumindest Standard-Softwareprodukte (vgl. Abschnitt 3.2.3) unterstützt werden. Ist das nicht der Fall, schränkt dies die Annahme seitens der Teilnehmer deutlich ein. Die Anforderung wird daher als *wichtig* priorisiert.

[NFA_Skalierbarkeit] **(2)** **Zusammenfassung:** Sicherstellung der Skalierbarkeit auf verschiedenen Ebenen (d.h. Föderations-, Interföderationsebene)
Begründung: Die Anforderung ist *wichtig*, um verschiedene Anwendungsfälle abdecken zu können.

[NFA_Unabhängigkeit] **(2)** **Zusammenfassung:** Sicherstellung der allgemeinen Anwendbarkeit für sowohl Identity Provider als auch Service Provider
Begründung: Ein Lösungsansatz unter Verwendung eines externen Faktorprüfers darf nicht für dedizierte, exklusive Entitäten entworfen sein, sondern dient der allgemeinen Masse. Die Anforderung ist daher *wichtig*.

[FA_Messbarkeit] **(1)** **Zusammenfassung:** Statistiken über MFA-fähige IDPs und durchgeführte Multi-Faktor-Authentifizierungen
Begründung: Diese Anforderung wird als *wünschenswert* priorisiert, da die Möglichkeit zur Messbarkeit und Statistik hier zu rein informativen Zwecken dient.

[NFA_Einrichtungsaufwand] **(4)** **Zusammenfassung:** Entlastung im Besonderen der Identity Provider durch Bereitstellung eines Fallback MFA-Workflows
Begründung: Die bestmögliche Entlastung der Identity Provider und Service Provider ist ein zentrales Ziel dieser Arbeit und wird daher als *essentiell* eingestuft.

[FA_Konformität] **(1)** **Zusammenfassung:** Konformes Verhalten des externen Faktorprüfers
Begründung: Konformes Verhalten trägt zu einem besseren Verständnis der involvierten MFA-Komponenten in eine Infrastruktur bei und wird daher als *wünschenswert* klassifiziert.

[FA_Dynamik] **(2)** **Zusammenfassung:** Flexibilität hinsichtlich der Auswahl und Nutzung von Zweitfaktoren bzw. Zweitfaktorprüfern
Begründung: Diese Anforderung wird als *wichtig* priorisiert, um Nutzern größtmögliche Flexibilität zu gewährleisten.

[FA_Benutzbarkeit] **(2)** **Zusammenfassung:** Unterstützung der Erwartbarkeit und einer intuitiven Benutzererfahrung

Begründung: Die Perspektive der Nutzer hinsichtlich der Benutzbarkeit ist ebenfalls zu berücksichtigen, weswegen die Anforderung als *wichtig* bewertet wird.

[FA_Fehlerbehandlung] **(1)** **Zusammenfassung:** Frühzeitige Fehlermeldungen

Begründung: Diese Anforderung wird als *wünschenswert* bewertet, um einen Benutzer frühzeitig hinsichtlich des Status seines Authentifizierungsprozesses zu informieren.

[SIA_Faktorprüfung] **(2)** **Zusammenfassung:** Überprüfen der Gültigkeit einer Multi-Faktor-Authentifizierung

Begründung: Um eine Multi-Faktor-Authentifizierung in Konformität zu den gängigen Definitionen hinsichtlich der Verwendung unterschiedlicher Faktortypen zu gewährleisten, muss an geeigneter Stelle überprüft werden, ob die bei einer Authentifizierung verwendeten Faktoren auch tatsächlich unterschiedlichen Typs sind. Die Anforderung wird somit als *wichtig* bewertet.

[SIA_Vertraulichkeit] **(2)** **Zusammenfassung:** Schutz vor Modifikation von Authentifizierung-informationen

Begründung: Diese Anforderung wird aufgrund des schützenswerten Charakters der durch MFA-zugreifbaren Dienste ebenfalls als *wichtig* eingestuft.

[DSA_Datenminimalisierung] **(2)** **Zusammenfassung:** Sparsame Verarbeitung von personenbezogenen Daten

Begründung: Diese Anforderung wird aufgrund den, v.a. in der EU, vorherrschenden Gesetzen zum Datenschutz (vgl. DSGVO) als *wichtig* priorisiert.

2.7.4 Gewichtung der Sub-Anforderungen der Hauptanforderung UM

In diesem Abschnitt und der folgenden Tabelle 2.4 werden die Sub-Anforderungen der letzten Hauptanforderung, d.h. der Hauptanforderung UM, priorisiert:

Tabelle 2.4: Gewichtete Anforderungen an ein Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien

Anforderung	**Gewichtung**	**Kurzbeschreibung und Begründung**
[FA_Terminologie]	**(4)**	**Zusammenfassung:** Universelle und uniform anwendbare Terminologie und Rollenbeschreibung

Begründung: Diese Anforderung wird als *essentiell* erachtet, da ohne eine universelle und uniform anwendbare Terminologie eine Vergleichbarkeit nicht garantiert werden kann. Darüber hinaus trägt sie zu einem besseren, gemeinsamen Verständnis - unabhängig von Terminologien aus zugrundeliegenden Protokollen, Standards, Technologien und Rahmenwerken - bei.

[FA_Service_Orientierung] **(4)** **Zusammenfassung:** Prinzip der Serviceorientierung und Bereitstellung verschiedener Sichten

Begründung: Für ein ganzheitliches Verständnis eines Authentifizierungsszenarios müssen neben dem rein technischen Austausch von Authentifizierungsinformationen zwischen Softwarekomponenten (z.B. protokollbasiert) ebenfalls die Service Aspekte (z.B. Prozesse wie Incident Management oder Quality-of-Service-Parameter) berücksichtigt werden. Die Anforderung wird daher als *essentiell* priorisiert.

[FA_Management-aspekte] **(2)** **Zusammenfassung:** Berücksichtigung von Managementaspekten

Begründung: Diese Anforderung wird als *wichtig* priorisiert, da sie zur vollständigen Abbildung eines Authentifizierungsszenarios beiträgt.

[FA_Nutzungsaspekte] **(2)** **Zusammenfassung:** Berücksichtigung von Aspekten zur Nutzung

Begründung: Analog zu vorheriger Anforderung und Argumentation wird auch diese Anforderung als *wichtig* priorisiert.

[FA_Rekursion] **(4)** **Zusammenfassung:** Fähigkeit zur Rekursion für verschachtelte Modell-Hierarchien

Begründung: Die Anforderung dient dazu, eine Abbildbarkeit von komplexen Szenarien zu gewährleisten und ist aufgrund der vorhandenen Heterogenität und Diversität in föderierten Szenarien *essentiell*.

[FA_Schablonen] **(1)** **Zusammenfassung:** Notwendigkeit für szenario-unabhängige Templates

Begründung: Schablonen als Output des universellen Beschreibungsmodells werden als *wünschenswert* priorisiert.

2.8 Integrierter Anforderungskatalog

In der folgenden Tabelle 2.5 sind die vier Hauptanforderungen sowie die abgeleiteten Sub-Anforderungen nochmals übersichtlich und gewichtet dargestellt.

Tabelle 2.5: Integrierter Anforderungskatalog

Hauptanforderung AK: Authentication-Assurance-Konzept		
[NFA_LoA_Minimalität]	.....	(4)
[NFA_LoA_Modularität]	.....	(4)
[NFA_LoA_Umsetzbarkeit]	.....	(4)
[FA_LoA_1FA]	.....	(2)
[FA_LoA_MFA]	.....	(2)
[FA_LoA_Protokollkompatibilität]	.....	(2)
[NFA_LoA_Unabhängigkeit]	.....	(2)
[NFA_LoA_Implementierbarkeit]	.....	(2)
[NFA_LoA_Verständlichkeit]	.....	(2)
[NFA_LoA_Eigenständigkeit]	.....	(1)
Hauptanforderung RM: Konzept zur Auswahl eines angemessenen Authentication-Assurance-Profils		
ohne Sub-Anforderungen (vgl. Abschnitt 2.6.3)		
Hauptanforderung WF: Anforderungen an einen Fallback MFA-Workflow		
[NFA_Integrierbarkeit]	.....	(4)
[FA_Koexistenz]	.....	(4)
[NFA_Einrichtungsaufwand]	.....	(4)
[NFA_Realisierbarkeit]	.....	(2)
[NFA_Unabhängigkeit]	.....	(2)
[FA_Dynamik]	.....	(2)
[SIA_Faktorprüfung]	.....	(2)
[NFA_Skalierbarkeit]	.....	(2)
[FA_Benutzbarkeit]	.....	(2)
[DSA_Datenminimalisierung]	.....	(2)
[SIA_Vertraulichkeit]	.....	(2)
[FA_Messbarkeit]	.....	(1)
[FA_Fehlerbehandlung]	.....	(1)
[FA_Konformität]	.....	(1)
Hauptanforderung UM: Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien		
[FA_Terminologie]	.....	(4)
[FA_Service_Orientierung]	.....	(4)
[FA_Rekursion]	.....	(4)
[FA_Managementaspekte]	.....	(2)
[FA_Nutzungsaspekte]	.....	(2)
[FA_Schablonen]	.....	(1)

2.9 Zusammenfassung und Bewertung

Ziel dieses Kapitels war es, den Fokus dieser Arbeit durch Skizzierung des Problemraums einzugrenzen und darauf basierend Anforderungen abzuleiten. Es wurden mehrere Szenarien diskutiert, die gezeigt haben, dass die Problemstellung in verschiedenen Bereichen wie **nationalen Identitätsföderationen**, **Interföderationen**, **Forschungsinfrastrukturen** und **kommerziellen Szenarien** vorhanden ist und somit eine valide Forschungsfrage darstellt, die es zu lösen gilt. Da die Anforderungen aus R&E (vgl. Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen) im Vergleich zu den diskutierten Szenarien aus dem kommerziellen Sektor nicht ausreichend deckungsgleich sind, wurden ausschließlich auf Basis der Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen Anforderungen systematisch erarbeitet, klassifiziert und typisiert. Dazu wurden zunächst basierend auf den identifizierten Problemstellungen und Defiziten der Szenarien vier Hauptanforderungen abgeleitet, die dann durch eine Top-Down Analyse verfeinert wurden. Die vier Hauptanforderungen sind:

- Hauptanforderung AK: Definition eines leichtgewichtigen Authentication-Assurance-Konzepts zum Austausch der Qualität durchgeführter Authentifizierungen
- Hauptanforderung RM: Umsetzungsunterstützung für Service Provider zur Auswahl eines angemessenen Authentication-Assurance-Profils
- Hauptanforderung WF: Analyse existierender MFA-Realisierungsoptionen und Konzeption eines Fallback MFA-Workflows für vollvermaschte Authentifizierungsszenarien
- Hauptanforderung UM: Service-orientierte und ganzheitliche Beschreib- und Modellierbarkeit von Entitäten und Diensten eines Authentifizierungsszenarios unabhängig von zugrundeliegendem Protokoll, Standard, Technologie oder Framework

Die daraus resultierenden Sub-Anforderungen der vier Hauptanforderungen wurden dabei gemäß ihres Typs unterschieden:

- Funktionale Anforderungen (FA)
- Nicht-funktionale Anforderungen (NFA)
- Sicherheitsanforderungen (SIA)
- Datenschutzanforderungen (DSA)

Darüber hinaus wurden die Anforderungen gemäß eines dreistufigen Gewichtungsschemas (*essentiell*, *wichtig* und *wünschenswert*) priorisiert. Letztlich gibt ein integrierter Anforderungskatalog, der in Tabelle 2.5 dargestellt ist, einen Überblick über alle identifizierten Anforderungen.

Im folgenden Kapitel 3 werden die Grundlagen und der Status quo ausführlich erläutert. Wo sinnvoll, wird auf Subsets von Anforderungen zurückgegriffen, um bspw. vorhandene Konzepte hinsichtlich deren Eignung gegen die Anforderungen zu evaluieren.

Kapitel 3

Grundlagen und Status quo

Inhalt dieses Kapitels

Da das **Interföderierte Identitätsmanagement** auf den Konzepten des **Föderierten Identitätsmanagements** und des **Identity & Access Managements** aufsetzt, wird in den Abschnitten 3.1 und 3.2 zunächst ein grundlegender Überblick über die beiden Konzepte gegeben. Im Anschluss wird in Abschnitt 3.3 Inter-FIM selbst betrachtet.

Darauffolgend wird in den Abschnitten 3.4 bis 3.6 wird eine Einführung in die Grundlagen der Benutzerauthentifizierung, den Forschungsansätzen zur **Multi-Faktor-Authentifizierung** sowie der **Level of Assurance** gegeben.

Nach der Darlegung verschiedener **Informations- und Service-Managementmodelle** in Abschnitt 3.7 schließt das Kapitel mit einer Zusammenfassung in Abschnitt 3.10 ab.

3.1 Identity & Access Management

IAM bezeichnet den übergeordneten Begriff für Komponenten und Prozesse innerhalb einer Organisation, die sich mit der Verwaltung von Identitäten, deren Authentifizierung und Autorisierung beschäftigen. Für ein ganzheitliches Verständnis werden zunächst **digitale Identitäten** betrachtet sowie, darauf aufbauend, **föderierte Identitäten**.

3.1.1 Identitäten

Für die hier vorliegende Arbeit sind insbesondere die folgenden zwei Typen von Identitäten relevant:

- **Digitale Identität:** Wird gemäß der ISO/IEC 29115 [ISO13b] als eine Menge von Attributen, die an eine Entität gebunden sind, definiert. Dadurch lassen sich bspw. reale Personen oder auch Objekte auf digitaler Basis eindeutig und unterscheidbar identifizieren [Cha09]. Eine weitere Definition [Kim05] beschreibt die *Menge der Attribute* als eine *Menge von Behauptungen* (*engl. claims*), die von einem digitalen Subjekt über sich selbst oder über eine andere Entität gemacht wird. Dabei können identifizierende Attribute bzw. Behauptungen z.B. der (Benutzer-) Name, die E-Mail-Adresse oder eine Gruppenzugehörigkeit sein, es sind jedoch auch komplexere Attribute (z.B. *multi-valued*) denkbar.
- **Föderierte Identität:** Föderierte Identitäten bauen auf den Eigenschaften digitaler Identitäten auf. Sie zeichnen sich dadurch aus, dass ein Nutzer mit einer föderierten Identität auf eine Vielzahl von (externen) Diensten zugreifen kann, ohne für jeden Dienst eine neue Identität (i.S.v. Benutzeraccount) zu benötigen. Eine föderierte

Identität ist folglich eine aggregierte bzw. übergreifende Identität, die gemäß [LDA18] ein digitales Subjekt erzeugt, dessen Identitätsattribute aus potentiell mehreren Sicherheitsdomänen stammen können. Föderierte Identitäten greifen typischerweise auf einen Identity Provider zurück, der als eine Art *Identity Broker* [LDA18] agiert und die Benutzerauthentifizierung durchführt.

3.1.2 IAM Komponenten und Prozesse

Vor der Entstehung von IAM-Systemen wurden identitätsbezogene Daten und deren Berechtigungen üblicherweise innerhalb einer Organisation redundant an mehreren Stellen gepflegt. Sobald nun ein Datensatz aktualisiert werden musste, bspw. aufgrund einer Adressänderung eines Benutzers, mussten die Daten an sämtlichen Stellen aktualisiert werden. Wurden die Daten aber nur bei einigen, nicht aber bei allen Diensten aktualisiert, ergaben sich dadurch sehr schnell Inkonsistenzen in der Benutzerdatenhaltung. [Hom07]

Ein grundlegendes Ziel von IAM ist daher die Etablierung eines *zentralen Datenbestandes*, anhand dessen Identitätsdaten inklusive deren Zugriffsrechte konsistent und entkoppelt von Zielsystemen/-ressourcen gepflegt werden [Hom07]. Dies wird typischerweise unter Zuhilfenahme eines Verzeichnisdienstes, z.B. Lightweight Directory Access Protocol (LDAP)-basiert oder mithilfe eines relationalen Datenbankmanagementsystems (RDBMS), implementiert. Die Identitätsdaten werden dazu aus verschiedenen Quellsystemen, wie bspw. aus Verwaltungssystemen extrahiert und ggf. konsolidiert. Die Zielsysteme sind anhand von Schnittstellen an das IAM-System angeschlossen, das dienstübergreifend, aber domänenintern, sämtliche Identitätsdaten und deren Berechtigungen zur Authentifizierung und Autorisierung verwaltet. Ein derartiges IAM-System wurde z.B. im Rahmen des IntegraTUM Projektes [BB10] der Technischen Universität München in Zusammenarbeit mit dem Leibniz-Rechenzentrum campusübergreifend eingeführt.

Neben eines zentralen Datenbestandes und den dazu erläuterten IAM Komponenten und Schnittstellen sind auch *IAM-Prozesse* charakteristisch. Dazu zählen neben dem Vorhandensein organisatorischer (z.B. Person tritt in Organisation ein oder verlässt diese) und technischer Prozesse zum Umgang mit Identitäten auch die Prozesse der Authentifizierung und Autorisierung (z.B. Gewähren/Entziehen von Zugriffsrechten). [DFN10a]

Die Authentifizierung stellt dabei die Überprüfung der Echtheit einer Entität dar [Shi07] und wird aufgrund des thematischen Schwerpunkts dieser Arbeit ausführlich in Abschnitt 3.4 beleuchtet.

3.2 Föderiertes Identitätsmanagement

FIM greift auf das Konzept einer (Identitäts-) Föderation zurück und geht eine Stufe über das in Abschnitt 3.1 beschriebene, domäneninterne IAM hinaus.

Eine **Föderation** bezeichnet dabei eine Menge von Providern (speziell Identity Provider und Service Provider) und Benutzern [Int09], die zum Zwecke der gegenseitigen Dienstnut-

zung kollaborieren. Dadurch, dass die Benutzerverwaltung von dedizierten Identity Providern übernommen wird, ist die Benutzerverwaltung von den eigentlichen Dienstbetreibern entkoppelt, sodass den Benutzern ein organisationsübergreifender Zugriff auf Dienste ermöglicht wird. Somit kann ein Benutzer auch ohne vorheriges Importieren von Benutzerdaten einen Dienst außerhalb der eigenen Heimatorganisation nutzen.

Aus Realisierungssicht kommen dabei Protokolle wie die Security Assertion Markup Language (SAML) oder OpenID Connect (OIDC) zum Einsatz. Die beiden Protokolle werden in Abschnitt 3.2.2 genauer beschrieben.

FIM hat aus Perspektive der Usability den Vorteil, dass ein Nutzer nur eine föderierte Identität (vgl. Abschnitt 3.1.1) benötigt, mit der er/sie auf eine Vielzahl von Diensten, auch außerhalb seiner eigenen Organisation, zugreifen kann. Dies ermöglicht eine verbesserte User Experience aufgrund der Fähigkeit des **Single Sign On (SSO)** [Cha09]. SSO bzw. in deutsch Einmalanmeldung bedeutet in diesem Kontext, dass ein Nutzer nach einer erfolgten, einmaligen Authentifizierung auch auf weitere Dienste zugreifen kann, ohne sich bei diesen erneut reauthentifizieren zu müssen. Ferner geht FIM sparsam mit der Bereitstellung von Benutzerdaten an Dienstbetreiber um, da diese erst *on demand* dem Dienstbetreiber zur Verfügung gestellt werden.

Aus Sicht eines Dienstbetreibers kann dieser auf die Implementierung eines eigenen Identitätsmanagements verzichten, da das Management der Identitäten an die entsprechende Heimatorganisation des Benutzers delegiert wird. Durch FIM kann der Dienstbetreiber folglich einen größeren, potentiell unbekannten, Nutzerkreis bedienen.

Damit FIM funktioniert, muss zunächst im Rahmen eines übergreifenden Trust Managements Vertrauen zwischen den involvierten Teilnehmern etabliert werden. Auf organisatorischer Ebene findet dies u.a. durch (vertragliche) Vereinbarungen statt, während auf technischer Ebene das Vertrauen (insbesondere zur Sicherstellung der Authentizität und Integrität) u. a. durch kryptographische Mittel, wie Signaturen und Zertifikate, hergestellt wird.

Vertiefend zu den grundlegenden FIM-Konzepten werden in Abschnitt 3.2.1 die involvierten Rollen des föderierten Identitätsmanagements näher betrachtet. Darauffolgend werden in Abschnitt 3.2.2 FIM-Standards und darauf aufbauend Softwareprodukte (vgl. Abschnitt 3.2.3) sowie in Abschnitt 3.2.4 FIM-Architekturmodelle erläutert.

3.2.1 FIM-Rollenmodell

Im FIM-Umfeld sind drei grundlegende Rollen, d.h. zwei Provider-Rollen sowie die Rolle des Benutzers relevant, deren Zusammenhänge in Abbildung 3.1 darstellt sind. Die Rollenbezeichnung orientiert sich dabei meist am zugrundeliegenden Protokoll; hier exemplarisch anhand des Protokolls SAML:

- **Identity Provider (IDP):** Bezeichnet diejenige Entität bzw. Organisation, die eine Benutzerverwaltung betreibt und Authentifizierungsbestätigungen für ihre Nutzer ausstellt. Zur Weiterleitung dieser Information betreibt der Identity Provider i.d.R.

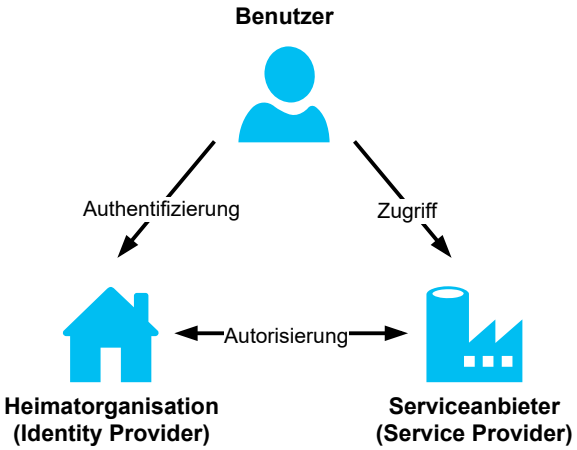


Abbildung 3.1: FIM Rollenmodell

eine technische Komponente, die analog zur Rolle bspw. als SAML Identity Provider (SAML IDP) bezeichnet wird. Je nach Architektur kann der Betrieb eines SAML IdP auch an eine andere Entität ausgelagert werden (vgl. *zentralisiert* versus *dezentralisiert* [Hom07] in Abschnitt 3.2.4). Der SAML IDP greift in einem derartigen Fall dann auf die Datenquelle (z.B. LDAP, Active Directory) des entsprechenden Identity Providers zurück. Im R&E Umfeld entspricht der Identity Provider üblicherweise der Heimatorganisation des Nutzers. Die Identität eines Nutzers wird dabei von genau einem Identity Provider verwaltet, da andernfalls Inkonsistenzen auftreten würden. Durch Forschungsansätze in Richtung eduID [DFN19, SUN21, SUR21a, SWI21a] soll im wissenschaftlichen Umfeld eine lebenslange ID (d.h. eine eduID) etabliert werden, die auch bei Wechsel der Organisation portabel ist.

- **Service Provider (SP):** Eine Entität bzw. Organisation wird als Service Provider bezeichnet, wenn sie der Föderation einen Dienst zur Verfügung stellt. Da ein SP im Rahmen von FIM selbst keine Benutzerverwaltung betreibt, vertraut ein SP den Aussagen der IDPs. Basierend auf den Aussagen des IDPs zur Identität des Nutzers und der durchgeführten Authentifizierung entscheidet ein SP über den Zugriff des Nutzers auf den Dienst. Auch hier ist eine technische Schnittstelle (z.B. SAML Service Provider (SAML SP)) zum Informationsaustausch notwendig.

- **Principal bzw. Nutzer:** Ein Nutzer besitzt i.d.R. eine föderierte Identität für deren Verwaltung seine Heimatorganisation (Identity Provider) zuständig ist. Dazu durchläuft der Nutzer üblicherweise einen Aufnahmeprozess (z.B. Immatrikulation an einer Universität) anhand dessen er identifiziert wird und eine eindeutige Kennung zugewiesen bekommt. Diese Kennung umfasst, abhängig von den individuellen Eigenschaften des Nutzers und seines Status, eine Reihe von identifizierenden Attributen. Diese dienen sowohl zur Zugriffsentscheidung, als auch als Voraussetzung bzw. Personalisierung zur eigentlichen Dienstnutzung.

Ferner gilt zu beachten, dass eine Entität bzw. Organisation potentiell die Rolle eines IDPs sowie eines oder mehrerer SPs einnehmen kann.

Da die FIM-Rollen üblicherweise analog zu den technischen Komponenten bezeichnet werden, ist aus dem Kontext nicht immer vollständig ableitbar, ob die organisatorische Rolle oder die technische Komponente gemeint ist. Aus diesem Grund werden im Rahmen dieser Arbeit technische Komponenten explizit mit dem entsprechenden Protokoll versehen, d.h. beispielsweise SAML IDP bzw. SAML SP oder analog bei OpenID Connect (vgl. Abschnitt 3.2.2.3) OIDC OP (OpenID Connect Provider) bzw. OIDC RP (OpenID Connect Relying Party).

3.2.2 FIM-Standards

Historisch betrachtet kamen mit **SAML 1.0** [PP01, OL01] und der mit Microsoft Passport[1] konkurrierenden **Liberty Identity Federation** [WE03] erste Standards zu Identitätsföderationen um die Jahrtausendwende auf den Markt. Durch die Entwicklung neuer Versionen und Erweiterungen näherten sich die beiden Spezifikationen zunehmend an, was schließlich in einer Zusammenführung der beiden Spezifikationen resultierte und die Basis für SAML 2.0 formte [Ora10].

In Abschnitt 3.2.2.1 wird daher ein Überblick über die **Security Assertion Markup Language 2.0** [CKPM05], die momentan intensiv in R&E Anwendung findet, gegeben, während in Abschnitt 3.2.2.3 ein weiterer, relativ junger FIM-Industriestandard, **OpenID Connect** [SBJ+14b], eine Erweiterung des Autorisierungsprotokoll **OAuth 2.0** [Har12], vorgestellt wird.

3.2.2.1 Security Assertion Markup Language (SAML)

SAML [CKPM05] ist ein XML-basiertes Framework des OASIS-Konsortiums (Organization for the Advancement of Structured Information Standards), entwickelt vom OASIS Security Service Technical Committee, zum Austausch von Attributs-, Authentifizierungs- und Autorisierungs-Informationen. Die erste Version, SAML 1.0, stammt aus dem Jahr 2002, die momentan aktuelle Version ist SAML 2.0 (2005).

Neben des Austausches genannter Informationen zwischen Benutzer (bzw. Browser), SAML IDP und SAML SP anhand von SAML Assertions, wird im Bereich der Forschung und Lehre SAML ebenfalls zur Etablierung des (technischen) Vertrauens zwischen den Entitäten eingesetzt. Dies geschieht anhand einer zentralen SAML-Metadatendatei, die von allen Teilnehmern regelmäßig aktualisiert werden muss. Daher werden in diesem Abschnitt zunächst die zum Verständnis notwendigen Grundlagen von SAML geschaffen.

Der original genehmigte Spezifikationssatz von SAML umfasst insgesamt acht Dokumente: Assertions and Protocols [CKPM05] (auch: SAML Core), Bindings [CHK+05], Profiles

[1] https://account.live.com/ – Microsoft Passwort stammt aus dem Jahr 1999 und wurde später in *Windows Live ID* umbenannt.

[HCH+05], Metadata [CMPM05], Authentication Context [KCM+05], Conformance Requirements [MPM05], Security and Privacy Considerations [HPM05a], Glossary [HPM05b]. In den ersten vier aufgelisteten Dokumenten werden die **Kernelemente von SAML** spezifiziert, die im Folgenden vorgestellt werden.

SAML Assertions

SAML Assertions sind „Behauptungen“ anhand derer eine Entität drei Arten von Aussagen (engl. *statements*) über ein Subjekt (z.B. einen Nutzer) machen kann [CKPM05]:

- *Authentication Statements* werden von der authentifizierenden Entität eines Subjektes erstellt und enthalten Aussagen u.a. über den (Miss-) Erfolg, den Zeitpunkt sowie die Art der Authentifizierung.
- *Attribute Statements* enthalten Attribute zur Identifikation eines Subjekts (z.B. Name, Adresse), die nicht zur eigentlichen Authentifizierungs- bzw. Autorisierungsbestätigung benötigt werden. Im Gegensatz zu den Authentication und Authorization Decision Statements, definieren die Attribute Statements keine Syntax und Semantik dieser Assertions, sodass sich die Absender- und Empfängerseite vorab auf ein gemeinsames Attributschema einigen müssen. [Hom07]
- *Authorization Decision Statements* geben eine positive oder negative Auskunft darüber, ob ein Subjekt die Berechtigung besitzt auf eine Ressource zuzugreifen.

SAML Protocols

Mittels *SAML Protocols* werden für sechs verschiedene Aktionen Request-Response Abläufe festgelegt, diese sind [RHP+08]:

- Das *Authentication Request Protocol* definiert, wie Assertions mit Authentication Statements und optional Attribute Statements von einer Entität zu einem Subjekt angefordert werden können.
- Das *Single Logout Protocol* dient zur nahezu gleichzeitigen Termination aller Sessions eines Benutzers, bspw. nach Timeout.
- Das *Assertion Query and Request Protocol* definiert eine Menge von Anfragen, um existierende Assertions anhand der Assertion ID abzufragen (Request) oder nach Assertions über Suchparamter zu suchen (Query).
- Das *Artifact Resolution Protocol* ermöglicht anhand von Referenzen SAML-Nachrichten zu versenden und diese aufzulösen.
- Das *Name Identifier Management Protocol* stellt Mechanismen zur Verfügung, um den Wert oder das Format eines Name Identifiers zu ändern.
- Das *Name Identifier Mapping Protocol* ermöglicht es, Identifier aufeinander abzubilden.

SAML Bindings

SAML Bindings definieren, welches Nachrichten- oder Kommunikationsprotokoll für SAML Request-/Response-Nachrichten verwendet wird. Protokollbindungen gemäß [CHK+05] sind: *SAML SOAP*, *Reverse SOAP (PAOS)*, *HTTP Redirect*, *HTTP POST*, *HTTP Artifact* und *SAML URI*. Ein HTTP Redirect Binding definiert also, wie eine SAML-Nachricht mit HTTP Redirects transportiert werden kann.

SAML Profiles

SAML Profiles beschreiben Kombinationsmöglichkeiten und deren Einschränkungen bei der Verwendung der zuvor beschriebenen SAML Assertions, SAML Protocols und SAML Bindings. Dadurch lassen sich verschiedene Use Cases gemäß Anwendungszweck passend abbilden. Insgesamt werden acht Profile definiert, deren Terminologie Analogien zu den SAML Protocols aufweisen [HCH+05, RHP+08]:

- Das *Web Browser SSO Profile* definiert, wie das Authentication Request Protocol, SAML Responses und Assertions in Kombination mit HTTP Redirect, HTTP POST und HTTP Artifact Binding verwendet werden, um SSO mit Webbrowsern zu implementieren.
- Das *Enhanced Client and Proxy (ECP) Profile* definiert ein spezielles SSO-Profil mit Reverse-SOAP and SOAP Bindings.
- Das *Identity Provider Discovery Profile* beschreibt einen Mechanismus für Service Provider, um herauszufinden, welche Identity Provider ein Nutzer zuvor besucht hat.
- Das *Single Logout Profile* zeigt die Verwendung des Single Logout Protocol zusammen mit SOAP, HTTP Redirect, HTTP POST und HHTP Artifact Binding auf.
- Das *Assertion Query/Request Profile* definiert die Verwendung des Assertion Query and Request Protocol mit synchronen SAML Bindings, wie bspw. SOAP.
- Das *Artifact Resolution Profile* legt fest, wie das Artifact Resolution Protocol mit synchronen SAML Bindings (z.B. SOAP) verwendet werden kann.
- Das *Name Identifier Management Profile* definiert wie das gleichnamige SAML-Protocol in Kombination mit den SAML Bindings SOAP, HTTP Redirect, HTTP POST und HTTP Artifact genutzt werden kann.
- Das *Name Identifier Mapping Profile* zeigt auf, wie das Name Identifier Mapping Protocol ein synchrones SAML Binding verwenden kann.

SAML Metadata

Metadaten [CMPM05] sind in SAML erforderlich, um die gemäß eines SAML Profiles benötigten Vereinbarungen und Informationen (Endpunkte, Schlüssel, Zertifikate etc.) auf eine standardisierte Art und Weise auszutauschen. Eine Metadaten-Datei beginnt dabei typischerweise mit einem <EntityDescriptor> bzw. <EntitiesDescriptors>, je nachdem wie

viele Entitäten in einer Metadaten-Datei enthalten sind [Pöh16]. Ein singulärer <EntityDescriptor> stellt somit ein Container-Element dar, um eine Entität unter Verwendung einer eindeutigen entityID zu beschreiben. Zur Verdeutlichung der SAML-Metadaten zeigt das Listing 3.1 exemplarisch die (aus Platzgründen stark gekürzten) Metadaten des LRZ-IDPs, der in der Interföderation eduGAIN registriert ist.

```
1  </EntityDescriptor>
2    <EntityDescriptor entityID="https://idp.lrz.de/idp/shibboleth">
3      <Extensions>
4        <mdrpi:RegistrationInfo registrationAuthority="https://www.aai.dfn.de"
       registrationInstant="2009-05-27T12:36:25Z">
5            ...
6        </mdrpi:RegistrationInfo>
7        <mdattr:EntityAttributes>
8          <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-
       certification" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri
       ">
9            <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
10         </saml:Attribute>
11         <saml:Attribute Name="http://macedir.org/entity-category-support"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
12           <saml:AttributeValue>http://www.geant.net/uri/dataprotection-code-of
       -conduct/v1</saml:AttributeValue>
13           <saml:AttributeValue>http://refeds.org/category/research-and-
       scholarship</saml:AttributeValue>
14         </saml:Attribute>
15         <saml:Attribute Name="http://aai.dfn.de/loa/degree-of-reliance"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
16           <saml:AttributeValue>advanced</saml:AttributeValue>
17         </saml:Attribute>
18       </mdattr:EntityAttributes>
19     </Extensions>
20     <IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0 urn:
       oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
21       <Extensions>
22         <saml1md:Scope regexp="false">lrz.de</saml1md:Scope>
23         <mdui:UIInfo>
24           <mdui:DisplayName xml:lang="de">Leibniz-Rechenzentrum (LRZ)</mdui:
       DisplayName>
25           <mdui:Description xml:lang="de">Identity Provider fuer Mitarbeiter
       des Leibniz-Rechenzentrums und der Bayerischen Akademie der Wissenschaften
       </mdui:Description>
26             ...
27         </mdui:UIInfo>
28       </Extensions>
29       <KeyDescriptor use="encryption">
30         <ds:KeyInfo>
31           <ds:KeyName>lrzidp.lrz.de</ds:KeyName>
32           <ds:X509Data>
33             ...
34           </ds:X509Data>
35         </ds:KeyInfo>
36       </KeyDescriptor>
```

```
37        <KeyDescriptor use="signing">
38          ...
39        </KeyDescriptor>
40        <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings
      :SOAP-binding" Location="https://idp.lrz.de:8443/idp/profile/SAML1/SOAP/
      ArtifactResolution" index="1"/>
41        ...
42        <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:
      AuthnRequest" Location="https://idp.lrz.de/idp/profile/Shibboleth/SSO"/>
43        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
      POST" Location="https://idp.lrz.de/idp/profile/SAML2/POST/SSO"/>
44        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
      Redirect" Location="https://idp.lrz.de/idp/profile/SAML2/Redirect/SSO"/>
45        ...
46      </IDPSSODescriptor>
47      ...
48      <Organization>
49        <OrganizationName xml:lang="de">e38</OrganizationName>
50        <OrganizationDisplayName xml:lang="de">Leibniz-Rechenzentrum der
      Bayerischen Akademie der Wissenschaften</OrganizationDisplayName>
51        <OrganizationURL xml:lang="de">http://www.lrz.de</OrganizationURL>
52        ...
53      </Organization>
54      <ContactPerson contactType="administrative">
55        ...
56      </ContactPerson>
57      <ContactPerson contactType="technical">
58        ...
59      </ContactPerson>
60      <ContactPerson contactType="support">
61        ...
62      </ContactPerson>
63      <ContactPerson contactType="other" remd:contactType="http://refeds.org/
      metadata/contactType/security">
64        <GivenName>LRZ Security Team</GivenName>
65        <EmailAddress>mailto:abuse@lrz.de</EmailAddress>
66      </ContactPerson>
67    </EntityDescriptor>
```

Listing 3.1: Exemplarischer Auszug der LRZ-IDP Metadaten (gekürzt) [GÉ21a]

Wie in Listing 3.1 ersichtlich, sind neben Schlüsselinformationen und Endpunkten eine Reihe zusätzlicher Informationen über eine Entität enthalten. Dazu zählt bspw. die Konformität zu einer der DFN-Verlässlichkeitsklassen „Degree of Reliance“ innerhalb des <mdattr:EntityAttributes> (ab Zeile 7), die besagt, dass das LRZ die Anforderungen der *advanced*-Klasse[2] (siehe Zeilen 15 bis 17) an die Assurance bzw. Verlässlichkeit erfüllt (vgl. auch DFN Verlässlichkeitsklassen in Abschnitt 3.6.2.1).

SAML-Metadaten stellen somit ein zentrales Konzept dar, um Vertrauen auf technischer Ebene in (Inter-) Föderationen zwischen den Entitäten zu vermitteln.

[2] D.h. persönliche Identifizierung, Ausweisen anhand personalisiertem Account, Datenkorrektheit und -aktualisierung innerhalb von 2 Wochen

In SAML-Föderationen werden die teilnehmenden Entitäten typischerweise in einer zentralen Metadatendatei registriert, deren Verwaltung i.d.R. der Föderationsbetreiber übernimmt. Im Fall von eduGAIN ist die Metadatenverwaltung an ein hierarchisches Modell gekoppelt (vgl. Abschnitt 3.3.1), sodass die Betreiber der nationalen Föderationen die Metadaten ihrer Teilnehmer aggregieren, während auf Interföderations-Ebene (d.h. eduGAIN) wiederum die jeweiligen nationalen Metadatensätze aggregiert werden.

SAML Authentifizierungs-Workflow

Nach der Darstellung der grundlegenden Konzepte von SAML wird in folgender Abbildung 3.2 der generelle Ablauf (in Form eines UML-Sequenzdiagramms) einer Ein-Faktor-Authentifizierung in SAML unter Verwendung des Web Browser SSO Profiles aufgezeigt. Da die jeweiligen Schritte bereits textuell in Abschnitt 2.2 erläutert wurden (siehe Seiten 18 und 19), wird an dieser Stelle auf eine erneute textuelle Auflistung verzichtet.

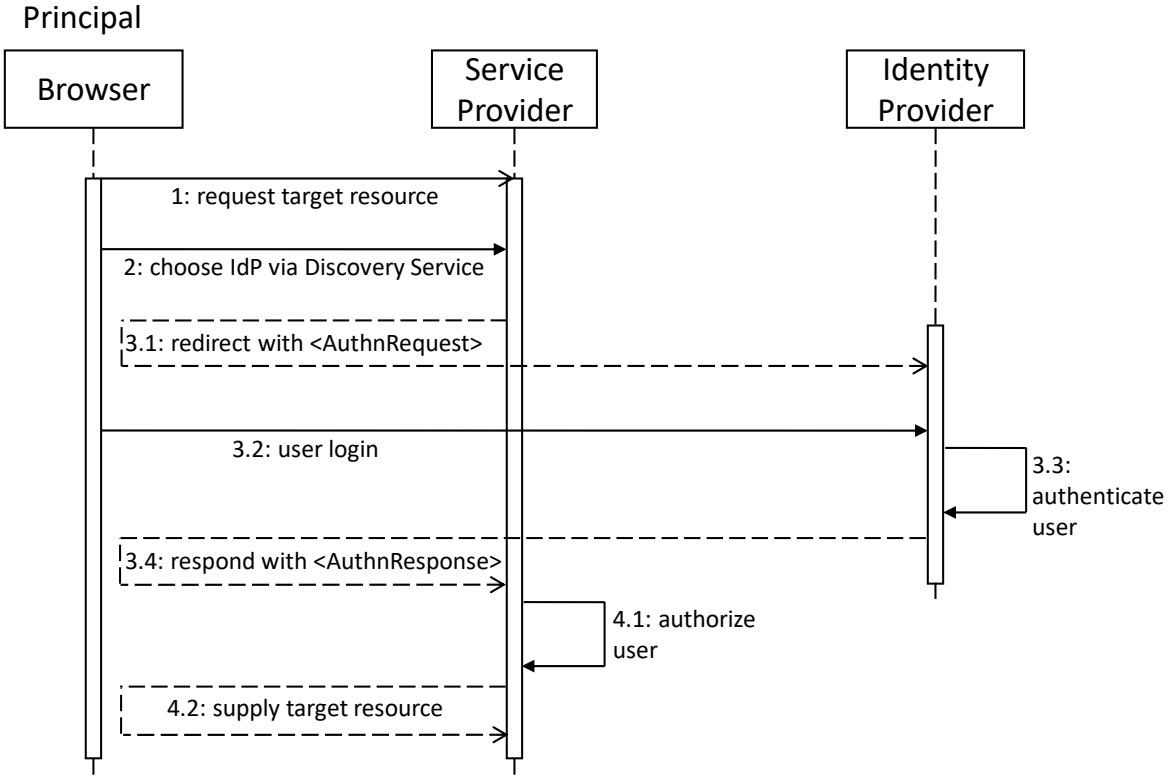


Abbildung 3.2: Genereller Ablauf einer Ein-Faktor-Authentifizierung in SAML

3.2.2.2 OpenID Connect (OIDC)

OIDC [SBJ+14b] ist ein Standard der OpenID Foundation, der das Autorisierungsprotokoll OAuth 2.0 [Har12] um eine zusätzliche Identitätsebene zum Zweck der Endnutzer-Authentifizierung erweitert. Erste Ansätze zur Erweiterung des OAuth 2.0 Standards um eine zusätzliche Authentifizierungsschicht erfolgten bereits mithilfe der OpenID Spezifikation 1.0 im Jahr 2005, die dann im Jahr 2007 mit der OpenID Version 2.0 überarbeitet wurde. 2014 verabschiedete die OpenID Foundation dann aufgrund von diversen Verbesserungen und Erweiterungen das komplett überarbeitete Protokoll OpenID Connect.

OIDC kann an dieser Stelle eher als das Protokoll des kommerziellen Sektors, bzw. des Consumer-Bereiches angesehen werden, da bspw. bekannte Unternehmen wie Google oder Microsoft sogenannte **OpenID Provider (OP)**, das Pendant zum SAML IDP, zur Verfügung stellen, die dann mit Webdiensten, die wiederum als **OIDC Relying Party (RP)** agieren (vgl. SAML: Service Provider), verknüpft werden können. Der Betreiber eines Webdienstes kann dann, analog zu SAML, auf die Implementierung eines eigenen Identitätsmanagements verzichten, da sich der Benutzer mit einem bereits existierenden Account authentifizieren kann.

Die aktuelle Version von OIDC ist Version 1.0, wobei die OIDC-Funktionalität in dem Core-Dokument [SBJ+14b] spezifiziert ist. Dieses beschreibt, wie die Authentifizierung als Schicht über OAuth 2.0 implementiert wird und wie Behauptungen (engl. *claims*) (vgl. SAML Attribute) verwendet werden, um Informationen über Endnutzer zu kommunizieren [Ope21b].

Während sich das Autorisierungsprotokoll OAuth mit dem Ausstellen von **Access Tokens** beschäftigt, ergänzt OIDC als Identitätsebene den Authentifizierungsworkflow also hauptsächlich um das Ausstellen eines **ID Tokens**. Das ID Token (JSON Web Token) ist ein von dem Access Token separat gehandhabtes Token, das Informationen über die Identität des Benutzers und der durchgeführten Authentifizierung enthält.

Die in OIDC definierten Authentifizierungsflows bauen dabei auf den durch OAuth definierten **Grant Types** auf. OAuth definiert insgesamt vier Grant Types [Har12], wobei jeweils einer oder mehrere Endpunkte (d.h. Authorization Endpoint, Token Endpoint) kontaktiert werden. Die OIDC Relying Party bzw. der Service Provider wird in OAuth als *Client* bezeichnet, wohingegen der OpenID Provider bzw. Identity Provider als *Server* bezeichnet wird. Im Folgenden werden die vier OAuth Grant Types kurz umrissen [Har12, Kaw17]:

- *Authorization Code*:
  - Der Client wird zunächst zu einem Authorization Server geleitet und erhält dort einen Authorization Code, welcher beim Token Endpoint zum Erhalt eines Access Tokens eingelöst wird.
  - Anwendungsfall: für klassische Webanwendungen geeignet, da durch die direkte Übertragung des Access Tokens an den Client eine Verbindung ohne Mitlesen des Benutzers bzw. des User-Agents zum Authorization Server aufgebaut werden kann.

- *Implicit*:
  - Stellt eine vereinfachte Form des Authorization Code Flows dar. Hier erhält der Client das Access Token direkt. Ein Authorization Code wird nicht ausgestellt.
  - Anwendungsfall: ermöglicht eine verbesserte Ansprechbarkeit bzw. Reaktionsfähigkeit aufgrund des verkürzten Flows und ist daher bspw. für Clients geeignet, die direkt im Browser ausgeführt werden.
- *Resource Owner Password Credentials*:
  - Hier können Benutzername und Passwort des Endnutzers direkt als eine Autorisierungserlaubnis herangezogen werden, um ein Access Token zu erhalten.
  - Anwendungsfall: sollte nicht mehr verwendet werden, da es im OAuth 2.1 Draft bereits als deprecated eingestuft wird [HPL21].
- *Client Credentials*:
  - Hier werden Client Credentials als Autorisierungserlaubnis herangezogen.
  - Anwendungsfall: z.B. wenn der Client gleichzeitig der Nutzer ist (Maschine-zu-Maschine-Interaktion).

Diese Liste wird von OIDC folgendermaßen ergänzt bzw. angepasst. Der Implicit und Authorization Code Flow basieren dabei auf den gleichnamigen OAuth 2.0 Grant Types [SBJ+14b, Kaw17, Bro17]:

- *Authorization Code Flow*: Der Ablauf ist analog zum OAuth Authorization Code mit der Erweiterung, dass der Token Endpoint neben dem Access Token zusätzlich noch ein ID Token ausstellt.
- *Implicit Flow*: In diesem Ablauf wird der Benutzer vom Authorization Server mit einem ID Token und, sofern angefragt mit einem Access Token, direkt zum Client zurückgeschickt.
- *OIDC Hybrid Flow*: Dieser Ablauf ist eine Kombination der beiden vorhergehenden. Durch Angabe des Response Types im Authentication Request können hier verschiedene Kombinationen aus Code und (ID) Token angefragt werden.

Anhand des UML-Sequenzdiagramms in Abbildung 3.3 wird der OIDC Authorization Code Flow grafisch verdeutlicht. Hier zeigt sich, dass der OIDC Workflow den SAML HTTP Redirect und POST Bindings z.T. sehr ähnlich ist. Die Notwendigkeit für ein ID Token wird in der Autorisierungsanfrage anhand des scope-Wertes „openid“ mitgeteilt, dadurch ergibt sich folgender Ablauf [SBJ+14b]:

1. Ein Benutzer möchte sich bei einem Dienst anmelden. Dazu generiert der Client (OIDC RP) eine Authentifizierungsanfrage, die er an den Authorization Endpoint des Servers (OIDC OP) via HTTP Redirect schickt.
2. Der Benutzer authentifiziert sich beim Server (z.B. mittels Benutzername und Passwort) und bestätigt so, dass er sich bei dem entsprechenden Dienst anmelden möchte.

3. Der Server leitet den Benutzer mit einem Authorization Code zum Client zurück.
4. Anhand des Authorization Codes kann der Client nun eine Antwort, die ein ID Token und ein Access Token im Response Body enthält, anfragen.
5. Der Client validiert das ID Token und fragt die Benutzerdaten beim UserInfo Endpoint des Servers an.
6. Der Benutzer erhält Zugriff auf den Dienst.

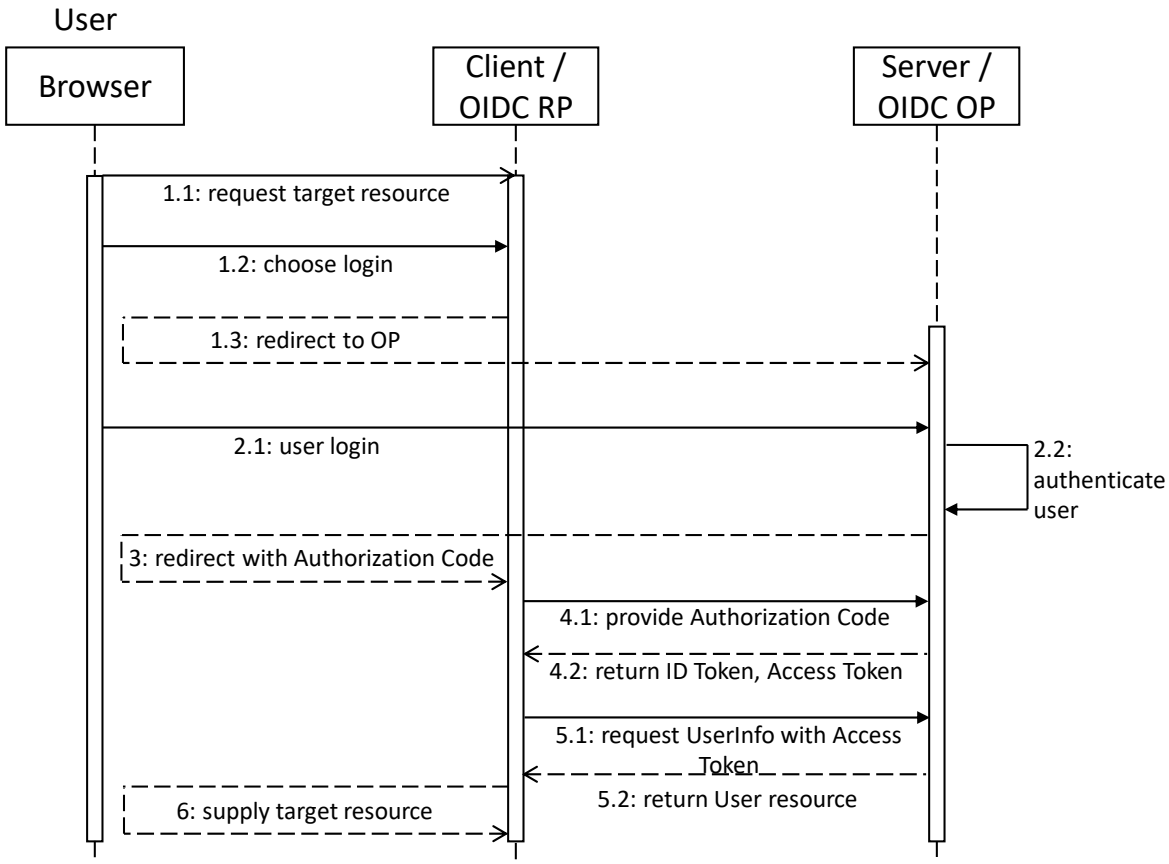


Abbildung 3.3: Genereller Ablauf einer Ein-Faktor-Authentifizierung in OIDC

Neben OIDC Core, das die OIDC-Kernelemente und -funktionalität beschreibt, existieren eine Reihe von optionalen Dokumenten, wie bspw. zur Discovery [SBJJ14] und Dynamic Registration [SBJ14a], die beschreiben, wie Relying Parties dynamisch OpenID Provider entdecken können und wie dynamische Client-Registrierung in OIDC funktioniert. Letzteres unterscheidet sich grundlegend vom SAML-Protokoll, da in OIDC die Metadaten dynamisch

ausgetauscht werden können und nicht in einer statischen Metadatendatei vorab registriert werden müssen.[3]

Weitere ergänzende, optionale Dokumente betreffen u.a. das Session Management [dMAS+20], den Front-Channel Logout [Jon20] oder den Back-Channel Logout [JB20].

Zwar können in OIDC auf dynamische Art und Weise Metadaten entdeckt und Clients registriert werden, jedoch sind die ausgetauschten Informationen alle nicht verifiziert (*engl. self-asserted*) und es existiert kein Mechanismus zur Etablierung von Vertrauen. Anhand der sich noch im Draft-Status befindenden **OpenID Connect Federation (2021)** [HJS+21] wird erstmals ein Ansatz spezifiziert, wie technisches Vertrauen zwischen RPs und OPs in OIDC dynamisch und zentralisiert auf Basis einer Trusted Third Party etabliert werden kann. Die Spezifikation bezieht dabei die Erfahrungen von SAML-Identitätsfödertionen ein und beschreibt wie OIDC Identitätsfödertionen anhand eines oder mehrerer Level von „Trust Issuer“ realisiert werden können.

Gemäß [Jon19] besteht der Hauptunterschied zu SAML darin, dass die Metadaten hierarchisch aufgebaut sind, sodass Teilnehmer Aussagen über sich selbst machen können. In SAML hingegen werden die Metadaten der Teilnehmer von den Operateuren einer (Inter-) Föderation gesammelt, zusammengeführt und flach, nicht hierarchisch, publiziert.

Der momentane OIDC Federation Draft [HJS+21] basiert auf einer *Trust Chain*, die auf Blatt-ebene (OP oder RP) mit selbst-signierten *Entity Statements* beginnt, über Entity Statements ausgestellt von *Intermediates* über dessen untergeordnete Blattentitäten fortgesetzt wird und mit einem Entity Statement des obersten Intermediate, ausgestellt von einem *Trust Anchor*, endet. Ein Entity Statement ist dabei ein signiertes JSON Web Token (JWT), das Behauptungen (sog. *claims*) über eine Entität enthält. Zu den *claims* zählen u.a. Issuer (iss), Subject (sub), Expiration Time (exp), metadata, constraints und müssen stets einen *Signing Key* enthalten, sodass untergeordnete Entity Statements überprüft werden können. Darüber hinaus erlaubt der Draft, analog zu SAML, die Verwendung von *Trust Marks* innerhalb der Metadaten, die die Erfüllung gewisser Anforderungen eines Ökosystems widerspiegeln. Trust Marks werden i.d.R. von einer durch die Föderation akkreditierten *Authority* signiert, wobei die Föderation auch bestimmte selbst-signierte Trust Marks erlauben kann. In SAML sind diese bspw. innerhalb der Metadaten mittels <mdattr:EntityAttributes> umgesetzt.

3.2.2.3 Vergleich von SAML und OIDC

In der folgenden Tabelle 3.1 sind die grundlegenden Gemeinsamkeiten und Unterschiede der beiden FIM-Standards nochmals übersichtlich dargestellt:

[3] Um einen neuen Client dynamisch beim Authorization Server (AS) zu registrieren, sendet der Client eine HTTP-POST-Anfrage mit seinen Client Metadaten an den Client Registration Endpoint des Servers. Nach erfolgreicher Registrierung schickt der Client Registration Endpoint die registrierten Metadaten, inklusive AS-spezifischer Werte, an den Client zurück (HTTP 201). [SBJ14a]

Tabelle 3.1: Vergleich der Protokolle SAML und OIDC

Kriterien	**SAML 2.0**	**OIDC**
Ziel und Zweck	Offener Standard, Framework zum Austausch von Attributs-, Authentifizierungs- und Autorisierungs-Informationen	Offener Standard zur Authentifizierung, erweitert das Autorisierungsprotokoll OAuth 2.0 um einen Identitäts-Layer
Terminologie	Identity Provider Service Provider Attribute	OpenID Provider Relying Party Scopes und Claims
Format	XML	JSON
Benutzerinformation anhand von	Assertion	ID Token
Discovery	ja	ja
Dynamische Client Registrierung	nein, Austausch der Metadaten nicht Teil der SAML-Spezifikation	ja, Registrierung unbekannter RPs und OPs möglich
Mobile Apps	nein	ja, sowohl Webbrowser als auch Mobile Apps
Vertrauensaufbau	anhand von Metadaten	aktuell nur Draft-Spezifikation vorhanden

Zusammenfassend und im Hinblick auf die in Kapitel 2 abgeleiteten (Haupt-) Anforderungen wird deutlich, dass die Hauptanforderung AK (Authentication-Assurance-Konzept) bspw. die Protokollkompatibilität (vgl. Sub-Anforderung [FA_LoA_Protokollkompatibilität]) explizit fordert. Auch mit Hauptanforderung UM (Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien) wird die Notwendigkeit eines protokoll-agnostischen Modells beschrieben, was durch die Sub-Anforderung [FA_Terminologie] widergespiegelt wird. Des Weiteren zielt Spezifikation eines Fallback MFA-Workflows (Hauptanforderung WF) ebenfalls auf einen Workflow, unabhängig vom zugrundeliegenden FIM-Protokoll, ab.

3.2.3 FIM-Softwareprodukte

In diesem Abschnitt werden exemplarisch zwei bekannte Open Source Softwareprodukte, **Shibboleth** sowie **SimpleSAMLphp**, betrachtet. Dabei stellt Shibboleth neben der namensgleichen Open Source Implementierung zusätzlich einen Forschungsansatz im Bereich des föderierten Identitätsmanagements dar [Hom07]. Während es sich bei den beiden Implementierungen primär um SAML-Produkte handelte, wurde mit der steigenden Popularität von OIDC zunehmend an dessen Unterstützung gearbeitet, sodass größtenteils be-

reits entsprechende Erweiterungen existieren.[4]. Insbesondere in R&E greifen viele wissenschaftliche und hochschulnahe Einrichtungen auf die Shibboleth- oder SimpleSAMLphp-Implementierung zurück.

3.2.3.1 Shibboleth

Die erste Version der Open Source Implementierung Shibboleth wurde 2003 von der US-amerikanischen Internet2-Initiative/MACE (Middleware Architecture Committee for Education) auf Basis von SAML 1.1 entwickelt. Inzwischen ist die Software Teil des internationalen Shibboleth Consortium, das die Weiterentwicklung, den Support und die Wartung der Software sicherstellt. Mit dem Update im Jahr 2005 von SAML auf Version 2.0 erschien auch ein Jahr später Shibboleth 2.0. Die momentan aktuelle Shibboleth-Version ist 3.0 (Shibboleth SP) bzw. 4.0 (Shibboleth IDP). [Shi21]

Die Shibboleth-Software stetzt sich aus den folgenden Produkten zusammen [Shi21]:

- **Identity Provider:** Stellt eine SSO-Lösung für IAM-betreibende Organisationen auf Basis von Java zur Verfügung. Der Shibboleth IDP besitzt einbauten Support für eine Vielzahl von Authentifizierungssystemen und ermöglicht aufgrund seiner Erweiterbarkeit die Unterstützung verschiedenster Szenarien.
- **Service Provider:** Stellt das Gegenstück zur IDP Software dar, die in C++ implementiert ist und die Integration mit bekannten Webservern unterstützt.
- **Embedded Discovery Service:** Der eingebettete Lokalisierungsdienst stellt ein Webinterface zur Auswahl des Identity Providers durch den Nutzer zur Verfügung. Dieser wird zusammen mit der SP Implementierung installiert und kann anhand HTML, Javascript und CSS individualisiert werden.
- **Centralized Discovery Service:** Im Gegensatz zum eingebetteten Lokalisierungsdienst handelt es sich hierbei um eine zentralisierte Variante, die bspw. von Betreibern einer Föderation eingesetzt werden kann.
- **Metadata Aggregator:** Das Tool, entweder Kommandozeilen-basiert oder Web-service-basiert, ermöglicht das Einlesen, Verifizieren, Filtern und Transformieren von Metadaten. Es wird v.a. von Föderationsbetreibern zur Verwaltung der Metadaten mehrerer Identity Provider und Service Provider eingesetzt.

3.2.3.2 SimpleSAMLphp

SimpleSAMLphp (SSp) [Uni21] ist eine Open Source Implementierung in PHP, wobei das Projekt von dem norwegischen NREN Uninett geleitet wird. Die momentan aktuelle Version ist 1.19 (Jahr 2021).

[4] Im Jahr 2021 wurde bspw. im Rahmen des GÉANT-Projekts an der Unterstützung der OIDC OP Funktionalität für SimpleSAMLphp gearbeitet.

Der Fokus von SSp liegt hierbei auf den beiden zentralen Komponenten IDP und SP, die jedoch im Gegensatz zu Shibboleth auf einen gemeinsamen Software-Stack zurückgreifen. Soll der SSp-Software-Stack bspw. als SAML 2.0 Identity Provider genutzt werden, muss in der Konfigurationsdatei lediglich die Option *'enable.saml20-idp' => true,* gesetzt werden. Ferner verfolgt SSp einen stark modularen Ansatz und setzt dabei u.a. auf die Weiterentwicklung durch die Community. SSp ist somit flexibel erweiterbar und unterscheidet bei den ergänzenden Drittanbieter-Modulen zwischen den folgenden Erweiterungen [Uni21]:

- **Authentication Modules:** Ermöglicht die Implementierung eigener Authentifizierungsmethoden.
- **Authentication Processing Filters:** Unterstützt verschiedene Filter zur Verarbeitung nach einer stattgefundenen Authentifizierung.
- **Themes:** Anpassen der durch SSp bereitgestellten Seiten.
- **Modules:** Allgemeine Erweiterungen, wie bspw. neue Protokolle.

So ist bspw. ein Discovery Service, der in Shibboleth zusammen mit der SP Implementierung installiert wird, in SSp in Form eines entsprechenden Moduls vorhanden. Auch in Bezug auf MFA ist ein Modul vorhanden, dass eine Zwei-Faktor-Authentifizierung gegen einen PrivacyIDEA-Server [Net21] bereitstellt.

3.2.4 FIM-Architekturmodelle

Identitätsföderationen setzen sich aus einer beliebigen Anzahl an IDPs und SPs zusammen und lassen sich daher, technisch betrachtet, auf verschiedene Art und Weise implementieren. Während in kommerziellen Szenarien häufig 1:n (d.h. ein IDP, n SPs) oder n:1 (n IDPs, ein SP) Föderationen vorhanden sind, sind Identitätsföderationen in R&E aufgrund ihrer m:n (m IDPs, n SPs) Struktur komplexer ausgeprägt. Föderationen aus R&E lassen sich grob anhand drei Architekturmustern klassifizieren [GÉ17b]; Hybride sind jedoch möglich.

Im Folgenden werden die drei Architekturmuster gemäß [GÉ17b] kurz vorgestellt:

- **Vollvermascht (engl. Full Mesh)**: Das Hauptmerkmal dieses Musters ist (vgl. Abbildung 3.4), dass innerhalb der Föderation keine zentrale Komponente vorhanden ist, die SAML IDPs und SAML SPs miteinander verknüpft. Hier findet also eine direkte, bilaterale Kommunikation zwischen jedem SAML IDP mit jedem SAML SP statt. Realisiert ist dies mittels einer zentralen SAML-Metadatendatei, in der alle SAML IDPs bzw. SAML SPs der Föderation verzeichnet sind. Jeder SAML IDP bzw. SP hält eine Instanz der Datei, die regelmäßig aktualisiert wird. Zur Weiterleitung des Nutzers von SAML SP zu dessen SAML Home IDP kommt ein Discovery Service zum Einsatz, der bspw. zentral von der Föderation oder auch individuell von SAML SPs implementiert wird. Dieses Architekturmuster findet gemäß [GÉ17b] in rund 80% der Föderationen Anwendung. Dazu zählt bspw. die deutsche Föderation DFN-AAI sowie die amerikanische Föderation InCommon.

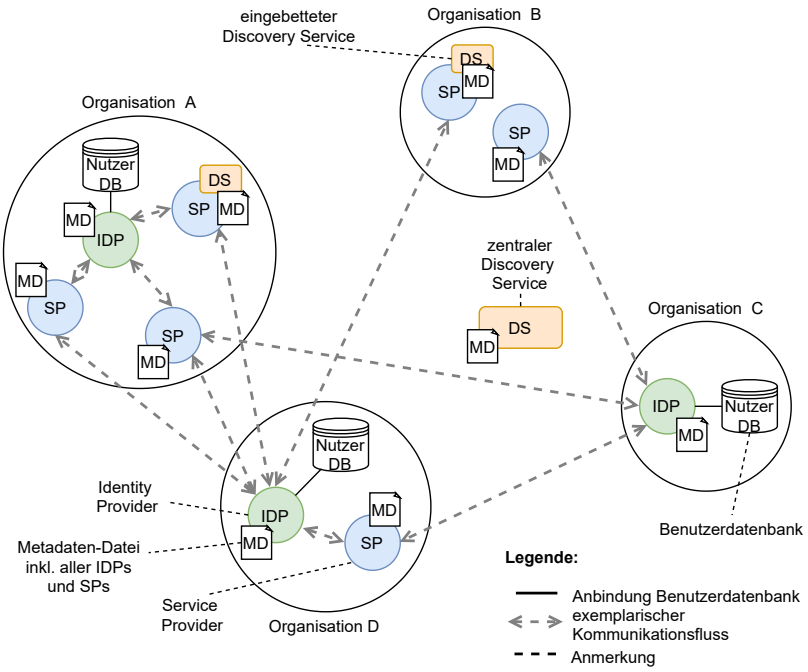


Abbildung 3.4: Full Mesh Föderationsarchitektur nach [GÉ17b]

- **Proxy-basiert mit verteiltem Login (engl. Hub&Spoke (H&S) Distributed Login)**: Im Gegensatz zur vollvermaschten Architektur findet in diesem Architekturmodell (siehe Abbildung 3.5) die gesamte Kommunikation über einen zentralen Hub bzw. Proxy statt. Dieser verhält sich aus Sicht eines SAML IDP wie ein SAML SP und vice versa. *Distributed Login* bedeutet in diesem speziellen Fall, dass es keinen zentralen SAML IDP innerhalb der Föderation gibt, sondern Organisationen nach wie vor ihren eigenen SAML IDP betreiben. Hinsichtlich der Realisierung benötigt jeder SAML IDP und SAML SP in einer proxy-basierten Föderation mit verteiltem Login nur die Metadaten des Hubs, während der Hub eine Metadatendatei hält, in dem alle SAML IDPs und SAML SPs verzeichnet sind. Der Discovery Service ist meist zentral beim Hub implementiert. Dieses Architekturmuster findet bspw. in der niederländischen Föderation SURF Anwendung.

- **Proxy-basiert mit zentralem Login (Hub&Spoke Centralized Login)**: Dieses Architekturmodell, dargestellt in Abbildung 3.6, ist seltener in der Verbreitung und kommt meist nur bei kleineren Föderationen, wie bspw. der norwegischen Föderation FEIDE, zum Einsatz. Ein Grund mitunter ist, dass es gemäß diesem Muster in der gesamten Föderation nur einen zentralen SAML IDP gibt, an den die Benutzerdatenbanken aller teilnehmenden Organisationen angeschlossen sind. Hier hält der zentrale SAML IDP die Metadaten aller SAML SPs, während die SAML SPs nur die Metadaten eines SAML IDPs benötigen. Jedoch ergeben sich aufgrund des Single Points of Failure besondere Anforderungen an Sicherheit, Verfügbarkeit und Skalierbarkeit.

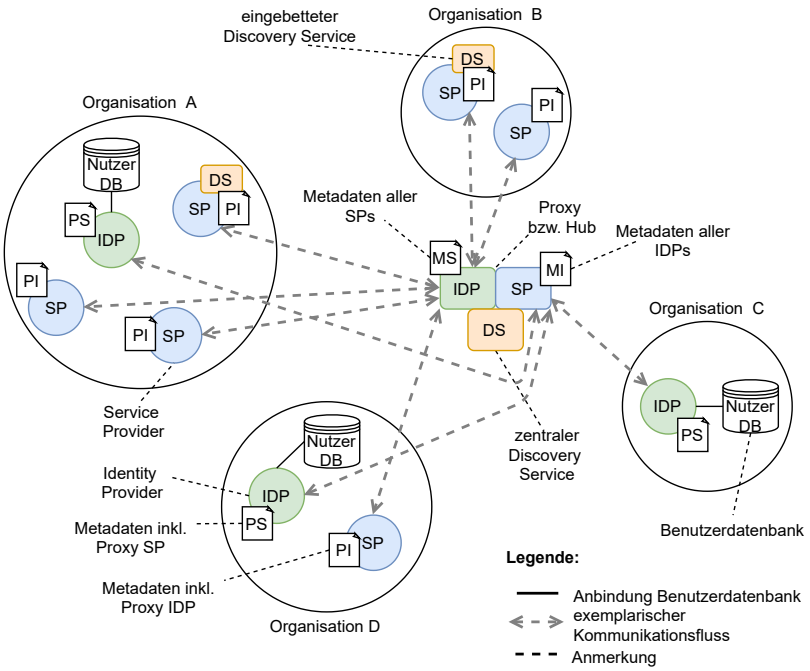


Abbildung 3.5: H&S Distributed Login Föderationsarchitektur nach [GÉ17b]

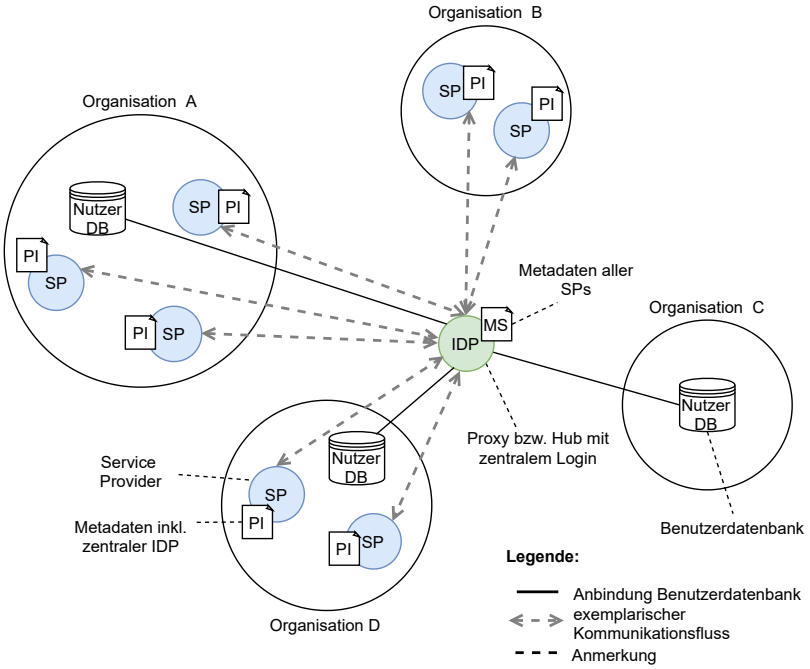


Abbildung 3.6: H&S Centralized Login Föderationsarchitektur nach [GÉ17b]

3.3 Interföderiertes Identitätsmanagement

Inter-FIM bezeichnet einen Ansatz, der FIM-Konzepte wiederverwendet und darauf aufbauend eine Identitätsinterföderation erzeugt. Dadurch können Teilnehmer einer Föderation nicht nur föderationsintern kollaborieren, sondern können auch mit Teilnehmern einer anderen Föderation *föderationsübergreifend* kommunizieren. Eine **Interföderation** stellt somit eine (Umbrella-) Föderation dar, deren Teilnehmer wiederum selbst Föderationen sind [Pöh16].

Anhand des Beispiels eduGAIN [GÉ18] wird im folgenden Abschnitt das Konzept Inter-FIM näher erläutert und beschrieben, wie die Etablierung eines Vertrauensverhältnisses (*engl. Trust Management*) zwischen den Entitäten auf verschiedenen Ebenen stattfindet. Vertrauen wird dabei sowohl durch technische als auch organisatorische Maßnahmen etabliert.

3.3.1 Interföderation eduGAIN

Wie bereits an früherer Stelle erläutert, wurde die Interfödertion eduGAIN etabliert, um die gegenseitige Dienstnutzung zum Zwecke der Forschung und Lehre zu erleichtern. Bei den teilnehmenden Föderationen handelt es sich also um der Forschung und Lehre zugewandte Föderationen, wie es bspw. in Deutschland bei der DFN-AAI der Fall ist.

Der **technische Vertrauensaufbau** geschieht in der Interföderation mittels SAML, wobei auf bestehende Konzepte des föderierten Identitätsmanagements zurückgegriffen wird [GÉ20b]:

- Damit eine Kommunikation zwischen den teilnehmenden Entitäten (d.h. IDPs, SPs) einer Interföderation möglich ist, teilen sie sich einen zentralen SAML-Metadatensatz (vgl. Abschnitt 3.2.4). Da jede nationale Föderation durch den Betrieb einer AAI bereits einen eigenen Metadatensatz besitzt, in dem potentiell auch nicht an der Interföderation teilnehmende IDPs und SPs vorhanden sein können, wird i.d.R. zunächst ein Metadatensatz generiert, der nur Entitäten enthält, die an der Interföderation teilnehmen.
- Generell gibt es zwei verschiedene Member-Modelle [GÉ20b]: bei *opt-in* müssen Entitäten explizit die Aufnahme in den Interföderations-Metadatensatz aktivieren, während bei *opt-out* alle Entitäten automatisch aufgenommen werden, außer sie deaktivieren dies explizit.
- Die föderationsspezifischen Metadatensätze werden dann mit dem Core Service von eduGAIN, dem *Metadata Distribution Service*, geteilt. Dieser aggregiert die Metadatensätze aller Föderationen, woraufhin sich dann die teilnehmenden Föderationen den aggregierten Metadatensatz herunterladen. Die Föderationen wiederum teilen die resultierenden Metadaten mit den entsprechenden IDPs bzw. SPs.
- Wie bereits in Listing 3.1 exemplarisch aufgezeigt, wird neben dem hier beschriebenen Austausch der Metadaten zum Vertrauensaufbau, der Austausch von Vertrauensinformation innerhalb des Metadatensatzes fortgesetzt. So enthält der Metadatensatz u.a.

Schlüssel- und Zertifikatsinformationen, die für eine sichere Kommunikation erforderlich sind. Darüber hinaus wird innerhalb der Metadaten die Konformität zu diversen Spezifikationen ausgedrückt.

Auf **organisatorischer Ebene** wird das Vertrauensverhältnis in eduGAIN durch einen Aufnahmeprozess und dem damit verbundenen Unterzeichnen von Verträgen etabliert [GÉ20b]. Abbildung 3.7 verdeutlicht das dadurch entstandene vertragliche Konstrukt der in eduGAIN teilnehmenden Entitäten, welches am Beispiel des Leibniz-Rechenzentrums erläutert wird. Grundsätzlich gilt hier, damit eine Organisation bzw. deren Benutzer eduGAIN nutzen können, muss die entsprechende Organisation zunächst eine Mitgliedschaft bei einem NREN zur Teilnahme an einer Identitätsföderation beantragen. Dadurch entsteht eine hierarchische Abhängigkeit, die in Abbildung 3.7 verdeutlicht wird.

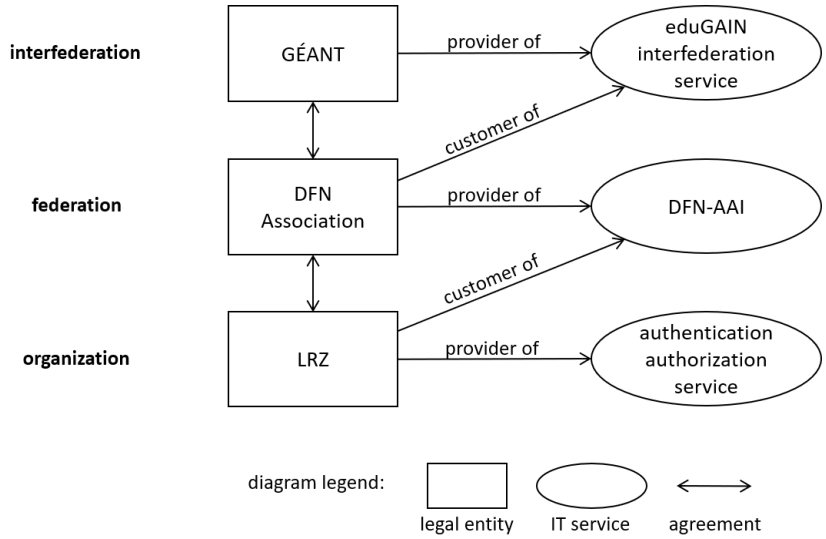


Abbildung 3.7: Organisatorisches Vertrauen bzw. vertragliches Konstrukt am Beispiel der Interföderation eduGAIN

- Auf **interföderiertem Level** (siehe Abbildung 3.7) muss der *eduGAIN joining process* [GÉ20b] durchlaufen werden, wobei direkte Teilnehmer bzw. Kunden von eduGAIN stets NRENs sind. In Deutschland ist das bspw. der DFN-Verein. Organisationen wie das Leibniz-Rechenzentrum (3. Schicht in Abbildung 3.7, von oben nach unten) können aufgrund der hierarchischen Abhängigkeit kein direkter Teilnehmer bzw. Kunde des eduGAIN Dienstes werden.
- **Föderiertes Level**: Im konkreten Beispiel hat der DFN-Verein den eduGAIN joining process durchlaufen und in diesem Zuge eine *Policy Declaration* [GÉ16] unterzeichnet, um Teilnehmer bzw. Kunde des Dienstes eduGAIN zu werden. Durch Unterzeichnen der Policy Declaration verpflichtet sich der DFN-Verein, der Provider der nationalen Identitätsföderation DFN-AAI, zur Einhaltung des eduGAIN-Vertragsrahmenwerks.
- **Organisatorisches Level**: Das Leibniz-Rechenzentrum in München ist u.a. Identity Provider für dessen Mitarbeiter (und z.T. Kunden) und wurde durch Abschluss eines

Vertrages mit dem DFN-Verein Teilnehmer der DFN-AAI Föderation. Eine Organisation kann dann entscheiden, ob ihre föderierten Dienste über die DFN-AAI hinweg auch für eduGAIN sichtbar bzw. nutzbar sein sollen. Hinsichtlich der Teilnahme in eduGAIN wenden NRENs unterschiedliche Methoden an. Bei der Methode opt-in, die auch die DFN-AAI verfolgt, müssen sich Organisationen explizit dafür entscheiden, an eduGAIN teilzunehmen und vice versa bei opt-out (vgl. oben).

Abschließend zusammengefasst stellt die Interföderation eduGAIN somit eine Infrastruktur bereit, die die *gegenseitige Dienstnutzung erleichtert*. Die Teilnahme an eduGAIN erzeugt jedoch nicht automatisch das Recht auf die Dienste anderer Föderationen bzw. Teilnehmer tatsächlich zugreifen zu dürfen. Dies muss u.U. bilateral zwischen den entsprechenden Teilnehmern ausgehandelt werden.

3.4 Authentifizierung

Der Prozess der Authentifizierung steht in engem Zusammenhang mit dem Begriff der **Authentizität**, der neben den Aspekten der *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* ein weiteres Schutzziel in der Informationssicherheit darstellt.

Die Authentizität (engl. *authenticity*), bezeichnet die Echtheit einer Entität (z.B. eines Subjekts oder Objekts) oder eines Attributs, die mittels Überprüfung verifiziert und damit die Entität bzw. das Attribut als vertrauenswürdig klassifiziert wird [Shi07]. Zur Verifikation der Authentizität wird im deutschen Sprachgebrauch zwischen den Verfahren der **Authentisierung** und der **Authentifizierung** unterschieden, die jedoch im umgangssprachlichen häufig verwechselt bzw. synonym verwendet werden.

Die folgende Grafik 3.8 verdeutlicht die Unterschiede.

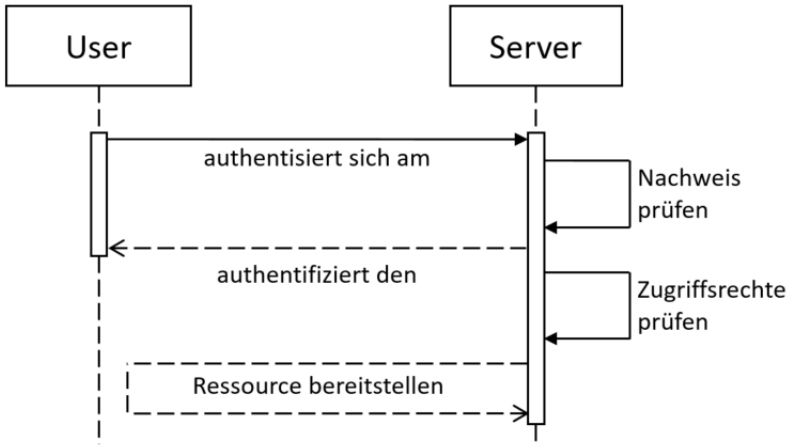


Abbildung 3.8: Zusammenspiel zwischen Authentisierung, Authentifizierung und Autorisierung

Die Authentisierung beschreibt somit die Behauptung der Authentizität basierend auf der Erbringung von Nachweisen (z.B. UserID und Passwort), während die Authentifizierung nach erbrachter Überprüfung der Nachweise den Rückkanal darstellt [Bun22]. Im Englischen wird zwischen den beiden Begriffen aufgrund wechselseitiger Zusammenhänge nicht unterschieden und das Verfahren unter dem Begriff *authentication* subsumiert. Der Informational RFC 4949 [Shi07] unterscheidet hier zwischen zwei grundlegenden Schritten beim Authentifizierungsprozess: Der Identifizierungsphase, wie bspw. das Vorzeigen des User Identifiers, sowie der Verifizierungsphase, die das Präsentieren bzw. Generieren des Berechtigungsnachweises als Beweis darstellt.

Für den weiteren Gebrauch im Rahmen dieser Arbeit wird der Begriff *Authentifizierung* dann verwendet, wenn das gesamtheitliche Verfahren betrachtet wird. Wird explizit die Authentisierung betrachtet, wird dies entsprechend textuell hervorgehoben.

Wie in Abbildung 3.8 aufgezeigt, findet auch die **Autorisierung** und **Zugriffskontrolle** in diesem Zusammenhang Anwendung. Die Autorisierung ist definiert als die initiale Vergabe von Rechten, wobei die technische Umsetzung, d.h. die Zugriffsentscheidung, was ein Benutzer mit einer Ressource machen darf, als Zugriffskontrolle bezeichnet wird [DC02].

Die Erbringung eines Nachweises durch den Benutzer erfolgt typischerweise auf Basis eines oder mehrerer **Authentifizierungsfaktoren**, oder kurz Faktor. Ein Faktor gehört stets einer Kategorie bzw. eines Typs an, der beschreibt auf welche Art und Weise ein Nachweis erbracht wird [GGF17b]. Abhängig von der Anzahl der Faktoren unterschiedlichen Typs (vgl. Abschnitt 3.4.1) ergeben sich dann unterschiedlich starke Möglichkeiten der Nachweiserbringung, die unter den Begriffen der **Ein-Faktor- und Multi-Faktor-Authentifizierung** (siehe Abschnitt 3.4.3) bekannt sind. Bei einer Multi-Faktor-Authentifizierung müssen mindestens zwei Faktoren *unterschiedlichen Typs* herangezogen werden [GGF17b], andernfalls läge keine gültige Multi-Faktor-Authentifizierung vor (vgl. Abbildung 3.9).

3.4.1 Klassifikation von Authentifizierungsfaktoren

Im Allgemeinen werden Authentifizierungsfaktoren in unterschiedliche *Typen* bzw. *Klassen* eingeteilt. Dieser Abschnitt präsentiert zunächst existierende Definitionen und erläutert des Weiteren anhand von Beispielen einige geläufige Implementierungen.

Weit verbreitet ist die Klassifikation der Authentifizierungsfaktoren in *something you know*, *something you have* und *something you are*, wie es etwa in [GGF17b] beschrieben ist:

- **something you know** beschreibt Faktoren, die durch den Benutzer zu merken sind, wie bspw. ein Passwort oder eine PIN. Derartige Faktoren sind besonders anfällig hinsichtlich Brute Force, Phishing oder Social Engineering Angriffen.
- **something you have** sind Faktoren, die ein Benutzer besitzt, wie bspw. ein Einmalpasswortgenerator (OTP Device). Auch Zertifikate sind als Besitztum definiert.
- **something you are** oder Biometrie. Dieser Faktortyp bezieht sich auf die Überprüfung von eindeutigen, körperbezogenen Eigenschaften, wie bspw. den Fingerabdruck,

die Iris oder das Gesicht. Hier verbleibt stets eine heuristische Fehlerrate (i.S.v. false positives, false negatives).

Die folgende Abbildung 3.9 verdeutlicht grafisch, welche Kombinationen (hier: in Form von Überlappungen dargestellt) von Authentifizierungsfaktoren gemäß Definition zu einer gültigen Multi-Faktor-Authentifizierung führen.

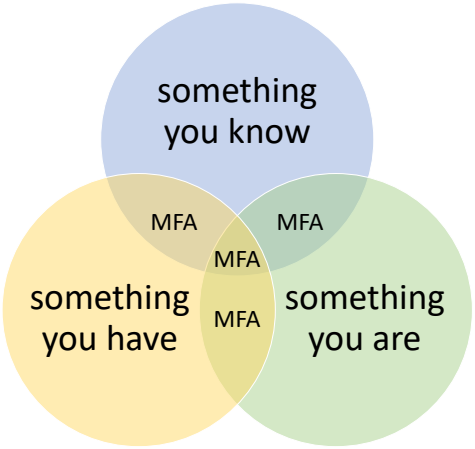


Abbildung 3.9: Gültige Kombinationsmöglichkeiten einer Multi-Faktor-Authentifizierung

Neben dieser Klassifikation existieren noch weitere Faktortypen wie bspw. von der International Telecommunication Union (ITU) [Int12] beschrieben. ITU definiert neben den drei bereits beschriebenen Faktortypen zusätzlich einen vierten Faktortyp. Dieser wird häufig als kein eigenständiger Faktortyp, sondern vielmehr als Teilaspekt von *something you are* angesehen:

- **something you do** zielt auf spezifische Verhaltensmuster von Nutzern, wie z.B. deren Augenbewegung, ab.

Darüber hinaus gibt es noch weitere neue, sich entwickelnde Faktortypen, wie bspw. zeit- oder ortsbezogene Faktoren. Da ständig neue Faktortypen und konkrete Implementierungen entwickelt werden, ist ein gemeinsames Verständnis über die verwendete Klassifikation von Authentifizierungsfaktoren maßgeblich, denn nur dann kann über die Quantität der Faktoren und die Qualität des Authentifizierungsprozesses entschieden werden.

Interessant an dieser Stelle zu erwähnen ist, dass die Authentifizierungsfaktoren gemäß zuvor genannter Klassifikation(en) von einem Authentifizierungssystem i.d.R. gar nicht unterschieden werden können. Sowohl bspw. ein Passwort (d.h. Wissensfaktor) als auch ein TAN einer TAN-Liste (d.h. Besitzfaktor) werden auf die gleiche Art und Weise in ein Authentifizierungssystem eingespeist; folglich wurde die Unterscheidung primär für Menschen gemacht.

3.4.2 Beispiele von Authentifizierungsfaktoren

Die Verwendung einer Kombination aus Benutzername und Passwort wird aktuell insbesondere bei Webauthentifizierungen als populäre Variante zur Ein-Faktor-Authentifizierung (1FA) herangezogen. Dennoch existieren pro Faktortyp meist mehrere unterschiedliche Realisierungen bzw. Produkte, wovon einige davon in der Tabelle 3.2 exemplarisch dargestellt sind:

Tabelle 3.2: Auszug exemplarischer Authentifizierungsfaktoren

Authentifizierung mittels	**Faktortyp**	**Kurzbeschreibung**	**Realisierung**	**Produktbeispiel**
PIN	Wissen	numerische Zahlenkombination	-	-
Zertifikat	Besitz	kryptographisch generierte Zeichenkette, z.B. mittels RSA/DSA oder Elliptischen Kurven (ECDSA)	Software, Hardware	X.509-Zertifikat, YubiKey [Yub21]
Einmalpasswort (OTP)	Besitz	Zeitbasiert (TOTP), HMAC-basiert (HOTP)	Software, Hardware	Google Authenticator (TOTP) [Goo22]
TAN-Liste	Besitz	Liste mit Einmalpasswörtern/-PINs	physisch, elektronisch	Papierbasierte TAN-Liste
Fingerabdruck	Inhärenz	Scannen des Fingerabdrucks, Vergleich Muster gegen Vorlage	Sensor	iPhone Touch ID [App22]

Bei einer Ein-Faktor-Authentifizierung wird, wie der Begriff bereits indiziert, nur ein Faktor zur Authentifizierung herangezogen. Dabei sollten jedoch laut [GFN+17] Biometriefaktoren, u.a. aufgrund der heuristischen Fehlerrate, nicht zur Ein-Faktor-Authentifizierung herangezogen werden.

3.4.3 Multi-Faktor-Authentifizierung

Im Gegensatz zur Ein-Faktor-Authentifizierung greift die **Multi-Faktor-Authentifizierung** (MFA) auf *mindestens zwei Faktoren unterschiedlichen Typs* zum Nachweis der Authentizität zurück [ISO13b]. Werden genau zwei Faktoren unterschiedlichen Typs verwendet, spricht man von einer **Zwei-Faktor-Authentifizierung** (2FA).

Im Allgemeinen wird 2FA bzw. MFA meist mit einer höheren Sicherheit assoziiert, dies ist jedoch nur gegeben, wenn einige Grundprinzipien zur Authentifizierung mit mehreren Faktoren eingehalten werden.

Dazu zählt zum Einen, wie zuvor genannt, die Einhaltung der Verwendung *unterschiedlicher Faktortypen* [ISO13b, GGF17b]. D.h. eine Authentifizierung mit zwei Passwörtern wird nicht als MFA angesehen. Dabei ist beim Faktortyp *something you have* zur Vorsicht geboten. Eine zertifikatsbasierte 1FA kombiniert mit einem OTP Device zur 2FA ist in der Praxis durchaus denkbar, sinngemäß handelt es sich jedoch auch hierbei nicht um eine gültige Multi-Faktor-Authentifizierung.

Zum Anderen muss die *Unabhängigkeit der Faktoren* gewährleistet sein [GFN+17]. Das bedeutet, dass ein Faktor nicht durch einen anderen Faktor zugreifbar sein darf. Kann also bspw. auf den zweiten Faktor durch Authentifizierung mit dem ersten Faktor zugegriffen bzw. dieser verändert werden, sind die Faktoren voneinander abhängig und die vermeintliche Zwei-Faktor-Authentifizierung ist nicht sicherer als eine Authentifizierung mit dem Schwächeren der Faktoren. Die Unabhängigkeit der Faktoren sollte im Idealfall während des gesamten Lebenszyklus eines Faktors aufrechterhalten werden. Besonders kritisch ist hierbei die initiale Registrierung eines neuen Faktors. In der Praxis kommt es häufig vor, dass die Erstregistrierung eine Ausnahme hinsichtlich der Unabhängigkeit darstellt und ein neuer Faktor durch Authentifizierung mit einem bereits existierenden Faktor registriert werden kann. Und erst nach diesem Schritt wird die Unabhängigkeit etabliert. Aus Security-Perspektive bedeutet das, dass ein Angreifer, sobald er ein Benutzerkonto mit nur einem Faktor kompromittiert hat, einen zweiten Faktor registrieren könnte und damit den echten Eigentümer von seinem Konto aussperren würde. Um dieser Gefährdung entgegenzuwirken, sollten weitere Faktoren immer direkt an den realen Eigentümer und nicht an die assoziierte digitale Identität gebunden werden. Dies ist natürlich mit entsprechend hohem Aufwand verknüpft (siehe u.a. Feststellung der Identität, Abschnitt 3.4.4), den man in der Praxis häufig zu umgehen versucht.

3.4.3.1 Abgrenzung zur Multiple-Channel und Multi-Stage Authentication

MFA ist folglich als eine Authentifizierung mit zwei oder mehreren unterschiedlichen Faktortypen definiert. Hier gibt es spezialisierte Ausprägungen, wie die Multiple-Channel Authentication als Teilmenge der Multi-Faktor-Authentifizierung, aber auch Abgrenzungen (vgl. Multi-Stage Authentication), was keine Multi-Faktor-Authentifizierung im eigentlichen Sinne darstellt. Diese werden im Folgenden kurz erläutert.

Die **Multiple-Channel Authentication** (MCA) ist definiert als eine Authentifizierung, bei der die involvierten Faktoren über verschiedene Kanäle oder Protokolle kommuniziert werden. Meist wird zwischen den beiden Konzepten in der Praxis nicht genauer unterschieden, jedoch sind MFA und MCA nicht deckungsgleich zu behandeln, denn nicht jede MFA ist auch eine MCA. Aus Security-Perspektive betrachtet, ergeben sich bei einer MCA die Vorteile, dass der Angreifer die Kanäle und die jeweiligen Schwächen kennen muss und darüber hinaus das Timing beim Anfangen der Faktoren ebenfalls eine Rolle spielt. [LDA17]

Im Gegensatz zur MCA handelt es sich bei der **Multi-Stage Authentication**, um keine gültige Multi-Faktor-Authentifizierung. Die Multi-Stage Authentication beschreibt hierbei einen Authentifizierungsprozess, bei dem ein Faktor herangezogen wird, um Zugriff auf einen weiteren Faktor zu erhalten [BDN+13]. Als Beispiel in [BDN+13] werden hier kryptographische Schlüssel genannt, die auf einem Server liegen und die nach Authentifizierung mit einem Passwort oder einer Passphrase auf das lokale System des Benutzers heruntergeladen werden können. Eine Multi-Stage Authentication ist in dem konkreten Beispiel folglich nur genauso sicher, wie das Passwort, das zum Herunterladen der kryptographischen Schlüssel verwendet wurde.

3.4.4 Authentifizierung versus Identitätsfeststellung

Wie bereits zu Beginn des Abschnitts 3.4 erläutert, beschäftigt sich die Authentifizierung mit der Überprüfung der Echtheit einer Entität bzw. einer Person, d.h. konkret mit der Überprüfung, ob eine Entität auch diejenige ist, die sie vorgibt zu sein. Dabei wird zur Nachweiserbringung auf die Verwendung einer oder mehrerer Authentifizierungsfaktoren (i.S.v. Wissensfaktor, Besitzfaktor etc.) zurückgegriffen. Im Rahmen eines Authentifizierungsverfahrens wird also folglich überprüft, ob es die *richtige bzw. authentische* Entität bzw. Person ist, nicht jedoch, ob die Entität bzw. Person auch tatsächlich in der realen Welt existiert. Dies ist Teil der **Identitätsfeststellung** (*engl. identity proofing, identity vetting*), im allgemeinen Sprachgebrauch auch als *Identifizierung* bezeichnet, die das Verfahren darstellt, das im Zusammenhang mit digitalen Identitäten verwendet wird, um eine möglichst verlässliche Assoziation zwischen digitaler und realer Identität herzustellen [GFL+17]. Das primäre Ziel stellt somit dar, sicherzustellen, dass die behauptete Identität in der realen Welt existiert, um darauf basierend eine Verbindung mit der digitalen Identität herzustellen.

Um eine klare Abgrenzung zwischen der Authentifizierung, die Fokus dieser Arbeit ist, und der Identitätsfeststellung (die ausgeklammert wurde) zu ziehen, werden zur Verdeutlichung der Prozess der Identitätsfeststellung sowie exemplarisch einige existierende Verfahren kurz betrachtet.

Eine Identitätsfeststellung ist insbesondere dann von Relevanz, wenn die von einer digitalen Identität getätigten Transaktionen bspw. aufgrund ihrer Kritikalität (vgl. Finanzsektor) eindeutig einer spezifischen realen Identität zugeordnet werden müssen. Die Identitätsfeststellung ist somit ein der Authentifizierung vorgelagerter Prozess und ist keinesfalls mit der Authentifizierung gleichzusetzen.

Gemäß NIST 800-63-3A [GFL+17] wird das grundlegende Verfahren zur Identitätsfeststellung in drei Schritte unterteilt:

1. **Resolution:** Sammeln von Informationen bzw. Attributen über die reale Person (*engl. Personally Identifiable Information (PII)*) sowie Sammeln von Identitätsbeweisen (z.B. Ausweis, Führerschein).
   Output: Das Individuum ist gegenüber einer Population bzw. einem Kontext einzigartig unterscheidbar.

2. **Validation:** Die erhaltenen Informationen (PII) werden gegenüber einer autoritativen Quelle überprüft und getestet, ob diese den Aufzeichnungen entsprechen. Beweismittel werden validiert.
   Output: Identitätsinformation ist authentisch, valide und korrekt und steht in Zusammenhang mit einer realen Identität.

3. **Verification:** Verifikation der Beweismittel anhand von Lebendigkeitsprüfung (*engl. Liveness Check*).
   Output: Die Identität des Antragstellers wurde erfolgreich überprüft und eine Verknüpfung zwischen behaupteter und real existierender Identität hergestellt.

Analog zur Authentifizierung kann eine Identitätsfeststellung eine unterschiedliche Stärke bzw. Verlässlichkeit aufweisen, je nachdem, auf welche Art und Weise eine Identitätsfeststellung stattgefunden hat. In Abbildung 3.10 sind die Verfahren zur Identitätsfeststellung exemplarisch gemäß drei hierarchischer, absteigender Klassen kategorisiert, die in entsprechenden Assurance Leveln (vgl. Abschnitt 3.6) widergespiegelt werden können.

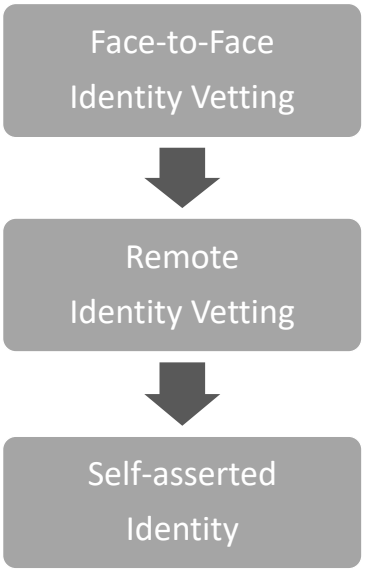


Abbildung 3.10: Einordnung von Verfahren zur Identitätsfeststellung

Es ist folglich zu beachten, dass bei einer Authentifizierung die reale Person nicht zwangsweise bekannt sein muss. Es sind auch Authentifizierungen anonymer bzw. pseudonymer Entitäten möglich, ohne dass eine vorangegangene Identitätsfeststellung stattgefunden hat.

Zusammenfassend sind die Authentifizierung und die Identitätsfeststellung zwei unterschiedliche Verfahren. Betrachtet man deren relative Häufigkeit, wird deutlich, dass, bezogen auf einen Benutzer, Authentifizierungen im Vergleich zu Identitätsfeststellungen logischerweise weitaus häufiger stattfinden. Während eine Authentifizierung stets bei Zugriff auf einen Dienst durchgeführt wird, findet eine Identitätsfeststellung typischerweise einmalig zu Beginn, z.B. bei Eröffnung eines neuen Benutzerkontos, oder zu weiteren definierten Zeitpunkten, wie bspw. beim Hinzufügen oder Wiederherstellen eines zweiten Faktors, statt.

3.5 Forschungsansätze zur Multi-Faktor-Authentifizierung in FIM

In diesem Abschnitt werden vier bekannte Forschungsansätze zur Multi-Faktor-Authentifizierung in FIM vorgestellt. Für jeden Forschungsansatz, im Folgenden als **MFA-Ansatz** bezeichnet, wird der grundlegende Workflow erläutert und dieser gegebenenfalls durch UML-Sequenzdiagramme verdeutlicht. Des Weiteren werden Softwareprodukte und Implementierungsbeispiele, wie sie z.T. bereits in R&E Organisationen und Föderationen Anwendung finden, aufgezeigt. Einige, zu diesem Thema veröffentlichen, Forschungsarbeiten werden ebenfalls betrachtet. Abschließend werden, unter Einbezug der Anforderungen aus Abschnitt 2.6.4, die MFA-Ansätze hinsichtlich ihrer Eignung in vollvermaschten Authentifizierungsszenarien diskutiert und bewertet.

Wie bereits an mehreren Stellen erläutert, kann der MFA-Ansatz des **IDP-seitigen MFAs** als Idealzustand betrachtet werden, da in diesem Fall i.d.R. die Heimatorganisation des Benutzers alle Faktoren, einschließlich der Registrierung, verwaltet und die verwendete MFA-Lösung bestenfalls für sowohl interne als auch föderierte Dienste herangezogen werden kann. Jedoch würde das für Identity Provider, z.B. in eduGAIN (vgl. Szenario Inter-FIM in Abschnitt 2.3), einen enormen Ressourcenaufwand bedeuten, der bei aktuell rund 4600 Identity Providern (Stand: Ende 2021) [GÉ21b] nicht unerheblich ist. Es wird daher deutlich, dass der Verlass auf eine IDP-seitige MFA-Implementierung als alleinige Lösung nicht ausreichend ist, sondern ein Fallback MFA-Workflow, der einen externen Zweitfaktorprüfer einbezieht, im Besonderen für kleinere Einrichtungen bzw. Einrichtungen mit geringer Ressourcenkapazität attraktiv ist.

In Szenarien, wo Proxies bereits als zentrale Instanz zwischen IDPs und SPs in das Ecosystem integriert sind (vgl. Szenario Forschungsinfrastrukturen in Abschnitt 2.4), kann MFA anhand eines **MFA-Ansatzes mit Proxy zwischen IDP und SP** mit relativ überschaubarem technischen Aufwand bereitgestellt werden. In Abschnitt 3.5.2 wird daher untersucht, inwiefern ein proxy-basierter MFA-Ansatz für vollvermaschte Authentifizierungsszenarien geeignet ist.

Ein weiterer MFA-Ansatz, der in Abschnitt 3.5.3 aus Gründen der Vollständigkeit erläutert wird, ist das **SP-seitige MFA**. Jedoch ist eine Realisierung durch den Service Provider nur bedingt sinnvoll, da hier die Vorteile einer entkoppelten Benutzerverwaltung, wie sie durch FIM eingeführt wird, verloren geht und dies erneut zu potentiellen Inkonsistenten und Redundanzen führen kann.

Ferner wurden im Rahmen der GÉANT Trust & Identity Activity weitere Optionen zur Bereitstellung von MFA untersucht [HLP+17]. Dabei wurde ein Proof-of-Concept (PoC) für ein **Attribute Authority (AA) basiertes MFA** entwickelt, welcher in Abschnitt 3.5.4 analysiert wird. AAs werden innerhalb (Inter-) Föderationen verwendet, um ergänzende, ggf. dienstspezifische Attribute über einen Benutzer bereitzustellen, die sonst von der Heimatorganisation eines Benutzers nicht verwaltet werden können (z.B. Zugehörigkeit zu Forschungsprojekten).

3.5.1 MFA-Ansatz: Identity Provider seitiges MFA

Beim IDP-seitigen MFA, das zugleich als Idealzustand erachtet wird, wird der erste und zweite Faktor IDP-seitig, i.d.R. durch die Heimatorganisation des Nutzers, bereitgestellt und betrieben.[5] Dies stellt eine sehr intuitive Variante dar, da die Organisation bereits ohnehin die Identitätsdaten ihrer Nutzer verwaltet und die Authentifizierung des ersten Faktors durchführt. Da in diesem Fall auch der zweite Faktor IDP-seitig verarbeitet wird, entsteht der signifikante Vorteil, dass dieser prinzipiell sowohl für den Zugriff auf interne Anwendungen als auch für den Zugriff auf (inter-) föderierte Dienste genutzt werden kann.

Eine Registrierung und Bindung des zweiten Faktors an den Nutzer kann hier mit relativ geringem Aufwand relativ stark durchgeführt werden. Üblich ist bspw., dass der Nutzer entweder direkt mit Eintritt in die Organisation einen zweiten Faktor ausgehändigt bekommt und/oder eine Service Desk basierte Variante, bei dem sich der Nutzer, bspw. anhand seines Mitarbeiterausweises, bei dem Service Desk seiner Institution identifiziert, um so einen zweiten Faktor an seine Identität zu binden.

Auf ein UML-Sequenzdiagramm zur schematischen Darstellung einer IDP-seitigen Multi-Faktor-Authentifizierung wird an dieser Stelle verzichtet. Die lesende Person wird hierzu auf Abbildung 3.2 verwiesen, wobei der Ablaufschritt „user login“ anstelle einer Ein-Faktor-Authentifizierung hier als Authentifizierung mit mehreren Faktoren anzusehen ist.

Ferner kann zur IDP-seitigen Realisierung von MFA ein Proxy herangezogen werden. Im Gegensatz zum MFA-Ansatz mit Proxy zwischen IDP und SP in Abschnitt 3.5.2, bei dem sich der Proxy „zwischen“ (SAML) IDP und (SAML) SP befindet, ist der Proxy hier „hinter“ dem (SAML) IDP verborgen, sodass Anfragen seitens des SPs nach wie vor zuerst an den IDP gerichtet werden, der dann für MFA den Proxy und dieser wiederum die an den Proxy angeschlossene MFA-Komponente kontaktiert (vgl. Abbildung 3.11).

3.5.1.1 Proxy zur IDP-seitigen Realisierung von MFA

In diesem speziellen Fall wird ein Nutzer *nach erfolgter 1FA* anhand eines Proxy-Servers zu einer technischen Komponente weitergeleitet, die für die Authentifizierung mittels zweiten Faktors zuständig ist. Der Vorteil der Verwendung eines Proxy-Servers ist, dass an den Proxy-Server eine oder potentiell mehrere technische Komponenten zur Realisierung einer Multi-Faktor-Authentifizierung geknüpft sein können. Ein Nutzer könnte somit mehrere Faktoren bzw. Faktortypen registrieren und vielleicht, sogar dienstabhängig, unterschiedliche Faktoren verwenden. Da der Proxy hier IDP-seitig sitzt, können hier prinzipiell auch organisationsinterne Dienste abgesichert werden. Jedoch muss zur Realisierung der (SAML) IDP angepasst werden, damit die Anfragen korrekt zwischen den technischen Entitäten geroutet werden. Zwar könnte eine Art standardisiertes Proxy-Template für Identity Provider

[5] Ausnahmen können IDP-seitige, extern gehostete MFA-Lösungen, z.B. cloud-basiert, sein, wobei ein entsprechender externer Provider die Bereitstellung und Verwaltung der Zweitfaktoren übernimmt. Dieser Fall wird jedoch gleichermaßen als IDP-seitige MFA-Implementierung interpretiert, da IDP-seitig alle Faktoren zusammengeführt und als aggregierte Response an den Service Provider übermittelt werden.

bereitgestellt werden, jedoch verbliebe der Aufwand zur Etablierung von MFA (inklusive organisatorischer Prozesse) nach wie vor auf Seiten des Identity Providers.

Das UML-Sequenzdiagramm in Abbildung 3.11 stellt die Schritte bei Verwendung eines IDP-seitigen Proxies schematisch dar. Dabei kann zwischen Proxy und der technischen Komponente zur Realisierung des zweiten Faktors prinzipiell auch ein beliebiges Protokoll eingesetzt werden. Aus Gründen der Übersichtlichkeit wird die Involvierung des Browsers (i.S.v. HTTP Redirects) in der Abbildung abstrahiert.

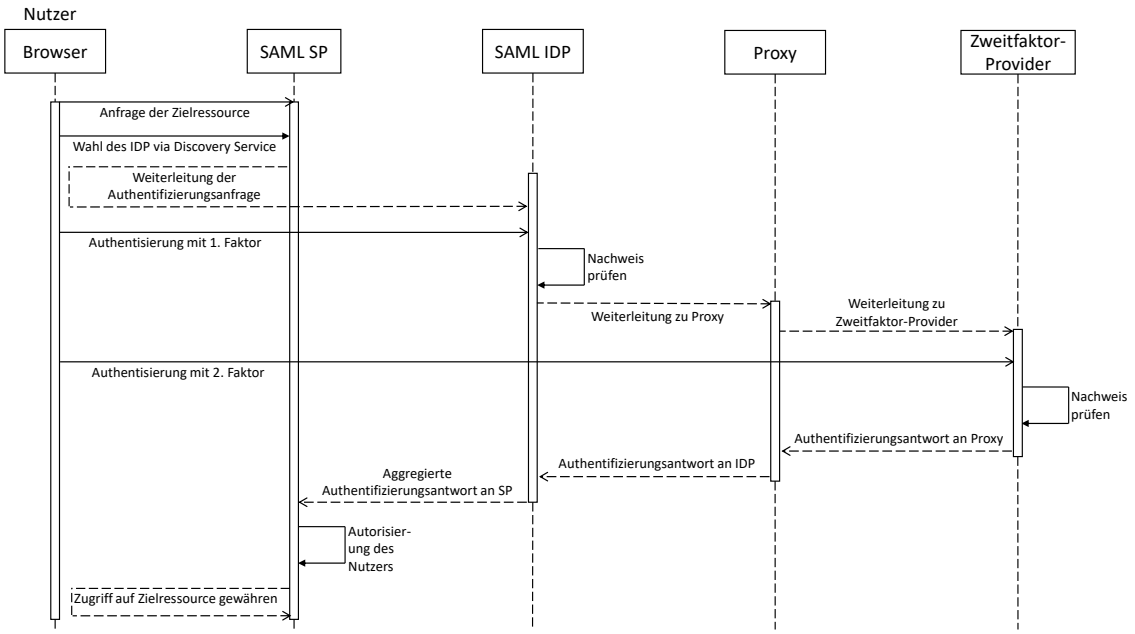


Abbildung 3.11: Schematischer Ablauf einer Multi-Faktor-Authentifizierung mit IDP-seitigem Proxy

Ergänzend zu den skizzierten MFA-Workflows wird in der nachfolgenden Auflistung ein Auszug der Softwareprodukte und Forschungsarbeiten zur IDP-seitigen MFA-Implementierung gegeben.

- Zu den Open Source Produkten, um eine existierende Authentifizierung durch einen zweiten Faktor zu verstärken, zählen bspw. LinOTP und privacyID3A. LinOTP [net20] stellt dazu eine modulare Architektur zur Verfügung, dessen zentrale Komponente der LinOTP Server ist. Es werden sowohl verschiedene Authentifizierungsfaktoren (z.B. SMS, HOTP/TOTP) als auch verschiedene Authentifizierungsprotokolle (z.B. RADIUS, SAML) unterstützt. Für SAML existiert ein LinOTP Modul für simpleSAMLphp. Ähnliche Funktionalität stellt auch privacyID3A [Net21], ein Fork von LinOTP, anhand eines modularen Authentication Servers zur Absicherung diverser Anwendungen (z.B. VPN, SSH, Web) bereit.
- Des Weiteren zählt zur IDP-seitigen MFA-Implementierung die von der U.S. amerikanischen Föderation InCommon ausgehandelte, zu vergünstigten Konditionen angebo-

tene Integration von Duo [Cis21, Int21]. Dies enthält im Besonderen die Integration von Duo mit Shibboleth Identity Providern [Shi21] als auch mit Apereo's Central Authentication Server [Ape21]. Generell bietet Duo sowohl in der Cloud gehostete (*engl. cloud-hosted*) als auch vor-Ort (*engl. on-premise*) Lösungen an. Zum Teil kommt hier ein sogenanntes Duo Access Gateway zum Einsatz, das wie ein IDP-seitiger Proxy agiert, sodass eine Abgrenzung hier nicht hundertprozentig trennscharf ist.

- Eine ähnliche Architektur wird in [SCS15] anhand eines erweiterten FIM Frameworks für sicheres MFA beschrieben. Dabei wird mittels einer OpenID konformen Architektur ein MFA as a Service (MFAaaS) konzeptioniert, dessen Ziel nicht die Bereitstellung eigener Authentifizierungsfaktoren ist, sondern auf einen transparenten Zugriff, von Third Party bereitgestellten Authentifizierungsfaktoren, abzielt. Gemäß [SCS15] könnte die MFAaaS Architektur dabei bspw. von Identity Providern sozialer Netzwerke oder Mobilfunknetzbetreibern bereitgestellt werden. MFAaaS unterscheidet zwischen zwei zentralen Komponenten, der Kernkomponente MFAS (Server), die die Logik und Ausführung von MFA implementiert sowie eines Multi-Factor Authentication Proxy (MFAP), der sich nutzerseitig, z.B. auf dem Gerät des Nutzers befindet, um lokale Authentifizierungsfaktoren auszuführen. Der high-level MFAaaS Workflow gemäß [SCS15] ist der Folgende: Ein Nutzer erfragt Zugriff auf einen Service (Schritt 1), der Service fragt ein bestimmtes Assurance Level beim MFAS an (Schritt 2), MFAS führt die dazu erforderlichen Authentifizierungen aus (Schritt 3), als letztes behauptet MFAS das Assurance Level gegenüber dem Service (Schritt 4). Die MFAaaS Architektur stellt dabei einen einheitlichen Endpunkt für Service Provider bereit (OpenID Provider) und verhält sich wie ein zentraler Identity Provider, der zur Realisierung von MFA diverse Faktoren, unter Verwendung verschiedener Interfaces, authentifiziert und, unter Berücksichtigung von Policies, die Ergebnisse der Authentifizierungen in einer Assertion an den SP kommuniziert.

3.5.2 MFA-Ansatz: Proxy zwischen IDP und SP

Eine weitere Möglichkeit zur Implementierung von MFA ist die Verwendung eines IDP-SP-Proxies, der als zentrale Vermittlungsstelle agiert und somit sowohl Anfragen empfängt, neue Anfragen versendet und Ergebnisse aggregiert. Dieser Ansatz findet häufig in Hub&Spoke Föderationen (vgl. Abschnitt 3.2.4) Anwendung, da diese ohnehin bereits auf einen zentralen Proxy zur Vermittlung zwischen SAML IDPs und SPs innerhalb einer Föderation zurückgreifen. Ein derartiger Proxy müsste somit lediglich um MFA-Funktionalität erweitert werden. Im Gegensatz zu Abschnitt 3.5.1.1, bei dem ein IDP-seitiger Proxy beschrieben wurde, zeigt der in Abbildung 3.12 skizzierte MFA-Workflow, dass der IDP-SP-Proxy bereits *vor* der Authentifizierung des ersten Faktors eingreift (d.h. Proxy zwischen IDP und SP). Im Vergleich zu Abbildung 3.11 ergeben sich somit jeweils unterschiedliche Workflows bzw. Nachrichtenflüsse.

Der Proxy und die angeschlossene MFA-Lösung wird dabei i.d.R. von einer Trusted Third Party, z.B. dem Betreiber einer R&E Föderation, betrieben. Im Hinblick auf die Registrierung der Faktoren, können dann bspw. vertrauenswürdige Vertreter aller Identity Provider

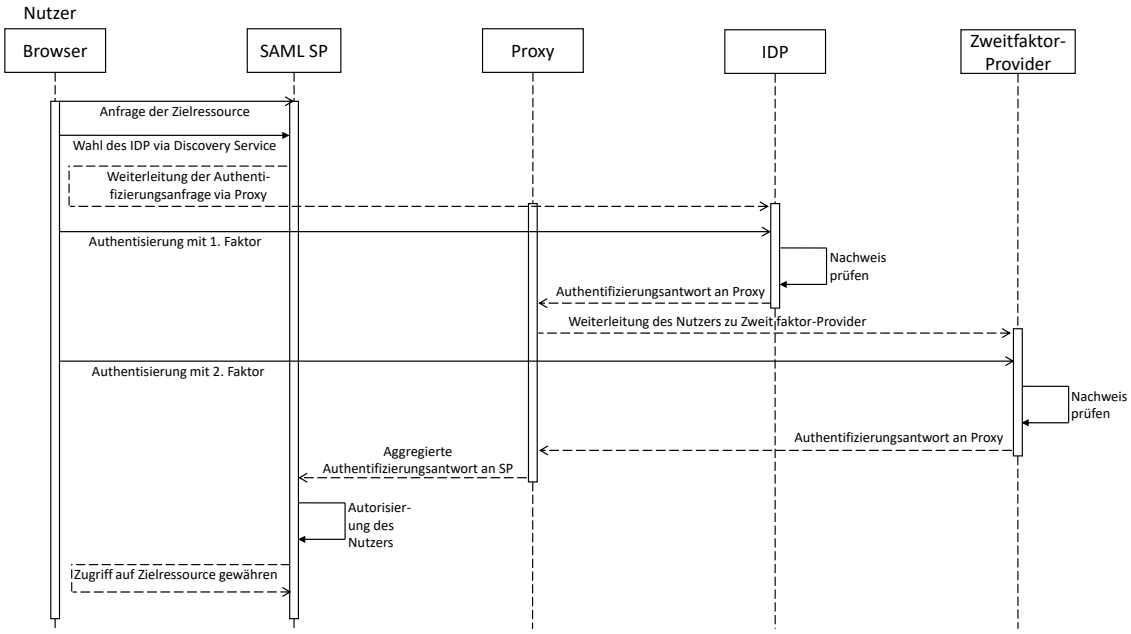


Abbildung 3.12: Schematischer Ablauf einer Multi-Faktor-Authentifizierung mit Proxy zwischen IDP und SP

die Registrierung der zusätzlichen Faktoren für ihre Nutzer vor-Ort im Auftrag des Betreibers des MFA-Proxies vornehmen. Jedoch stellt bei einem derartigen MFA-Ansatz der Proxy einen potentiellen Single-Point-of-Failure dar, weswegen dieser als besonders schützenswert gilt.

Lösungen bzw. Forschungsansätze, die auf einen proxy-basierten Ansatz zurückgreifen, werden nachfolgend kurz beschrieben.

- Zu den proxy-basierten Realisierungen zählt bspw. der durch die finnische Föderation HAKA angebotene Dienst *multi-factor authentication as a service*, dessen Source Code kostenfrei auf GitHub heruntergeladen werden kann [Laa17, CSC18]. HAKA betreibt dabei selbst eine Instanz des von ihnen entwickelten Dienstes. Gemäß [Laa17] unterstützt HAKA MFA zwei Anwendungsszenarien, die im Wesentlichen die Ansätze der Abschnitte 3.5.1.1 (IDP-seitiger Proxy) und 3.5.2 (Proxy zwischen IDP und SP) widerspiegeln. Das erste HAKA MFA Anwendungsszenario (vgl. Proxy zwischen IDP und SP) stellt das SP-initiierte MFA dar, bei dem ein SP alle Anfragen zum HAKA MFA Service weiterleitet. Der HAKA MFA Service leitet einen Nutzer dann zuerst zum Heimat-IDP weiter, danach führt der MFA Service die Authentifizierung des zweiten Faktors durch. Beim IDP-initiierten MFA von HAKA (vgl. IDP-seitiger Proxy) wird der HAKA MFA Service in den Heimat-IDP integriert. Ein Nutzer wird somit vom SP zuerst zu seinem Heimat-IDP geleitet, welcher die Authentifizierung des ersten Faktors durchführt und der dann den Nutzer inklusive seines Identifiers zum MFA Service zur Authentifizierung des zweiten Faktors weiterleitet. Bei dem durch HAKA gehos-

teten Service ist bei beiden Anwendungsszenarien die Identitätsfeststellung durch den IDP durchzuführen. Hierbei wird auf einen Registrierungscode per SMS, der dann dem MFA Service präsentiert wird, zurückgegriffen.

- Eine weitere, Open Source, proxy-basierte MFA-Lösung wird durch das niederländische NREN SURF[6] bereitgestellt. SURFsecureID, das ursprünglich unter dem Namen „Step-up authentication as-a-service“ bekannt war, ermöglicht unter Verwendung eines Proxies die Integration mit sowohl SAML IDPs, SAML SPs und anderen SAML Hubs [vdM17, SUR21b, SUR21c]. SURF betreibt dabei analog zu HAKA (s.o.) eine Instanz des von ihnen entwickelten Dienstes und stellt diesen ihren Teilnehmern zur Verfügung. Der durch SURF gehostete Service bietet hierbei zwei Optionen [SUR21c]: Für Institutionen/IDPs sowie für Service Provider. Bei der Option für Institutionen können bspw. interne (Cloud) Dienste abgesichert werden, indem der existierende 1FA-Login durch einen zweiten Faktor ergänzt wird. Die Option wird daher als „Second Factor Only“ bezeichnet und weist aufgrund des verwendeten SURFSecureID-Gateways Analogien zum IDP-seitigen Proxy aus Abschnitt 3.5.1.1 auf. Bei der gehosteten Option für Service Provider, vergleichbar mit dem aktuellen Abschnitt (d.h. Proxy zwischen IDP und SP, siehe Abbildung 3.12), ist das SURFsecureID-Gateway mit dem zentralen Föderationsproxy von SURF verknüpft, sodass ein Nutzer zuerst via Föderationsproxy zu seiner Heimatorganisation zur Authentifizierung mit dem ersten Faktor geleitet wird und dann über den Föderationsproxy und das SURFsecureID-Gateway die Authentifizierung des zweiten Faktors durchführt. Der Föderationsproxy, im Falle von SURF das sogenannte SURFconext, implementiert in diesem Fall die Policy-Entscheidungen wann und wofür MFA benötigt wird.
- Des Weiteren wird in [KFI10] ein äquivalentes Vorgehen unter Verwendung eines sogenannten IDP-Proxies zur Implementierung einer starken Authentifizierung in Identitätsföderationen vorgeschlagen. Um das angefragte Authentication Level zufriedenzustellen, kombiniert der IDP-Proxy, der als Mediator zwischen SP und IDPs agiert, die Authentifizierungen der dazu erforderlichen IDPs. Dazu wird ein IDP-Auswahlalgorithmus spezifiziert, der zwischen angefragtem, vorgeschlagenem und aktuellem Authentication Level unterscheidet.

3.5.3 MFA-Ansatz: Service Provider seitiges MFA

Aufgrund der Eigenschaften der delegierten Benutzerauthentifizierung in FIM stellt der SP-seitige MFA-Ansatz eine eher unübliche Variante dar. Bei diesem MFA-Ansatz implementiert der Service Provider die Realisierung des zweiten Faktors selbst. Das bedeutet konkret, dass der Service Provider eine Art vereinfachte Benutzerverwaltung betreiben muss, anhand derer er wiederkehrende Nutzer und die von ihm bereitgestellten Zweitfaktoren verwaltet. Würde jeder Service Provider MFA selbst implementieren, hätte dies somit zur Folge, dass ein Nutzer pro Dienst einen dedizierten zweiten Faktor registrieren muss. Ferner profitiert dieser Ansatz, im Vergleich zum IDP-seitigen Ansatz, höchstwahrscheinlich nicht von einer

[6] kurz für: *Samenwerkende Universitaire Reken Faciliteiten*

Vor-Ort-Identitätsfeststellung und Registrierung des zweiten Faktors, da ein Dienst eines föderierten oder interföderierten Szenarios üblicherweise an einem anderen Ort betrieben wird als sich die Heimatorganisation eines Nutzers befindet.

Da der SP-basierte MFA-Ansatz nur aus Gründen der Vollständigkeit erläutert wurde und den FIM-Prinzipien grundsätzlich entgegen steht, wird an dieser Stelle auf konkrete Implementierungsbeispiele verzichtet.

3.5.4 MFA-Ansatz: Attribute Authority (AA) basiertes MFA

Der letzte, zur Realisierung einer Multi-Faktor-Authentifizierung skizzierte Ansatz, stellt der **Attribute Authority (AA) basierte Ansatz** dar [GÉ17c, HLP+17].[7]

Bei dem AA-basierten MFA-Ansatz handelt es sich um einen PoC, der im Rahmen des GÉANT-Projektes entwickelt wurde, weswegen hier im Gegensatz zu den vorherigen Abschnitten, noch kein Beispiel aus dem Produktivbetrieb genannt werden kann.

Im Gegensatz zu dem MFA-Ansatz mit Proxy zwischen IDP und SP aus Abschnitt 3.5.2 verzichtet der AA-basierte Ansatz auf die Verwendung eines zentralen Proxies.[8] Hier ist stattdessen ein separater SAML SP (kurz: SAS SP) sowie ein SAML Identity Provider (SAS IDP) plus SAML Attribute Authority vorgesehen. Diese Komponenten können dann von einer dedizierten Trusted Third Party, z.B. eines Betreibers einer Identitätsföderation, betrieben werden.

Der allgemeine Ablauf des AA-basierten Ansatzes bei einem SP-initiierten Flow ist der Folgende. Auch hier gilt, wenn die Heimatorganisation des Nutzers bereits MFA implementiert und dies entsprechend kommuniziert, ist ein „Umweg“ über die Attribute Authority nicht notwendig. Andernfalls sieht der AA-basierte Workflow gemäß [GÉ17c] folgendermaßen aus:

- Nachdem ein SAML SP den Nutzer zu seinem SAML IDP weitergeleitet hat, authentifiziert sich der Nutzer mit seiner regulären Kombination aus Benutzername und Passwort. Aufgrund des Fehlens von MFA wird dem Nutzer eine Fehlerseite angezeigt, die dem Nutzer signalisiert, dass eine Multi-Faktor-Authentifizierung benötigt wird.
- Auf der Fehlerseite befindet sich ein Link zu dem innerhalb diesen Ansatzes notwendigen SAS SPs zu dem der Nutzer nach Klicken auf den Link weitergeleitet wird. Der SAS SP ist mit dem SAS IDP fest verdrahtet, sodass sich der Nutzer nun am SAS IDP mit seinem zuvor registrierten zweiten Faktor (z.B. TOTP Token) authentifizieren kann.

[7] Zur Erinnerung, **Attribute Authorities (AAs)** werden innerhalb eines föderierten Szenarios dafür verwendet, ergänzende, ggf. dienstspezifische Attribute über einen Benutzer bereitzustellen, die sonst von der Heimatorganisation eines Benutzers nicht verwaltet werden können (z.B. Zugehörigkeit zu Forschungsprojekten).

[8] Gemäß MFA-Ansatz mit Proxy zwischen IDP und SP führt der Proxy selbst keine Authentifizierungen durch, sondern leitet einen Nutzer lediglich zu den entsprechenden technischen Entitäten weiter. Gegensätzlich dazu übernimmt beim AA-basieren Ansatz der SAS IDP die Authentifizierung des zweiten Faktors.

- Nach erfolgreicher Authentifizierung wird der Nutzer zum eigentlichen Dienst zurück geleitet, der daraufhin eine Attributanfrage bei der AA stellt, deren Antwort das auf MFA gesetzte Attribut enthält.
- Sofern der gesamte Vorgang innerhalb eines festen Zeitrahmens (ca. 5-6 Minuten) stattfindet, erhält der Nutzer Zugriff auf den Dienst.

3.5.5 Abgleich mit den Anforderungen

Nachdem die Forschungsansätze und die damit verbundenen MFA-Workflows zur Realisierung einer Multi-Faktor-Authentifizierung in FIM präsentiert wurden, werde diese im nächsten Schritt gegen die Anforderungen aus Abschnitt 2.6.4 abgeglichen. Die Evaluation des MFA-Ansatzes mit Proxy zwischen IDP und SP basiert dabei auf den Dokumentationen der SURF und HAKA Implementierungen (vgl. Abschnitt 3.5.2), während das AA-basierte MFA (vgl. Abschnitt 3.5.4) in einer Testumgebung aufgesetzt und überprüft wurde.

Da das IDP-seitige MFA (siehe Abschnitt 3.5.1), wie bereits mehrfach erläutert, den Idealzustand gemäß der drei Szenarien aus Kapitel 2 darstellt und das SP-seitige MFA nur aus Gründen der Vollständigkeit dargestellt wurde und dieses dem FIM-Konzept mit delegierter Benutzerverwaltung konträr entgegensteht, wird an dieser Stelle auf eine Evaluation dieser Ansätze verzichtet. Als nächstes werden daher zuerst die verbleibenden MFA-Ansätze gegen die drei essentiellen Anforderungen abgeglichen, da deren Erfüllung als elementar gilt.

Hierbei zeigt sich, dass die beiden Ansätze die Anforderung [FA_Koexistenz] erfüllen, da der Fallback MFA-Workflow jeweils nur initiiert wird, wenn IDP-seitig kein MFA bereitgestellt werden kann. Mit Blick auf die essentielle Anforderung [NFA_Integrierbarkeit] zeigt sich, dass diese durch den MFA-Ansatz des AA-basierten MFAs erfüllt wird, während sie von MFA-Ansatz mit Proxy zwischen IDP und SP nicht erfüllt wird. Der Grund der Nichterfüllung liegt darin, dass rein technisch ein Proxy mit MFA-Fähigkeit gemäß Abschnitt 3.5.2 zwar in ein vollvermaschtes Szenario zwischen IDP und SP integrierbar wäre, dies jedoch grundlegende Änderungen am Grundsatz der Föderationsarchitektur erfordern würde, da IDPs und SPs dann nicht mehr direkt, sondern über den Proxy als „Umweg“ kommunizieren müssten. Es wäre zwar denkbar, dass nur die SPs, die MFA erfordern, zusammen mit denjenigen IDPs, die kein MFA bereitstellen, an einen Proxy angeschlossen werden, jedoch hätte dies, technisch betrachtet, eine neue Föderation zur Folge, da sich eine Föderation letztendlich über die Metadaten definiert. Die Anforderung [NFA_Skalierbarkeit] gilt demgegenüber jedoch als erfüllt, da die Ansätze prinzipiell auf verschiedene Ebenen skalierbar sind, auch wenn architekturbedingt (vgl. Anforderung [NFA_Integrierbarkeit]) der Ansatz nicht zwangsweise das beste Mittel der Wahl sein muss. Der technische Einrichtungsaufwand (vgl. [NFA_Einrichtungsaufwand]) wird bei beiden Ansätzen, unter der Annahme, dass diese jeweils as-a-Service betrieben und gewartet werden, sowohl IDP-seitig als auch SP-seitig als gering eingeschätzt. Sowohl bei der Softwarekomponente IDP als auch SP müsste die Konfiguration entsprechend angepasst werden, sodass eine korrekte Weiterleitung zwischen den Entitäten stattfindet. In diesem Zuge wird auch die Anforderung [FA_Konformität] von beiden Ansätzen erfüllt, da sich sowohl Proxy als auch AA gegenüber dem SP als spezia-

lisierter IDP verhalten. Da bei dem AA-basierten MFA-Ansatz SP-seitig etwas mehr Einrichtungsaufwand erforderlich ist (u.a. Konfiguration Attribute Query und Fehlerseite, vgl. Abschnitt 3.5.4) wird die Anforderung an dieser Stelle nur als teilweise erfüllt bewertet. Der organisatorische Einrichtungsaufwand zur Etablierung der Verfahren (z.B. Binden des Zweitfaktors an den Nutzer) wurde hier nicht berücksichtigt, da dies nicht generalisiert bewertbar ist und auch der AA-basierte MFA-Ansatz über die organisatorischen Verfahren keine Aussagen trifft. Bei den beiden Ansätzen gilt die Anforderung [NFA_Realisierbarkeit] als erfüllt, da beide Ansätze sowohl in Shibboleth als auch SimpleSAMLphp realisiert werden können. Die beiden Softwareprodukte wurden in Abschnitt 3.2.3 beschrieben und zählen momentan zur Standardsoftware in R&E. Auch [NFA_Unabhängigkeit] gilt bei beiden als erfüllt, da die Ansätze nicht auf einen spezifischen IDP bzw. SP zugeschnitten sind. Ein Nutzer könnte somit einen Zweitfaktor beim entsprechenden Dienst registrieren und somit auf alle MFA-erfordernden SPs zugreifen, die den entsprechenden Ansatz unterstützen. Hinsichtlich der Benutzererfahrung (vgl. [FA_Benutzbarkeit]) wird bei dem MFA-Ansatz mit Proxy zwischen IDP und SP die Anforderung als erfüllt bewertet, während der AA-basierte MFA-Ansatz diese nur teilweise erfüllt. Dies lässt sich darauf zurückführen, dass beim AA-basierten MFA ein Benutzer zwar frühzeitig eine Fehlermeldung bekommt (wodurch die Anforderung [FA_Fehlerbehandlung] erfüllt wird), der Workflow aber aufgrund der vielen Weiterleitungen (*engl. redirects*) etwas umständlich erscheint. Die Erfüllung der Anforderung [FA_Dynamik] und [SIA_Faktorprüfung] ist bei dem MFA-Ansatz mit Proxy zwischen IDP und SP von der Implementierung abhängig und wird vom AA-basierten MFA-Ansatz nicht erfüllt. Zwar können beim AA-basierten MFA hinsichtlich der [FA_Dynamik] und unter der Annahme, dass mehrere AAs mit derartiger Funktionalität in einer Infrastruktur (z.B. Interföderation) bereitgestellt werden, mehrere Attributanfragen an verschiedene AAs gestellt werden, jedoch kann hier, soweit festgestellt wurde, keine Auswahl durch den Benutzer erfolgen. Aufgrund des statischen Charakters findet im PoC auch keine Überprüfung der Authentifizierungsfaktoren statt. Während [SIA_Vertraulichkeit] von beiden Ansätzen als erfüllt bewertet wird, gilt die Anforderung [DSA_Datenminimalisierung] von dem MFA-Ansatz mit Proxy zwischen IDP und SP als nicht erfüllt, da nun die gesamte Kommunikation über den Proxy laufen muss, sodass die Informationen aus verschiedenen Quellen zusammengeführt und an einen SP übermittelt werden können. Die Anforderung [FA_Messbarkeit] ist beim MFA-Ansatz mit Proxy zwischen IDP und SP zwar implementierungsabhängig, jedoch wird diese an dieser Stelle als erfüllt erachtet, da Statistiken aufgrund des zentralen Proxies leicht gesammelt werden können.

Abschließend bewertet und unter Berücksichtigung der Gewichtung G(p) zeigt sich, dass der AA-basierte MFA-Ansatz für vollvermaschte Szenarien als die geeignetere Variante scheint. Bei dem MFA-Ansatz mit Proxy zwischen IDP und SP fällt besonders die Nichterfüllung der Anforderung [NFA_Integrierbarkeit], die als elementar gilt, stark ins Gewicht. Im Gegensatz zum MFA-Ansatz mit Proxy zwischen IDP und SP hat der AA-basierte MFA-Ansatz v.a. Schwächen hinsichtlich der Dynamik, Benutzbarkeit und Faktorprüfung. In den folgenden Kapiteln wird daher ein Fallback MFA-Workflow erarbeitet, der die Grundprinzipien des AA-basierten Ansatzes wiederverwendet, d.h. Verzicht auf eine zentrale Instanz, stattdessen SP-seitiges Triggern des Fallback MFA-Workflows. Einen derartigen Fallback MFA-Workflow gibt es, soweit nach ausführlicher Literaturrecherche bekannt, derzeit nicht.

Tabelle 3.3: Abgleich mit existierenden MFA-Ansätzen

Anforderung	**Gewichtung**	**MFA-Ansatz: Proxy zwischen IDP und SP**	**MFA-Ansatz: AA-basiertes MFA**
[NFA_Integrierbarkeit]	(4)	✗	✓
[FA_Koexistenz]	(4)	✓	✓
[NFA_Einrichtungsaufwand]	(4)	IDP: ✓ SP: ✓	IDP: ✓ SP: (✓)
[NFA_Realisierbarkeit]	(2)	✓	✓
[NFA_Unabhängigkeit]	(2)	✓	✓
[FA_Dynamik]	(2)	i.a.	✗
[SIA_Faktorprüfung]	(2)	i.a.	✗
[NFA_Skalierbarkeit]	(2)	✓	✓
[FA_Benutzbarkeit]	(2)	✓	(✓)
[DSA_Datenminimalisierung]	(2)	✗	✓
[SIA_Vertraulichkeit]	(2)	✓	✓
[FA_Messbarkeit]	(1)	✓	(✓)
[FA_Fehlerbehandlung]	(1)	i.a.	✓
[FA_Konformität]	(1)	✓	✓
$G(p) = \sum w \cdot p$	G(p) max 62	45	49

✓: Anforderung erfüllt (2 Punkte)
(✓): Anforderung teilweise erfüllt (1 Punkt)
i.a.: Implementierungsabhängig, daher nicht generalisiert bewertbar (1 Punkt)
✗: Anforderung nicht erfüllt (0 Punkte)

wobei w: Gewichtung, p: Punkte und $G(p)$: Gesamtsumme Punkte

Das Ziel ist, dass v.a. Infrastrukturen mit einer hohen Quantität an Teilnehmern, die potentiell global verteilt sind, nicht an einen einzigen (externen) Zweitfaktorprüfer gebunden sind, sondern dass neben den IDPs und SPs beliebig viele Zweitfaktorprüfer existieren können, die anhand des zu spezifizierenden MFA-Workflows dynamisch bzw. flexibel kontaktiert werden können.

In diesem Zuge wird der Begriff **Two-Plus Provider** (kurz: **TPP**) eingeführt, der einen solchen externen Faktorprüfer bezeichnet. Die Bezeichnung „Two-Plus“ leitet sich daraus ab, dass der erste Faktor durch einen zweiten *oder einen weiteren Faktor* ergänzt wird; so könnte prinzipiell auch eine Zwei-Faktor-Authentifizierung um einen weiteren, d.h. einen dritten Faktor, erweitert werden.

3.6 Level of Assurance

Eng im Zusammenhang mit der Authentifizierung steht auch das Konzept der **Level of Assurance (LoA)**, welches in diesem Abschnitt weiter präzisiert wird. Dazu werden in Abschnitt 3.6.1 LoA-Normen und -Standards betrachtet, meist umfangreiche Dokumente mit einer Vielzahl von Anforderungen; während in Abschnitt 3.6.2 einige konkrete Implementierungen in R&E Föderationen erläutert werden.

Der Begriff Level of Assurance, in deutsch z.T. auch mit **Verlässlichkeitsklassen** oder **Vertrauensniveau** übersetzt, beschreibt ein Konzept, das im Zusammenhang von Identitäten und Authentifizierungen verwendet wird, um eine Aussage über die Qualität bzw. den Grad der Verlässlichkeit von Identitäten (engl. *identity assurance*) sowie Authentifizierungen (engl. *authentication assurance*) zu treffen. LoA beschreibt den Grad des Vertrauens (Trust), dass eine vorgelegte Behauptung zusätzlich mit Beweisen versehen ist, um zu zeigen, dass sie wahr ist [LDA19]. In SAML könnte dementsprechend eine SAML Assertion mit zusätzlichen Informationen angereichert werden, die Rückschlüsse über die Art und Weise, wie Identitäten verwaltet und Authentifizierungen durchgeführt werden, geben.

Im Rahmen der **Identity Assurance** werden all jene Prozeduren betrachtet, die sich mit dem Management von Identitäten beschäftigen [GGF17b]. Dazu zählen bspw. die oben beschriebene Identitätsfeststellung (vgl. Abschnitt 3.4.4), das Ausstellen und das Management von Credentials inklusive deren Erneuerung (*engl.: credential renewal*) und das Ersetzen von Credentials.

Die **Authentication Assurance** deckt Kriterien und Prozeduren hinsichtlich der Authentifizierung ab [GGF17b]. Dazu zählen z.B. Kriterien über Authentifizierungsfaktoren (z.B. Passwortlänge, -komplexität), deren verifizierende Stellen, aber auch Prozeduren, was bei dem Verlust bzw. Vergessen eines Authentifizierungsfaktors zu tun ist.

LoA-Konzepte sind v.a. dann von zentraler Bedeutung, sobald die Prozesse der Authentifizierung und Autorisierung (vgl. FIM) voneinander entkoppelt sind und eine Entität eine Zugriffsentscheidung auf Basis einer delegierten Authentifizierung treffen muss. LoA-Konzepte beziehen sich dabei nicht primär auf personenbezogene Daten bzw. Attribute, sondern geben

eine Aussage über die Qualität der zugehörigen Metadaten, bspw. der durchgeführten Identitätsfeststellung (z.B. keine versus Vor-Ort-Identitätsfeststellung) oder Authentifizierung (z.B. Passwortstärke).

LoA-Standards existieren bereits von bekannten, offiziellen Standardisierungsstellen wie dem National Institute of Standards and Technology (vgl. Abschnitt 3.6.1.1) oder der ISO/IEC (vgl. Abschnitt 3.6.1.2), die jedoch im Bereich der R&E Föderationen oft kaum Anwendung finden. Häufig handelt es sich bei diesen Normen um sehr umfassende Industriestandards (vgl. z.B. NIST-Standard mit rund 250 Seiten), die aufgrund strikter Vorgaben nicht 1:1 in R&E Föderationen umgesetzt werden können. Daher haben viele R&E Föderationen eigene, ihren Bedürfnissen entsprechende Verlässlichkeitsklassen definiert. In Abschnitt 3.6.2 werden einige exemplarisch erläutert. Jedoch sind die dort präsentierten Verlässlichkeitsklassen föderationsspezifisch, d.h. sie finden nur in der jeweiligen Föderation Anwendung; eine föderationsübergreifende Lösung gibt es zum Zeitpunkt der Recherche nicht.

3.6.1 Level of Assurance (LoA) Normen und Standards

In diesem Abschnitt werden zunächst existierende LoA-Normen und -Standards betrachtet. Dabei handelt es sich um Standards, die von Standardisierungsstellen wie der NIST oder der ISO/IEC herausgegeben wurden. Desweiteren werden die EU-Verordnung eIDAS, das Identity Assurance Framework der Kantara Initiative sowie Vectors of Trust, ein vorgeschlagener Standard der IETF, betrachtet.

3.6.1.1 NIST Special Publication 800-63 Version 3 Digital Identity Guidlines

Die Special Publication 800-63 Suite [Nat17] ist ein Rahmenwerk des National Institute of Standards and Technology (NIST). Es wurde ursprünglich für U.S. Bundesbehören entwickelt, wurde jedoch aufgrund zunehmender Anwendungsfälle an nationale und internationale LoA-Standards angeglichen [GGF17a]. Die NIST SP 800-63 Suite ersetzt die Vorgängerversion SP 800-63-2 [BDN+13] und ist ein umfassendes Rahmenwerk, das mit der Version 3 erstmals in vier Dokumente aufgeteilt ist. Das Dokument SP 800-63-3 [GGF17b] ersetzt die Kapitel 1 bis 4 der SP 800-63 Version 2 und befasst sich einerseits mit allgemeinen, informativen Aspekten (Zweck, Einleitung, Definitionen und Abkürzungen, Digital Identity Model etc.) und andererseits mit einem normativen Teil. In diesem Dokument werden erstmals die Assurance-Komponenten eingeführt und folgendermaßen unterteilt:

- Identity Assurance Level (IAL)
- Authentication Assurance Level (AAL)
- Federation Assurance Level (FAL)

Gemäß dieser Einteilung orientiert sich auch die Struktur der weiteren Dokumente. NIST SP 800-63A *Enrollment and Identity Proofing Requirements* [GFL+17] beschreibt drei Identity Assurance Level und die damit verbundenen Prozeduren und Anforderungen. Folgende Auflistung fasst kurz und knapp IAL 1 bis IAL 3 zusammen:

- IAL 1: keine Verbindung zu einer realen Identität notwendig
- IAL 2: Angemessene Beweise vorhanden, dass eine Identität mit einer Person der realen Welt assoziiert werden kann
- IAL 3: Physische Anwesenheit zur Identitätsfeststellung notwendig

NIST SP 800-63B *Authentication and Lifecycle Management* [GFN+17] beschreibt analog zu den drei IALs drei Assurance Level zur Authentication Assurance (AAL 1 bis AAL 3):

AAL1 verkörpert eine geringe Authentication Assurance, wobei eine Ein-Faktor-Authentifizierung ausreichend ist.

AAL2 bietet eine hohe Authentication Assurance, u.a. durch Verwendung zwei verschiedener Authentifizierungsfaktoren, einem sicheren Protokoll sowie kryptografischen Mitteln.

AAL3 bietet eine sehr hohe Authentication Assurance und fordert darüber hinaus einen Hardware-basierten Faktor sowie einen weiteren zum Schutz vor Impersonation.

Das letzte Dokument NIST SP 800-63C *Federations and Assertions* [GRS+17] liefert Richtlinien zur Nutzung von föderierten Identitäten sowie für Assertions zur Implementierung von Identitätsföderationen. Analog zu den zuvor beschriebenen Dokumenten gibt es auch hier drei Assurance Level (FAL1 bis FAL3):

- FAL1: Bearer Assertion,[9] signiert vom Identity Provider
- FAL2: Bearer Assertion, signiert vom Identity Provider, verschlüsselte Assertion zum Service Provider
- FAL3: Nutzung einer Key Assertion, signiert vom Identity Provider, verschlüsselte Assertion zum Service Provider

Die gesamte Dokumenten-Suite ist mit circa 250 Seiten äußerst umfangreich. Darüber hinaus verweist die Dokumentation z.T. auf weitere Standards und definiert somit einen strikten Raum zur Implementierung der Anforderungen.

3.6.1.2 ISO/IEC 29115:2013

Die internationale Norm ISO/IEC 29115:2013 *Information technology – Security techniques – Entity authentication assurance framework* [ISO13b] spezifiziert ein Framework zum Management der Authentication Assurance von Entitäten und bezieht sich dabei auf sämtliche Prozesse, Managementaktivitäten und Technologien in Bezug auf Identitäten im Rahmen einer Authentifizierungs-Transaktion.

Auf technischer Seite werden die drei Phasen *Enrolment phase*, *Credential management phase* und *Entity authentication phase* betrachtet, aus organisatorischer und Management-Sicht kommen u.a. Kriterien zur rechtlichen und vertraglichen Einhaltung, zur Service Etablierung und externen Servicekomponenten hinzu. [ISO13b]

[9] Gemäß [GGF17b] eine Assertion wobei deren Besitz als Identitätsnachweis ausreichend ist.

Die Norm, bei der es sich um einen gemeinsamen Standard mit der International Telecommunication Union handelt (ITU-T X.1254 [Int12]), spezifiziert insgesamt vier LoAs und ist im Vergleich zur NIST SP 800-63-3 mit weniger als 40 Seiten deutlich übersichtlicher gehalten:

- Level 1 - Low: Geringes oder kein Vertrauen in die behauptete Identität
- Level 2 - Medium: Ein gewisses Vertrauen in die behauptete Identität
- Level 3 - High: Hohes Vertrauen in die behauptete Identität
- Level 4 - Very high: Sehr hohes Vertrauen in die behauptete Identität

Level 1 stellt kaum Anforderungen an den Authentifizierungsmechanismus (z.B. keine kryptographischen Maßnahmen notwendig) und für Level 2 ist eine Ein-Faktor-Authentifizierung ausreichend. Ab Level 3 ist eine Multi-Faktor-Authentifizierung erforderlich. [Int12]

3.6.1.3 EU-Verordnung eIDAS

eIDAS (kurz für: *Electronic Identification, Authentication and Trust Services*) ist eine EU-Verordnung mit der Nr. 910/2014 [Eur14] des Europäischen Parlaments und des Rates, die die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt regelt, mit dem Zweck eine Vereinfachung und Interoperabilität auf europäischer Ebene herzustellen. eIDAS berücksichtigt dazu u.a. die zuvor beschriebene internationale ISO-Norm 29115 und definiert gegensätzlich dazu nur drei Level of Assurance. Diese werden in eIDAS äquivalent auch als „Sicherheitsniveau“ bezeichnet. Unterschieden wird dabei zwischen den folgenden Niveaus:

- niedrig: begrenztes Vertrauensmaß
- substanziell: substanzielles Vertrauensmaß
- hoch: höheres Vertrauensmaß

Die (Mindest-) Anforderungen zur Erfüllung der hierarchischen Niveaus sind in der Durchführungsverordnung (EU) 2015/1502 [Eur15a] der Kommission vom 8. September 2015 festgeschrieben. Zur Erfüllung eines Sicherheitsniveaus sind Kriterien aus den folgenden Bereichen zu berücksichtigen:

- Anmeldung: einschließlich Beantragung und Eintragung, Identitätsnachweis und -überprüfung sowie Verknüpfung von elektronischen Identifizierungsmitteln bei natürlichen und juristischen Personen
- Verwaltung elektronischer Identifizierungsmittel: einschließlich Merkmale und Gestaltung elektronischer Identifizierungsmittel, Ausstellung, Auslieferung und Aktivierung, Aussetzung, Widerruf und Reaktivierung sowie Verlängerung und Ersetzung
- Authentifizierung: einschließlich des Authentifizierungsmechanismus

- Management und Organisation: einschließlich Allgemeinen Bestimmungen, Veröffentlichte Bekanntmachungen und Benutzerinformationen, Informationssicherheitsmanagement, Aufbewahrungspflichten, Einrichtungen und Personal, Technische Kontrollen sowie Einhaltung und Prüfung

Der Fokus der Durchführungsverordnung liegt im Besonderen auf der elektronischen Identifizierung, während die Anforderungen an die Authentifizierung und den Authentifizierungsmechanismus äußert knapp gehalten sind. Hier fällt auf, dass keine konkreten Anforderungen an verwendete Authentifizierungsfaktoren definiert sind (z.B. minimale Passwortlänge, maximale Gültigkeit TOTP). Jedoch werden bereits ab dem Vertrauensniveau „substanziell“ unabhängige interne oder externe Prüfungen (Audits) gefordert.

3.6.1.4 Kantara Identity Assurance Framework

Die Kantara Initiative ist ein gemeinnütziger Industrieverband, der ein Identity Assurance Framework (IAF) basierend auf der NIST SP 800-63 Version 2 entwickelt hat. Das IAF kapselt zum einen Anforderungen der NIST und ergänzt diese durch von Kantara definierten Anforderungen. Das IAF ist auch unter dem Namen *Kantara Classic* bekannt, welches die erste Implementierung des IAF darstellt. Kantara Classic ist Teil des Kantara Trust Framework und ermöglicht Organisationen des öffentlichen und privaten Sektors, sich gemäß der *Kantara Service Assessment Criteria* (SAC) zertifizieren zu lassen. [Kan19c]

Daher stellt die Kantara Initiative auch Dokumentation zur Akkreditierung von Gutachtern, deren erforderliche Qualifikationen, Anforderungen und Kompetenzen bereit. Sämtliche Dokumentation zum IAF ist Teil des *Controlling Document Sets* [Kan19a].

Analog zur NIST stellt auch Kantara allgemeine Dokumentation (z.B. *IAF Overview*, *IAF Glossary*) bereit. Ein Überblick über die vier IAF Level of Assurance basierend auf der NIST ist in dem Dokument KIAF-1200 [Kan10] beschrieben. Die konkreten IAF-Anforderungen sind Teil des SAC-Sets. In KIAF-1410 [Kan18a] sind allgemein anwendbare Service Assessment Criteria beschrieben, in KIAF-1420 [Kan20] operationale SAC basierend auf NIST 800-63 Version 2. Die operationalen SAC sind dabei in sechs Teile untergliedert (Part A - Part F) [Kan20]:

- Part A - Credential Operating Environment
- Part B - Credential Issuing
- Part C - Credential Renewal and Re-issuing
- Part D - Credential Revocation
- Part E - Credential Status Management
- Part F - Credential Verification/Authentication

Jeder Part wird pro Assurance Level 1 bis 4 aufgegriffen und listet die entsprechenden Anforderungen auf.

Die neue, dritte Version der NIST 800-63 greift Kantara in den Dokumenten KIAF-1430 [Kan19b] und KIAF-1440 [Kan18b] auf. Die Zertifizierung gemäß dieser Dokumente (Trust Mark *Kantara.next.gen*) ist ebenfalls Teil des übergreifenden Kantara Trust Framework.

3.6.1.5 Vectors of Trust

Vectors of Trust (VoT) [RJ18] ist ein vorgeschlagener Standard, der aus der Internet Engineering Task Force (IETF) stammt. VoT greift dabei auf die Aussage zurück, dass ein einfacher (numerischer) Wert, wie z.B. Level 1 oder „low“, zur Repräsentation eines Vertrauenslevels zwar einfach zu verarbeiten und zu vergleichen ist, dies jedoch Szenarien aus der realen Welt nur schlecht abbilden kann. Aus diesem Grund schlägt VoT einen Ansatz basierend auf Vektoren vor, der die verschiedenen Aspekte innerhalb einer Transaktion als orthogonale Aspekte betrachtet und somit ermöglicht, dass die Aspekte voneinander unabhängig behauptet werden können. Ein ähnlicher Ansatz findet bereits in der aktuellen NIST Version 3 Anwendung, die zwischen Komponenten bzw. Leveln zur Identity Assurance (IAL), Authentication Assurance (AAL) und Federation Assurance (FAL) unterscheidet.

Die momentan aktuelle Version von VoT unterscheidet zwischen vier orthogonalen Komponenten [RJ18]:

- Identity Proofing (P)
- Primary Credential Usage (C)
- Primary Credential Management (M)
- Assertion Presentation (A)

Jeder Komponente ist dabei ein eindeutiger sog. *demarcator* zugewiesen (P, C, M, A). Um den Wert einer Komponente auszudrücken, wird empfohlen, dass für natürliche Ordnungen eine Ziffer und für andere Fälle Kleinbuchstaben verwendet werden. Hier kann entweder auf die Werte der VoT Spezifikation zurückgegriffen oder eigene, spezifischere Werte definiert werden. Gemäß VoT repräsentiert „P0“ bspw. eine Identitätsfeststellung, bei der keine Überprüfung stattgefunden hat.

Insgesamt zeigt sich, dass der Fokus von VoT auf der vektorbasierten Architektur liegt und weniger auf der Definition konkreter Werte, da die durch VoT bereitgestellten Werte nicht Teil der eigentlichen Spezifikation sind, sondern in den Appendix A ausgelagert wurden. Dazu kommt, dass die aufgelisteten Werte sehr high-level definiert sind und je nach Anwendungsfall weiter konkretisiert werden müssen.

3.6.2 Level of Assurance in R&E

Dieser Abschnitt beschreibt exemplarisch die LoA-Konzepte der deutschen Identitätsföderation DFN-AAI, der amerikanischen Föderation InCommon sowie die Profiles of Authentication Assurance der Grid-Infrastruktur (IGTF).

Generell sind die von den Föderationen entwickelten Assurance Level und Profile auf die jeweiligen Bedürfnisse der entsprechenden Föderation zugeschnitten und sind somit äußerst föderationsspezifisch. Sie finden dementsprechend nur in der jeweiligen Föderation Anwendung und werden länderübergreifend i.d.R. nicht interpretiert. Aus diesem Grund wird auf die detaillierte Darstellung weiterer LoA-Konzepte anderer Föderationen verzichtet.

Darüber hinaus ist zu erwähnen, dass eine Vielzahl von Föderationen in eduGAIN keine eigenen Assurance Level definiert und im Einsatz haben. Auch die Interföderation eduGAIN hat zum Zeitpunkt der Recherche keine föderationsübergreifenden Assurance Level definiert.

3.6.2.1 DFN-AAI Verlässlichkeitsklassen

Die deutsche Föderation DFN-AAI definiert drei Klassen der Verlässlichkeit [DFN17]: *Test*, *Basic* und *Advanced*. Wie der Name bereits indiziert, ist die Klasse Test lediglich für Testzwecke vorgesehen; für den produktiven Betrieb stehen in der DFN-AAI effektiv die beiden Klassen Basic und Advanced zur Verfügung. Die Zuordnung zu einer Klasse erfolgt sowohl von Seiten des Identity Providers (mittels Konformitätserklärung) als auch von Seiten des Service Providers (gemäß dem Schutzbedarf der Ressource) selbst und wird anhand von drei Kriterien ermittelt [DFN17]:

- **Identifizierung (I)**: Das Verfahren der Organisation zur Identifizierung (Basic: Identifizierung mit Rückantwort von einer eindeutigen Adresse, Advanced: persönliche Identifizierung mit amtlichem Dokument)
- **Authentifizierung (A)**: Das Verfahren der Organisation zum Ausweis einer Identität (Basic: Ausweisen anhand eindeutiger digitaler Adresse , Advanced: Ausweisen anhand personalisiertem Account mit Passwort oder Zertifikat)
- **Qualität des IdMs (D)**: Das Verfahren der Organisation zur Pflege (Datenhaltung und Prozesse) der Identitäten (Basic: Datenkorrektheit und -aktualisierung < 3 Monate, Advanced: Datenkorrektheit und -aktualisierung < 2 Wochen)

Die jeweiligen Klassen werden durch mehrere, separate SAML-Metadatensätze in der DFN-AAI realisiert.

3.6.2.2 InCommon Assurance Program

Die U.S. Föderation InCommon bietet als Teil ihres Assurance-Programms zwei Identity Assurance-Profile an: **Bronze** und **Silver** [InC13b].

Bronze ist vergleichbar mit NIST LoA 1 und beschränkt sich auf die angemessene Verlässlichkeit, dass sich bei jeder Authentifizierung hinter einer Identität bzw. einem Subject Identifier dieselbe Person verbirgt. Bronze definiert keine Anforderungen an die Identitätsfeststellung, sondern besagt lediglich, dass eine angemessene Sorgfalt bei der Ausstellung der

Credentials stattzufinden hat. Aus diesem Grund eignet sich Bronze nicht für hochkritische Dienste.

Das Assurance-Profil **Silver** ist äquivalent zu NIST LoA 2 und eignet sich für einfache finanzielle Transaktionen. Silver erweitert die Anforderungen den Bronze-Profils durch Hinzufügen von Kriterien zur Identitätsfeststellung und zu Identitätsinformations-Records. Desweiteren besitzt Silver stärkere Anforderungen an Credentials sowie deren Management.

Die Kriterien bzw. Anforderungen, die abhängig vom jeweiligen Profil erfüllt sein müssen, sind gemäß des InCommon Identity Assurance Assessment Frameworks [InC13a] in acht funktionale Bereiche unterteilt (in Englisch aufgelistet):

1. *Business, Policy and Operational Criteria*
2. *Registration and Identity Proofing*
3. *Credential Technology*
4. *Credential Issuance and Management*
5. *Authentication Process*
6. *Identity Information Management*
7. *Assertion Content*
8. *Technical Environment*

Zum Nachweis der Konformität erfordert das Silver-Profil ein Audit. Im Falle des Bronze-Profils ist ein Audit optional, notwendig ist jedoch eine Erklärung der jeweiligen Organisation, dass die Anforderungen umgesetzt sind.

Obwohl die Identity-Assurance-Profile strukturiert, durchdacht und in Anlehnung an eine ältere NIST-Version entstanden sind, findet es in der U.S. Föderation kaum Anwendung, sodass sich daraus schließen lässt, dass die von der NIST abgeleiteten Anforderungen zu komplex sind.

3.6.2.3 IGTF Profiles of Authentication Assurance

Die *Interoperable Global Trust Federation* (IGTF) ist ein Gremium, das sich mit der Etablierung von Richtlinien und Anleitungen für interoperable, globale Vertrauensbeziehungen zwischen Providern befasst. Die Community betreibt außerdem eine über mehrere Kontinente verteilte Public-Key-Infrastruktur (PKI) für Grid-Computing, wozu zum Zwecke des Ressourcenzugriffs ebenfalls mehrere Assurance-Profile spezifiziert wurden. [IGT21]

Die als *Aspen*, *Birch*, *Cedar* und *Dogwood* bezeichneten Assurance-Profile orientieren sich dabei nicht an einem hierarchischen Modell, sondern definieren Mindestanforderungen in unterschiedlichen Bereichen [GE16]:

- Identität: einschließlich End-Identität, Subscriber und Identitätsfeststellung sowie Identifier Zuweisung

- Operationale Anforderungen: einschließlich der Kommunikation zwischen ausstellenden und registrierenden Autoritäten, Credential Prozess, Management zugewiesener Credentials, IT-System Sicherheit, Credential Stärke und Gültigkeit sowie Identifikation von Credential-Richtlinien
- Sicherheit am Standort
- Verantwortlichkeiten für Publikation und Repositories
- Audits
- Privacy und Vertraulichkeit
- Kompromittierung und Wiederherstellung bei Disastern
- Andere Verpflichtungen

Auch hier zeigt sich, dass die Assurance-Profile kontextspezifisch definiert wurden, da bspw. die Abschnitte zur Identität und zu den operationalen Anforderungen einen starken Fokus auf PKI-Gegebenheiten legen.

3.6.3 Abhängigkeiten zwischen LoA-Normen, -Standards und -Konzepten

Wie in Abschnitt 3.6.1 verdeutlicht wurde, sind einige der dort präsentierten LoA-Normen und -Standards voneinander abhängig, bauen aufeinander auf oder ergänzen sich. In der folgenden Abbildung 3.13 wird dieser Zusammenhang grafisch veranschaulicht. Föderationsspezifische Assurance Level bzw. Profile sind hier nicht abgebildet.

Aufgrund existierender Abhängigkeiten und z.T. der Ergänzung weiterer Anforderungen, lassen sich die Assurance Level der jeweiligen LoA-Rahmenwerke nicht ohne weiteres aufeinander abbilden. Innerhalb einer NIST Draft-Version von 2017 [GGF17a] zeigt ein informatives Mapping der Level of Assurance mit anderen LoA-Rahmenwerken, dass SP 800-63 Version 3 die Anforderungen einiger anderer LoA-Standards erfüllt, eine 1:1 Korrelation jedoch nicht möglich ist. Oftmals liegen die Unterschiede bzw. Abweichungen weniger in den Prozeduren selbst sondern eher im Bereich der Rechtslage und der begleitenden Normen [Cry18].

Bezüglich der quantitativen Anzahl von Assurance Leveln wird deutlich, dass meist drei oder vier Level definiert sind. Dabei scheint die Bereitstellung einer eingeschränkten Auswahlmöglichkeit (z.B. drei Level bzw. Optionen), auch bei Betrachtung anderer Sektoren wie bspw. dem Marketing, optimal zu sein [KVB09].

3.6.4 Abgleich mit den Anforderungen

In diesem Abschnitt werden die skizzierten LoA-Normen und -Standards sowie die erläuterten LoA-Konzepte aus R&E gegen die in Kapitel 2 definierten Anforderungen abgeglichen. Die daraus resultierenden Ergebnisse sind in Tabelle 3.4 zusammengefasst dargestellt.

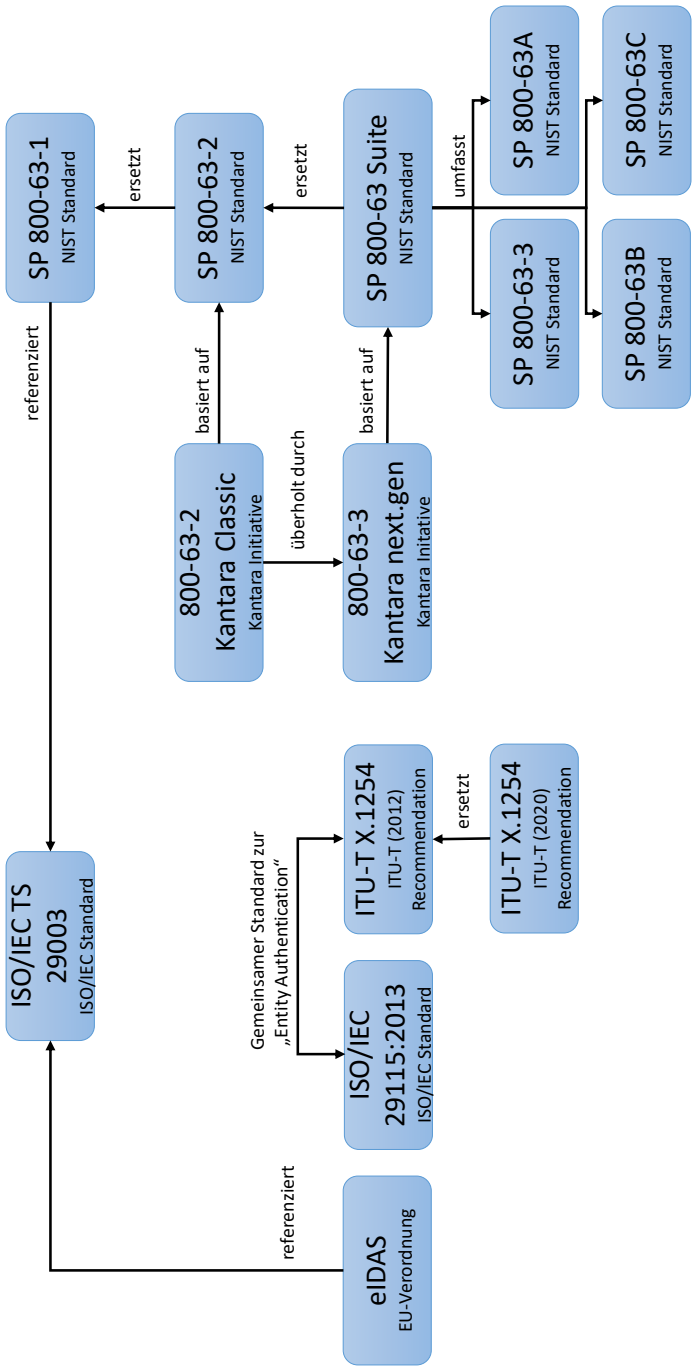


Abbildung 3.13: Zusammenhang von LoA-Standards und -Frameworks

Da die InCommon Assurance-Profile inzwischen als veraltet anzusehen sind und VoT den Fokus eher auf das Architekturkonzept legt, wird auf einen Abgleich mit den Anforderungen an dieser Stelle verzichtet. In Bezug auf Kantara erfolgt der Abgleich mit den Anforderungen gemäß des SAC-Sets für Kantara Classic. Zum Abgleich der Anforderungen des gemeinsamen Standards der ISO/IEC und ITU-T wird der Standard bzw. die Empfehlung X.1254 der ITU-T herangezogen. Hierbei wird die X.1254-Version aus dem Jahr 2012 verwendet, da die überarbeitete Version aus dem Jahr 2020 zum Zeitpunkt der Recherche noch nicht verfügbar war.

Beim Abgleich des NIST-Standards gegen die Anforderungen zeigt sich, dass die als wichtig klassifizierten Anforderungen [FA_LoA_1FA] und [FA_LoA_MFA] erfüllt werden, jedoch essentielle Anforderungen wie [NFA_LoA_Minimalität] oder [NFA_LoA_Umsetzbarkeit] aufgrund der Quantität der Spezifikation (circa 250 Seiten insgesamt) sowie der Komplexität als nicht erfüllt erachtet werden. Es zeigt sich also, dass NIST zwar jeden möglichen Aspekt der Assurance berücksichtigt, jedoch das Verhältnis zwischen angemessenem Nutzen und Aufwand eher in den Hintergrund gerückt wird.

Gegensätzlich dazu steht das Konzept der DFN-AAI Verlässlichkeitsklassen. Diese definieren zwar ein Minimum an Kernanforderungen, jedoch zeigt sich bei Betrachtung der Anforderungen [FA_LoA_1FA] und [FA_LoA_MFA], dass hier keine konkreten Anforderungen an Authentifizierungsfaktoren gestellt werden. In diesem Fall sind die Kriterien eher zu unspezifisch und müssten stattdessen feingranularer definiert sein.

Zusammenfassend zeigt sich, dass die hier evaluierten Assurance-Konzepte entweder zu umfassend sind (vgl. z.B. NIST-Standard) oder konträr dazu (vgl. DFN-AAI Verlässlichkeitsklassen) zu unspezifisch sind. Auch mit den anderen evaluierten LoA-Rahmenwerken konnte kein passendes Rahmenwerk mit Kriterien zur Authentication Assurance in angemessenem Verhältnis zwischen Aufwand und Nutzen zum Zweck der FIM-Szenarien aus Kapitel 2 identifiziert werden. Es ist daher ein Authentication-Assurance-Konzept notwendig, welches den in Kapitel 2 spezifizierten Anforderungen genügt.

Die Spezifikation eines neuen Authentication-Assurance-Konzepts rechtfertigt sich dabei im Besonderen durch die immense Größe der Interessensgruppe, die davon profitiert. In Kapitel 2 wurde dazu sowohl der Anwendungsfall eduGAIN mit über 8000 Entitäten (vgl. Szenario Inter-FIM) als auch der Anwendungsfall internationaler Forschungsinfrastrukturen verdeutlicht. Hinzu kommt, dass die Spezifikation eines Authentication-Assurance-Konzepts aus der Perspektive von R&E noch nicht föderationsübergreifend und im Detail betrachtet wurde. Ferner werden in Kapitel 6 Maßnahmen zur offiziellen Registrierung des Authentication-Assurance-Konzepts ergriffen.

Tabelle 3.4: Abgleich mit existierenden LoA-Rahmenwerken

Anforderung	**Gewichtung**	**NIST 800-63 v3**	**eIDAS**	**Kantara IAF**	**DFN-AAI Verlässlichkeitsklassen**	**IGTF Authentication Profiles**	**ITU-T X.1254**
[NFA_LoA_Minimalität]	(4)	✗	(✓)	✗	✓	(✓)	(✓)
[NFA_LoA_Modularität]	(4)	✓	✗	✗	✗	✗	✗
[NFA_LoA_Umsetzbarkeit]	(4)	✗	✗	✗	✓	(✓)	(✓)
[FA_LoA_1FA]	(2)	✓	✗	✓	✗	(✓)	(✓)
[FA_LoA_MFA]	(2)	✓	✗	✓	✗	✗	(✓)
[FA_LoA_Protokollkompatibilität]	(2)	✓	✓	✓	✓	✓	✓
[NFA_LoA_Unabhängigkeit]	(2)	(✓)	✗	✓	✓	✓	✓
[NFA_LoA_Implementierbarkeit]	(2)	✗	✗	✗	✓	(✓)	(✓)
[NFA_LoA_Verständlichkeit]	(2)	✗	✗	✗	✓	✓	✗
[NFA_LoA_Eigenständigkeit]	(1)	(✓)	✓	✗	✓	(✓)	(✓)
$G(p) = \sum w \cdot p$	G(p) max 50	23	10	16	34	25	23

✓: Anforderung erfüllt (2 Punkte)
(✓): Anforderung teilweise erfüllt (1 Punkt)
✗: Anforderung nicht erfüllt (0 Punkte)

wobei w: Gewichtung, p: Punkte und $G(p)$: Gesamtsumme Punkte

3.7 Informations- und Service-Managementmodelle

Dieser Abschnitt beschäftigt sich mit Informations- und Service-Managementmodellen, anhand derer Informationen und Entitäten im Zusammenhang mit Services und deren Lebenszyklus auf strukturierte Art und Weise beschrieben und modelliert werden können.

Die aus den Szenarien abgeleitete Hauptanforderung UM (vgl. Abschnitt 2.5) sowie deren Sub-Anforderungen haben die Zweckmäßigkeit und die erforderlichen Eigenschaften für ein Modell zur Beschreibung und Abbildung von Authentifizierungsszenarien verdeutlicht.

Im Rahmen dieses Abschnitts werden zwei als prinzipiell geeignet erachtete Modelle eingeführt; das **TM Forum Information Framework (SID)** sowie das **MNM Service Model (MSM)**. Während sich SID eher auf Informationen in Form von *Aggregate Business Entities* fokussiert, stellt MSM ein service-orientiertes Modell mit mehren Sichten zur Verfügung. Es werden deren Schlüsselkonzepte beschrieben und überprüft, inwieweit diese zur Wiederverwendung bzw. Erweiterbarkeit für Authentifizierungsszenarien geeignet sind.

In Abschnitt 3.7.3 findet dann ein Abgleich gegen die Anforderungen und die Auswahl eines geeigneten Modells statt.

3.7.1 TM Forum Information Framework (SID)

SID ist ein Framework, das durch das Telemanagement Forum (TMF) entwickelt wurde. Das Framework wurde jedoch nicht vollständig neu entwickelt, sondern basiert auf mehreren Quellen aus der Telekommunikationsbrache, wie ITU-T (International Telecommunication Union - Telecom) und DMTF (Distributed Management Task Force). SID gehört zu einem zusammenhängenden Satz von TM Forum Frameworks, deren Gesamtheit unter dem Begriff „Frameworx“, mit „x“ subsumiert ist. Dazu zählen u.a. ein Prozess Framework (eTOM), ein Application Framework (TAM), open APIs sowie Metriken. [Tel20b]

SID [Tel20b] fokussiert sich hierbei auf die Dekomposition von Informationen und ergänzt die in eTOM [Tel20a] definierten Prozesse um einen standardisierten Weg zur Strukturierung und Implementierung von Informationen. Die verwendete Beschreibungssprache ist technolgieunabhängig und objektorientiert. Zur Abbildung werden UML-Diagramme, insbesondere UML-Klassendiagramme, verwendet.

Zur Unterstützung der generischen Abbildung von Informationen greift SID auf acht verschiedene *Domänen* zurück (dazu zählen u.a. Customer Domain, Service Domain, Resource Domain). Jede dieser Domänen besteht aus mehreren definierten *Aggregate Business Entities* (core entities), die einen eng zusammenhängenden Satz von geschäftsrelevanten Entitäten repräsentieren. Entitäten des Modells, die noch nicht vollständig ausgereift sind, werden i.d.R. durch *TM Forum Member Contributions* im Laufe der Zeit entwickelt.

Als Teil der unterstützenden Dokumentation werden verschiedene *Information Modeling Pattern* beschrieben, um oft auftretende Anforderungen abbilden zu können (z.B. *Business Interactions*). Darüber hinaus werden verschiedene Techniken bereitgestellt, wie organisationsspezifische Entitäten in der eigenen SID-Implementierung hinzugefügt werden können.

3.7.2 MNM Service Model (MSM)

MSM [GHH+01, GHK+01, GHH+02] ist ein generisches, service-orientiertes Modell, dass durch das Munich Network Management (MNM) Team entwickelt wurde. Es stellt eine systematische Methodologie bereit, um Akteure eines Services sowie deren inter- und intra-organisatorische Abhängigkeiten zu analysieren und abzubilden. MSM unterscheidet dazu zwischen drei verschiedenen Sichten, die den gesamten Lebenszyklus eines (IT) Services berücksichtigen [ZS18]:

- **MSM Basic Service Model**: Dient zur grundlegenden Identifikation teilnehmender Rollen (Customer, User, Provider) und deren Beziehungen.
- **MSM Service View**: Ermöglicht die Beschreibung von Services unabhängig von der Service-Implementierung.
- **MSM Realization View**: Repräsentiert die provider-interne Realisierung eines Services.

Im Gegensatz zur domänenspezifischen Gruppierung von Informationen in SID, klassifiziert MSM Service-Interaktionen lediglich anhand von *Usage* und *Management* Funktionalität. Des Weiteren ermöglicht MSM eine rekursive Anwendung von Services (*chaining*) zur Darstellung von Sub-Service Abhängigkeiten.

3.7.3 Abgleich mit den Anforderungen

Im Folgenden werden die Anforderungen aus Abschnitt 2.6.5 erneut aufgegriffen und sowohl SID als auch MSM gegen die spezifizierten Anforderungen evaluiert. Die Ergebnisse sind in Tabelle 3.5 aggregiert zusammengefasst.

Es zeigt sich, dass der Abgleich der Anforderungen mit SID und MSM deckungsgleiche Ergebnisse liefert. Bspw. erfüllen sowohl SID als auch MSM die Anforderungen [FA_Terminologie], [FA_Managementaspekte] und [FA_Nutzungsaspekte] nur teilweise. Dies lässt sich darauf zurückführen, dass beide Modelle zwar grundsätzlich die Abbildung von Management- und Nutzungsaspekten ermöglichen, jedoch weitere Spezialisierungen für Authentifizierungsszenarien notwendig sind.

Zusammenfassend handelt es sich bei SID um ein sehr umfassendes Framework, das erst durch Anwendung der anderen TM Forum Frameworks eine Abbildung des Gesamtbilds ermöglicht. Dazu zählt insbesondere eTOM, dessen darin beschriebene Core Prozesse den Lebenszyklus eines oder mehrerer Informations-Entitäten aus SID managen. Ferner ist SID aufgrund dessen Herkunft auf Telekommunikations-Szenarien spezialisiert.

Der Fokus von SID ist die Abbildung von Informationen einer gesamten Organisationsstruktur (z.B. Service Provider Sicht) basierend auf mehreren Domänen und umfasst somit bspw. auch Prozesse zu Human Resources (HR). MSM hingegen betrachtet gezielt Services und die damit verbundenen Akteure und Abhängigkeiten unabhängig von organisatorischen Grenzen. Da föderierte Szenarien hochgradig organisationsübergreifend sind, scheint MSM

Tabelle 3.5: Abgleich der Anforderungen gegen SID und MSM

Anforderung	**Gewichtung**	**TM Forum SID**	**MNM Service Model**
[FA_Terminologie]	(4)	(✓)	(✓)
[FA_Service_Orientierung]	(4)	✓	✓
[FA_Rekursion]	(4)	✓	✓
[FA_Managementaspekte]	(2)	(✓)	(✓)
[FA_Nutzungsaspekte]	(2)	(✓)	(✓)
[FA_Schablonen]	(1)	✗	✗
$G(p) = \sum w \cdot p$	G(p) max 34	24	24

✓: Anforderung erfüllt (2 Punkte)
(✓): Anforderung teilweise erfüllt (1 Punkt)
✗: Anforderung nicht erfüllt (0 Punkte)

wobei w: Gewichtung, p: Punkte und $G(p)$: Gesamtsumme Punkte

das geeignetere Ausgangsmodell zu sein, weswegen dieses Modell, dessen Charakteristik und Eigenschaften zur weiteren Verfeinerung für authentifizierungsbezogene Dienste und Akteure herangezogen wird (vgl. Abschnitt 5.1).

3.8 Zusammenfassung der Perspektiven und Dimensionen des Problemraums

Nachdem die Grundlagen und der Status quo ausführlich beleuchtet und existierende Konzepte gegen die Anforderungen abgeglichen wurden, wird der IST-Stand zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM in Form mehrerer Perspektiven und Dimensionen visualisiert zusammengefasst. **Perspektiven** dienen in Abbildung 3.14 zur Repräsentation verschiedener Sichtweisen, während **Dimensionen** die verschiedenen Aspekte des Problemraums adressieren.

Insgesamt wird der IST-Zustand aus drei Perspektiven betrachtet:

- organisationsbezogene Perspektive
- föderierte bzw. intraföderierte Perspektive
- föderationsübergreifende bzw. interföderierte Perspektive

Zu den drei Perspektiven kommen sechs Dimensionen hinzu, welche z.T. in Form von Abschnitten in der Kapitelstruktur von Kapitel 3 direkt wiedergefunden werden können:

- Architekturmodelle
- MFA-Forschungsansätze

- Authentifizierungsinformationen
- föderierte Protokolle
- Softwareprodukte
- Trust Management

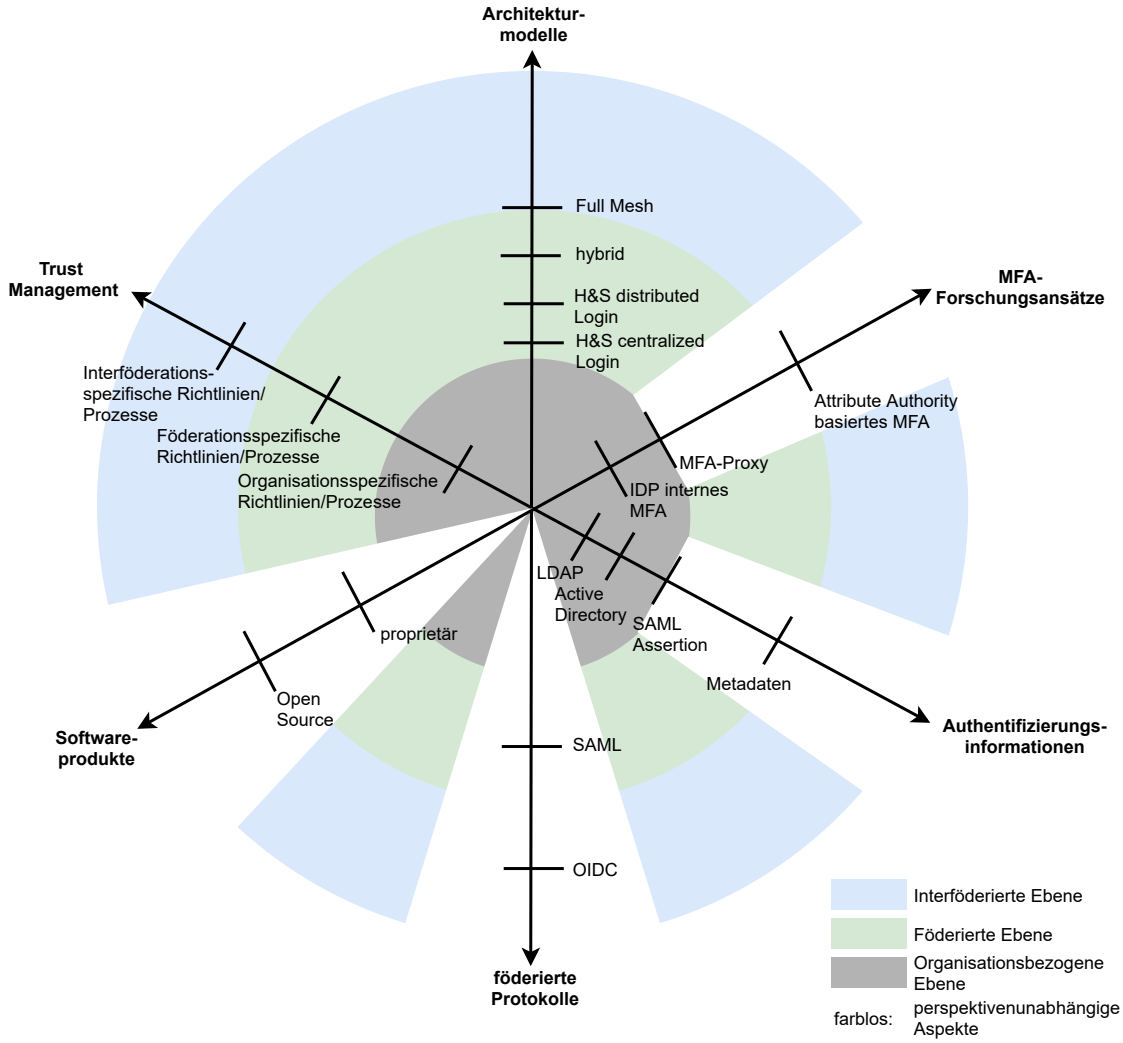


Abbildung 3.14: Darstellung des IST-Zustandes basierend auf einem Dimensionsstern inklusive verschiedener Perspektiven

Die sechs Dimensionen sind in Abbildung 3.14 anhand von nach außen zeigenden Pfeilen dargestellt. Die verschiedenen Perspektiven werden anhand eingefärbter, kreisförmiger Bereiche repräsentiert. Nicht eingefärbte Bereiche innerhalb des Dimensionssterns deuten dabei auf zusammengeführte bzw. -gefasste Perspektiven hin. Dies zeigt sich bspw. bei der Dimension der Softwareprodukte, da hier in jeder Perspektive sowohl proprietäre als auch Open Source Software zum Einsatz kommen kann. Aspekte, die auf dem Grenzbereich zwischen zwei

Perspektiven abgebildet sind, z.B. „Full Mesh“ in der Dimension der Architekturmodelle, werden den beiden, angrenzenden Perspektiven zugeordnet.

Die Dimension der Architekturmodelle visualisiert bspw. den Abschnitt 3.2.4, in dem die verschiedenen Architekturmodelle von Identitätsföderationen beschrieben wurden, während die Dimension des Trust Managements Bezug auf das Konzept der Level of Assurance (vgl. Abschnitt 3.6) und den Vertrauensaufbau (vgl. z.B. hierarchischer Vertrauensaufbau in eduGAIN in Abschnitt 3.3.1) nimmt. Die Dimension der Authentifizierungsinformationen verdeutlicht, dass Informationen bezogen auf eine Benutzerauthentifizierung grundsätzlich verschiedene Ausprägungen annehmen können und somit auch auf unterschiedliche Art und Weise kommuniziert werden. Authentifizierungsinformation kann dabei sowohl low-level Information, die von einem LDAP-Server an einen SAML IDP kommuniziert wird, sein oder aber auch high-level Information über Prozesse im Zusammenhang mit Authentifizierungen (z.B. Verlust eines Faktors). Letzteres steht wiederum in engem Zusammenhang mit der Dimension des Trust Managements, da die in Abschnitt 3.6 beschriebenen LoA-Konzepte Anforderungen an authentifizierungsbezogene Prozesse stellen.

Die in Abbildung 3.14 visualisierten Perspektiven und Dimensionen stehen somit in einem gegenseitigen Abhängigkeitsverhältnis und müssen bei der Konzeption einer Architektur in Kapitel 4 berücksichtigt werden.

3.9 Eingliederung der Arbeit in den Forschungsstand

In diesem Abschnitt wird die Dissertation in den Forschungsstand eingegliedert und aufgezeigt, wie die Dissertation zur Forschung in diesem Kontext beiträgt. Dazu wird das CARS Modell von Swales [Swa90] herangezogen, das insgesamt drei Aktionen, die als „Moves“ bezeichnet werden, definiert:

1. Der erste Move, die Eingliederung der Arbeit in den Forschungskontext, wurde in Kapitel 2 und 3 ausführlich durchgeführt, indem der Forschungsbereich, dessen Wichtigkeit sowie der State-of-the-Art ausführlich vorgestellt und diskutiert wurde.
2. Der zweite Move, der in diesem Abschnitt von Relevanz sein wird, definiert verschiedene Positionen, um aufzuzeigen, was der Beitrag der eigenen Forschung ist und wie sich dieser von bereits Vorhandenem abgrenzt. Die Positionen, wobei nicht alle sondern i.d.R. nur eine anzuwenden ist, sind gemäß des CARS Modells die Folgenden [Swa90, Men19]:
    - Gegenposition (*engl. Counter Claiming*): Vertreten einer Gegenposition und Unterlegung mit Thesen
    - Forschungslücke (*Indicating a Gap*): Aspekt, dem noch zu wenig Aufmerksamkeit zuteil wurde
    - In-Frage-Stellen (*engl. Question Arising*): Hinterfragen von Thesen
    - Forschungstradition (*engl. Continuing Tradition*): Weiterführen früherer Forschung

3. Der dritte Move, stellt das Einführen der eigenen Forschung dar. Dies wird im Besonderen ab Kapitel 4 deutlich.

Ziel dieses Abschnitts ist der zweite Move und das damit verbundene Abbilden einer Position auf die vorliegende Dissertation. Da die Dissertation jedoch modulare Konzepte spezifiziert, wird jeder erarbeiteter, zentraler Hauptanforderung (vgl. Abschnitt 2.5) eine Position zugeordnet:

- **Hauptanforderung AK und RM**, die an dieser Stelle gemeinsam betrachtet werden und die die Notwendigkeit eines leichtgewichtigen Authentication-Assurance-Konzept sowie dessen Umsetzungsunterstützung für Service Provider verdeutlichen, zeigen, dass ein bereits bekanntes Problem aus der Perspektive von R&E noch nicht übergreifend und im Detail beleuchtet wurde. Die Kapitel 1 bis 3 verdeutlichen jedoch, dass der Kontext R&E zunehmend an Relevanz gewinnt, weswegen die Forschungslücke anhand von Beiträgen dieser Dissertation gefüllt wird.
- **Hauptanforderung WF**, die Spezifikation eines Fallback MFA-Workflows für vollvermaschte Authentifizierungsszenarien, beschäftigt sich ebenfalls mit einer Forschungslücke, da der Fokus bisheriger MFA-Ansätze (vgl. Abschnitt 3.5) auf der IDP-seitigen Implementierung oder der Verwendung eines Proxies lag. Wie im nachfolgenden Kapitel noch ersichtlich werden wird, wird ein SP-seitiger, dynamischer[10] MFA-Workflow konzipiert, da diesem Vorgehen aus Sicht der Autorin bisher zu wenig Aufmerksamkeit geschenkt wurde.
- **Hauptanforderung UM** befasst sich mit der Beschreib- und Modellierbarkeit von Authentifizierungsszenarien. In Abschnitt 3.7 wurde gezeigt, dass zwar verschiedene Modelle vorhanden sind, diese aber zum Zwecke von Authentifizierungsszenarien weiter spezialisiert werden müssen. Die Umsetzung der Hauptanforderung UM wird daher als Forschungstradition interpretiert, da die Forschung zu einem vorhandenen Modell, dem MNM Service Modell (vgl. Abschnitt 3.7.2), weitergeführt wird.

Im folgenden Kapitel 4 werden die Beiträge dieser Arbeit anhand einer Architektur in einen Zusammenhang gesetzt. Zuvor wird noch in Abschnitt 3.10 eine abschließende Bewertung durchgeführt.

3.10 Abschließende Bewertung

Dieses Kapitel hat den **State-of-the-Art im Identity & Access Management**, im **Föderierten Identitätsmanagement** sowie im **Inter-Föderierten Identitätsmanagement** zusammengefasst. Neben der Einführung zentraler Begriffe wurde hier das Rollenmodell in FIM vorgestellt sowie aktuelle Standards bzw. Protokolle des föderierten Identitätsmanagements präsentiert. Ferner wurden Softwareprodukte und Architekturmodelle betrachtet und der Vertrauensaufbau in Inter-FIM exemplarisch anhand der Interföderation eduGAIN skizziert.

[10] *Dynamisch* im Sinne eines MFA-Workflows, der keine statische Kombination von Faktoren bzw. Faktorprüfern vorgibt, sondern eine beliebige Kombination unterstützt.

In Abschnitt 3.4 wurden dann die **Grundlagen zur Authentifizierung** und **Multi-Faktor-Authentifizierung** geschaffen und darauf aufbauend von der Identitätsfeststellung abgegrenzt. Darauffolgend wurden in Abschnitt 3.5 verschiedene Forschungsansätze zur Multi-Faktor-Authentifizierung in FIM vorgestellt und gegen die in Kapitel 2 definierten Anforderungen abgeglichen. Hierbei zeigte sich, dass keiner der evaluierten Ansätze die Anforderungen vollständig erfüllt, der AA-basierte MFA-Ansatz im Vergleich zum MFA-Ansatz mit Proxy zwischen IDP und SP für vollvermaschte Szenarien jedoch als die geeignetere Variante scheint. Da der AA-basierte MFA-Ansatz jedoch einige Schwächen aufweist, wird daher, aufbauend auf dessen Grundprinzipien, d.h. Verzicht auf eine zentrale Instanz, stattdessen SP-seitiges Triggern des MFA-Workflows, ein Fallback MFA-Workflow erarbeitet.

Den Abschnitten zur allgemeinen Benutzerauthentifizierung und den Forschungsansätzen zur Multi-Faktor-Authentifizierung in FIM nachfolgend wurden in Abschnitt 3.6 sowohl **LoA-Normen und -Standards** als auch **LoA-Konzepte in R&E** vorgestellt. Bei der Evaluation der vorgestellten LoA-Rahmenwerke wurde schlussgefolgert, dass kein Rahmenwerk in angemessenem Verhältnis zwischen Aufwand und Nutzen zum Zweck des föderierten Identitätsmanagements gemäß der drei Szenarien (nationales FIM, Inter-FIM, Forschungsinfrakstrukturen) steht, weswegen ein Authentication-Assurance-Konzept notwendig ist, welches den in Kapitel 2 spezifizierten Anforderungen genügt.

Anschließend wurden im Rahmen der Informations- und Service-Managementmodelle (vgl. Abschnitt 3.7) das **TMF Information Framework** sowie das **MNM Service Model** vorgestellt und gegen die in Abschnitt 2.6.5 definierten Anforderungen abgeglichen. Dabei zeigte sich, dass das MNM Service Model eine geeignete Grundlage zur Verfeinerung für authentifizierungsbezogene Szenarien darstellt.

Zuletzt wurde der aktuelle Forschungsstand auf mehrere Dimensionen abgebildet und anhand eines Dimensionssterns übersichtlich dargestellt. Anhand einer Eingliederung in den Forschungsstand wurden dann in die Beiträge dieser Dissertation positioniert (vgl. Abschnitte 3.8 und 3.9).

Im folgenden Kapitel 4 wird auf Basis der geschaffenen Grundlagen und der dargestellten Eingliederung in den Forschungsstand eine Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM konzeptioniert.

Kapitel 4

Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM

Inhalt dieses Kapitels

Auf Basis der in Kapitel 2 vorgestellten Szenarien sowie den präsentierten Grundlagen in Kapitel 3 werden in diesem Abschnitt die erforderlichen Komponenten und Konzepte für eine Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in einen Zusammenhang gesetzt.

Die Klassifikation der involvierten Komponenten orientiert sich dabei an den **vier Teilmodellen für Managementarchitekturen**, die dazu dienen, einen integrierten Ansatz der zu managenden Komponenten in einem heterogenen Umfeld zu erzielen [HAN99]. Dabei ist ein integrierter Ansatz gegeben, wenn auch die Informationen auf eine herstellerunabhängige Art und Weise interpretiert und diese anhand wohldefinierter Schnittstellen und Protokolle zugreifbar sind. Gemäß [HAN99] stellt eine sogenannte **Managementplattform** eine gute Voraussetzung dar, da sie Grundfunktionalität liefert und als offenes Trägersystem für Managementanwendungen gilt.

Bei Betrachtung der Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen aus Kapitel 2 sowie des Abschnitts 2.1, die die Szenarien als kollaborative Szenarien zur Erreichung gemeinsamer Ziele klassifizieren, wird jedoch klar, dass ein zentralisierter, plattformbasierter Ansatz den Szenarien aufgrund der bestehenden Autonomie der involvierten Entitäten widersprüchlich entgegensteht. Identity Provider, Service Provider und Infrastrukturen sind vielmehr als jeweils eigenständige, zu managende Bereiche anzusehen, die lediglich zum Zwecke der Erleichterung des Dienstzugriffs gegenseitig Informationen austauschen.

Folglich ist das Ziel dieser Arbeit nicht die Konzeption einer zentralen Managementplattform zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM, sondern vielmehr die Konzeption einer Architektur, die neue, modulare **Konzepte** für verschiedene Domänen und Funktionsbereiche bereitstellt, die bedarfsorientiert von Teilnehmern einer heterogenen Infrastruktur angewendet und integriert werden können. Dies hat jedoch zur Folge, dass die in [HAN99] spezifizierten Teilmodelle nicht mehr 1:1 anwendbar sind, weswegen lediglich das **Klassifikationsschema für Komponenten gemäß der vier Teilmodelle** extrahiert wird.

Somit ergibt sich auch die Definition des Begriffes **Komponente**, der in dieser Arbeit zunächst eine abstrakte Einheit bzw. einen Bestandteil von etwas Übergeordnetem repräsentiert hat und der nun unter Betrachtung der vier Teilmodelle genauer definiert wird (vgl. Tabelle 4.1).

Der Begriff **Konzept** wird synonym zum Begriff **Teillösung** verwendet und beschreibt die Kombination von Komponenten unterschiedlichen Typs, um jeweils auf die in Kapitel 1 identifizierten Fragestellungen eine Antwort zu liefern.

Der Aufbau des Kapitels ist der Folgende, wobei er sich an den erarbeiteten Hauptanforderungen AK, RM, WF und UM des Kapitels 2 orientiert:

In Abschnitt 4.1 wird zunächst einen kurzer Überblick über die vier Teilmodelle gemäß [HAN99] gegeben und gezeigt, welche **Typen von Komponenten** für eine strukturierte Ableitung des Idealzustandes zu berücksichtigen und folglich zu modellieren sind.

Die Abschnitte 4.2, 4.3, 4.4 und 4.5 spiegeln die vier Hauptanforderungen aus Kapitel 2 wieder, sodass die Architektur anhand von vier Teilen strukturiert und systematisch erarbeitet wird. Die Teile der Architektur werden dabei entsprechend der vier Hauptanforderungen bezeichnet, d.h. Architekturteil AK, Architekturteil RM, Architekturteil WF und Architekturteil UM.

In den Abschnitten 4.2.1 bis 4.2.4 werden die Komponenten des Organisations-, Informations-, Funktions- und Kommunikationsmodells, die für das Authentication-Assurance-Konzept relevant sind, eingeführt. Da ein Großteil der dort eingeführten Komponenten auch für die darauffolgenden Teile der Architektur von Relevanz sein werden, findet jeweils in denen, den Abschnitten 4.3 bis 4.5 untergeordneten Abschnitten eine Erweiterung der Organisations-, Informations-, Funktions- und Kommunikationsmodelle statt.

Der Abschnitt 4.6 gibt eine Zusammenfassung des Kapitels sowie einen Überblick über die resultierende Gesamtarchitektur.

4.1 Strukturierte Ableitung des Idealzustandes

Da durch die Konzeption einer Architektur sowohl neue Komponenten und Konzepte eingeführt als auch existierende erweitert werden, ist ein systematisches Vorgehen und eine sinnvolle Strukturierung erforderlich. Es soll klar hervorgehen, welchen Typ bzw. welche Ausprägung die involvierten „Komponenten“ besitzen, deren Begriffsdefinition in den vorherigen Kapiteln noch nicht weiter konkretisiert wurde. Die Klassifikation der Komponenten zur Konzeption einer Architektur greift dazu auf die vier Teilmodelle für Managementarchitekturen [HAN99] zurück. Gemäß [HAN99] sind die folgenden Elemente bzw. Komponenten, die in der Tabelle 4.1 in der rechten Spalte übersichtlich aufgelistet sind, auf eine herstellerunabhängige Art und Weise zu adressieren.

Tabelle 4.1: Extraktion der zu modellierenden Komponenten gemäß [HAN99]

Teilmodell	**Kurzbeschreibung**	**Klassifikation der Komponenten gemäß**
Organisationsmodell	Beschreibung von Organisationsaspekten, Rollen und Kooperationsformen	Rollen, Domänen, Interaktionen, Software
Funktionsmodell	Strukturierung von Managementfunktionalität	Funktionsbereiche, Funktionen
Informationsmodell	Darstellung der zu managenden Objekte	Management(informations-)objekte
Kommunikationsmodell	Spezifikation von Kommunikationsvorgängen	Kommunikationspartner, Kommunikationsmechanismus, Syntax und Semantik, (Management-) Protokolle

Zur Modellierung wird die objektorientierte **Unified Modeling Language (UML)** verwendet. Unter Berücksichtigung der Tabelle 4.1 werden die folgenden Komponenten der Architektur als **UML-Klassen** repräsentiert:

- **Rollen:** Die entsprechenden UML-Klassen werden hierfür mit dem Stereotyp *«role»* markiert.
- **Software:** Für Software kommt der Stereotyp *«software»* zum Einsatz.
- Managementobjekte, hier als **Informationsobjekte** bezeichnet, sind mit dem Stereotyp *«information»* versehen.

Zur Vermeidung unnötiger Komplexität wird auf die Modellierung von **Domänen** (siehe Organisationsmodell) an dieser Stelle verzichtet. Ferner werden **Interaktionen** bzw. die damit verbundenen **Interaktionskanäle**, die nicht über die identifizierte Software (siehe Software als Teil des Organisationsmodells) stattfinden, nicht explizit modelliert.[1]

Funktionen werden innerhalb der jeweiligen UML-Klasse als Methoden dargestellt, während **Funktionsbereiche** durch die Architekturteile AK, RM, WF und UM repräsentiert werden.

Die **Kommunikationspartner**, **-mechanismen** und -**protokolle** werden im Rahmen von UML-Sequenzdiagrammen adressiert.

Im folgenden Abschnitt wird zunächst der Teil der Architektur erarbeitet, der sich mit der Konzeption eines Authentication-Assurance-Konzeptes (vgl. Hauptanforderung AK in Abschnitt 2.5) befasst. Dazu werden die oben genannten Komponenten des Organisationsmodells, Funktionsmodells, Informationsmodells und Kommunikationsmodells eingeführt und aufgezeigt, welche Komponenten für welche Konzepte bzw. Teillösungen relevant sind.

4.2 Architekturteil AK: Authentication-Assurance-Konzept

Mit Hilfe des zu spezifizierenden Authentication-Assurance-Konzepts wird die Herausforderung gelöst, dass Service Provider momentan kaum Rückschlüsse über die Qualität einer vom Identity Provider durchgeführten Authentifizierung ziehen können, da Authentifizierungsinformationen wie bspw. Passwortlänge oder -komplexität, Zwei-Faktor-Authentifizierung ja/nein in den Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen nicht übergreifend und einheitlich kommuniziert werden. Aktuell müssen Service Provider den wenig konkreten Aussagen der Identity Provider vertrauen, ohne ein genaueres Verständnis über

[1] Interaktionskanäle sind Schnittstellen, oder in der UML-Terminologie gesprochen, Assoziationen deren Assoziationsstart und -ende jeweils eine Klasse des Typs «role» ist. Sie ermöglichen den Wissensaustausch zwischen den beiden involvierten Rollen und dienen üblicherweise zur Erfüllung einer Funktion (vgl. Funktionsmodell). Dies kann entweder mittels der in der Architektur identifizierten und involvierten Software erfolgen oder unter Verwendung anderer, beliebiger Kanäle (z.B. via E-Mail, Ticket-System oder von Mensch-zu-Mensch). Auf letzteres wird jedoch zum Zwecke eines verständlichen und übersichtlichen Architekturmodells verzichtet.

die Qualität der durchgeführten Authentifizierung zu besitzen. Dies ist jedoch insbesondere bei kritischen Diensten relevant.

Der Architekturteil AK beschäftigt sich somit mit der strukturierten Erarbeitung eines Authentication-Assurance-Konzepts (vgl. Hauptanforderung AK). Bevor die zentralen Informationsobjekte in Abschnitt 4.2.2 eingeführt werden, werden jedoch zunächst die für das Authentication-Assurance-Konzept relevanten und involvierten Rollen und Softwarekomponenten in Abschnitt 4.2.1 eingeführt. Nach Einführung der Informationsobjekte werden dann in den Abschnitten 4.2.3 und 4.2.4 Funktionen und Kommunikationsvorgänge erläutert.

Der hier erarbeitete Architekturteil AK wird dann an späterer Stelle, in den Abschnitten 4.3 bis 4.5, durch die entsprechenden Teillösungen und den dazu involvierten Komponenten zur Erfüllung der verbleibenden Hauptanforderungen erweitert.

4.2.1 Organisationsmodell

Sowohl in Kapitel 1 als auch im FIM-Rollenmodell des Kapitels 3 wurden die zentralen Entitäten bzw. Rollen in (Inter-) FIM Szenarien eingeführt und kurz beschrieben. In Abschnitt 4.2.1.1 werden die Rollen dann im Rahmen des Organisationsmodells erneut aufgegriffen, welche dann in Abschnitt 4.2.1.2 durch die zur Kommunikation des Authentication-Assurance-Konzepts benötigten Softwarekomponenten ergänzt werden.

4.2.1.1 Rollen

Die Rollen stellen eine zentrale Komponente der Architektur dar, da sie zur Kommunikation und dem damit verbundenen Austausch von Assurance-Information benötigt werden. Wie in Abschnitt 3.2.1 bereits ersichtlich wurde, sind in (Inter-) FIM Szenarien typischerweise die drei Rollen **Identity Provider**, **Service Provider** und **User** vertreten. Ferner ist auch die Rolle **Infrastructure Provider** zu berücksichtigen.

Die Rolle User repräsentiert dabei üblicherweise eine natürliche Person, während Provider i.d.R. legale Entitäten darstellen. Gemäß des Szenarios Inter-FIM aus Kapitel 2 sind somit ebenfalls Vereine denkbar, sodass eine Provider-Rolle auch von mehreren Personen aus potentiell unterschiedlichen Organisationen erbracht werden kann. Im Fortlauf der Architektur werden Provider-Rollen daher als aggregierte Rollen bezeichnet, da sie auch im Hinblick auf die Prozesse des Servicemanagements mehrere Sub-Rollen zusammenfassen. Dazu zählt bspw. die Rolle des Change Managers, die Rolle des Incident Managers sowie die des Service Desks.

Die folgende Auflistung gibt einen Überblick über die für den Architekturteil AK relevanten Rollen:

- **Infrastructure Provider** (UML-Klasse `InfrastructureProvider`): Übergeordnete Rolle zur Aggregation eines Infrastrukturbetreibers. Sie ist u.a. für den Betrieb, den

Support und die Wartung der Infrastruktur verantwortlich. Die untergeordneten Sub-Rollen können dabei bspw. von Personen verschiedener Organisationen eingenommen werden. Zum Beispiel stellt Organisation A einen Incident Manager bereit, während ein Personenkreis aus Organisation B den Service Desk für die Infrastruktur betreibt.

- **Identity Provider** (UML-Klasse `IdentityProvider`): Die Rolle des Identity Providers stellt analog zur Rolle des Infrastrukturbetreibers eine aggregierte Rolle dar.
- **Service Provider** (UML-Klasse `ServiceProvider`): Übergeordnete Rolle zur Aggregation eines Dienstbetreibers.
- **User** (UML-Klasse `User`): Die Rolle des Nutzers ist diejenige, die auf einen Dienst zugreifen und diesen nutzen möchte. Dazu muss der Prozess der Authentifizierung durchlaufen werden.

Eine visuelle Abbildung der Rollen anhand von UML-Klassen findet sich in Abbildung 4.1.

4.2.1.2 Software

In diesem Abschnitt wird die involvierte Software identifiziert. Auch hier verbleibt der Fokus auf derjenigen Software, die im unmittelbaren Bezug zur Verarbeitung von Authentication-Assurance-Information steht. Somit ergibt sich in Abbildung 4.1 der Architekturteil AK, der die dazu involvierten Rollen und Softwarekomponenten enthält.

In Bezug auf Software kommt somit die UML-Klasse `FIMswIDP` hinzu. Der Einfachheit halber wird diese gemäß der Abbildung 4.1 durch die Identity Provider Rolle betrieben, auch wenn bei Betrachtung der verschiedenen Architekturmuster von Föderationen (vgl. v.a. Hub & Spoke Architekturen mit zentralisiertem Login in Abschnitt 3.2.4) dies nicht zwangsweise der Fall sein muss.

`FIMswIDP` repräsentiert die technische Komponente, z.B. einen Shibboleth Identity Provider, der zur Authentifizierung und Verarbeitung von Authentication-Assurance-Informationen benötigt wird. Daran angeschlossene Verzeichnisdienste wie LDAP oder Active Directory sind nicht explizit modelliert.

Analog zu `FIMswIDP` wird Abbildung 4.1 durch `FIMswSP` ergänzt, die SP-seitig die technische Komponente zur Anfrage und Verarbeitung von Authentication-Assurance-Informationen repräsentiert.

Im folgenden Abschnitt werden unter Berücksichtigung der Anforderungen aus Abschnitt 2.6.2 die Informationsobjekte zur Authentication Assurance spezifiziert.

4.2.2 Informationsmodell

Gemäß [HAN99] wird ein Informationsmodell benötigt, um die Gesamtheit der zu managenden Objekte zu bestimmen. Dieses zeigt auf, wie Objekte identifiziert werden können, welche

Abhängigkeiten zwischen den Informationsobjekten bestehen und wie Informationsobjekte manipuliert werden können. Um später ein Gesamtbild der Architektur zu erreichen, in der sowohl existierende Komponenten als auch neue Komponenten und deren Abhängigkeiten abgebildet sind, wird im Folgenden die Abbildung 4.1 um die Informationsobjekte in Bezug auf die Authentication Assurance ergänzt.

Wie bereits in Kapitel 2 bei der Anforderungsanalyse deutlich wurde, stellt ein zentrales Ziel bei der Spezifikation eines Authentication-Assurance-Konzepts die Modularität (vgl. Anforderung [NFA_LOA_Modularität]) dar, d.h. die Trennung der Identity Assurance von der Authentication Assurance, um verschiedene Assurance bezogene Anwendungsfälle adäquat abdecken zu können. Dies führt zu einer Trennung der beiden Aspekte in der Architektur, sodass das UML-Klassenmodell der Architektur (vgl. Abbildung 4.1) zwischen den beiden Klassen `IDAssurance` und `AuthNAssurance` differenziert. Obwohl, wie bereits mehrfach erläutert, die Identity Assurance keinen Beitrag dieser Arbeit darstellt, werden Teile der Identity Assurance in Abbildung 4.1 modelliert; insbesondere auch unter dem Aspekt, dass sich aus der Kombination verschiedener Identitäts- und Authentifizierungsgrade unterschiedlich starke Assurance Level bzw. Profile ableiten lassen. Darüber hinaus sind, wie an späterer Stelle noch ersichtlich werden wird, die Spezifikationen zur Identity Assurance und Authentication Assurance Teil einer gemeinsamen Assurance Suite.

Bei den Klassen `IDAssurance` und `AuthNAssurance` handelt es sich jeweils um Informationsobjekte, die anhand von Leveln bzw. Profilen zwischen den verschiedenen Rollen ausgetauscht werden. Sie werden daher mit dem Stereotyp *«information»* versehen.

Ferner wird aus Gründen der Vollständigkeit die Klasse `UserID` eingeführt, deren Kriterien Teil der Identity Assurance sind. Diese Klasse repräsentiert die digitale Benutzeridentität bzw. den damit verbundenen User Identifier, der mittels Identitätsfeststellungsverfahren an die Klasse `User` gebunden wird. Diese Klasse ist insofern für die Authentifizierung relevant, da diese Klasse auch das zentrale Bindeglied für Authentifizierungsfaktoren darstellt.

Bezüglich der Authentication Assurance verdeutlichen die Anforderungen [FA_LoA_1FA]) sowie [FA_LoA_MFA]), dass sowohl Qualitätskriterien für Authentifizierungen mit einem Faktor als auch für Authentifizierungen mit mehreren Faktoren benötigt werden. Da, wie in Abschnitt 3.4.1 ersichtlich wurde, bei Authentifizierungen zwischen verschiedenen Typen von Authentifizierungsfaktoren unterschieden wird, wird die Klasse `AuthenticationFactor` eingeführt, die zusätzlich das Attribut `factorType` enthält. Die Klassen `AuthNFactorN` und `AuthNFactorN+1` erben dabei von der Klasse `AuthenticationFactor`. Die Abstraktion von konkreten numerischen Werten (wie z.B. `AuthNFactor1` anstelle `AuthnFactorN` bzw. `AuthNFactor2` anstelle `AuthNFactorN+1`, etc.) hin zur Verwendung der Bezeichner *n* und *n+1*, lässt sich darauf zurückführen, dass durch die Architektur auch Szenarien zu unterstützen sind, bei der eine existierende 2FA durch einen dritten Faktor erweitert werden soll.

Die in Abschnitt 3.6 analysierten LoA-Normen und -Standards sowie Konzepte aus R&E verdeutlichen, dass neben den Kriterien an Authentifizierungsfaktoren selbst (z.B. minimale Passwortlänge) auch Kriterien zu den Verfahren verbunden mit Authentifizierungsfaktoren zu definieren sind. Somit muss z.B. das Verfahren zum Zurücksetzen eines Passworts ebenfalls

sicher sein, da sonst eine Authentifizierung durch eine Kompromittierung des Verfahrens ausgehebelt werden kann. Somit wird ebenfalls die Klasse `AuthNProcedure` eingeführt, die die verschiedenen Verfahren in Bezug auf Authentifizierungen repräsentiert. Des Weiteren werden die entsprechenden Assoziationen mit den bereits eingeführten Klassen hergestellt.

Da es sich bei den Anforderungen [NFA_LoA_Minimalität], [NFA_LoA_Unabhängigkeit], [NFA_LoA_Umsetzbarkeit], [NFA_LoA_Implementierbarkeit], [NFA_LoA_Verständlichkeit] und [NFA_LoA_Eigenständigkeit] um Nicht-Funktionale Anforderungen handelt, können diese aufgrund ihres Charakters nicht explizit in Form von UML-Klassen bzw. Informationsobjekten modelliert werden.

Die letzte der Anforderungen stellt die Protokollkompatibilität ([FA_LoA_Protokollkompatibilität]) dar, um sicherzustellen, dass das Authentication-Assurance-Konzept mit FIM-Protokollen kommunizierbar ist. Wie dieses kommuniziert wird, ist ebenfalls nicht explizit in Abbildung 4.1 dargestellt. Gemäß [HAN99] werden hier Kommunikationsmodelle verwendet, um die involvierten Partner, Mechanismen und Nachrichtenflüsse darzustellen. Daher wird bei den Kommunikationsvorgängen in Abschnitt 4.2.4 ein entsprechendes UML-Sequenzdiagramm aufgezeigt.

Nachdem die zentralen Informationsobjekte in Bezug auf das zu spezifizierende Authentication-Assurance-Konzept vorgestellt wurden, wird im nächsten Schritt aufgezeigt, wie die Komponenten zusammengefasst bzw. gruppiert werden, um modulare Teillösungen zu erreichen.

Zur Gruppierung der Informationsobjekte wird daher der in Abbildung 4.1 dargestellte Auszug der Architektur um farbliche, gestrichelte Markierungen erweitert. Graue Markierungen umfassen dabei Bereiche, die keinen Beitrag bzw. Leistung dieser Arbeit darstellen, während rote Markierungen Beiträge dieser Arbeit darstellen, die entweder in Kapitel 5 erarbeitet werden oder die bereits publiziert wurden und auf die in Kapitel 5 Bezug genommen wird.

Gemäß Abbildung 4.1 sind die Informationsobjekte, die Teil der Identity Assurance sind, daher grau umrahmt, da die Identity Assurance keinen Beitrag dieser Arbeit darstellt und da die Herausforderung zur Spezifikation eines Identity-Assurance-Konzepts [LAB+18, REF18a] in der REFEDS Assurance Working Group [REF20a] ohne die aktive Beteiligung der Autorin gelöst wurde. Aktuell wird aber unter Leitung der Autorin der REFEDS Assurance Working Group an der Version 2 des REFEDS Identity Assurance Frameworks gearbeitet.

Eine neue Teillösung bzw. Konzept stellt hier das **Ein-Faktor-Authentifizierungs-Profil** (SFA-Profil) dar, das Anforderungen an die Qualität einer Authentifizierung mit einem Faktor stellt. Dieses wurde von der Autorin dieser Arbeit und ihrem Kollegen Michael Schmidt federführend anhand vielzähliger Feedback-Iterationen und Diskussionen als Teil der REFEDS Assurance Working Group erarbeitet und ist daher in Abbildung 4.1 als neue Komponente markiert. Aufgrund dessen ist das Ein-Faktor-Authentifizierungs-Profil bereits vor der Veröffentlichung dieser Arbeit unter dem Namen REFEDS Single Factor Authentication Profile online verfügbar [ZSL19, Zie18, REF18c]. In Kapitel 5 wird somit die bereits veröffentlichte Spezifikation aufgegriffen.

Da ein **Multi-Faktor-Authentifizierungs-Profil** (MFA-Profil) bereits ebenfalls unter dem Namen REFEDS Multi Factor Authentication Profile existiert [REF17], dieses aber im Rahmen dieser Arbeit lediglich erweitert wird, ist die publizierte Version in Abbildung 4.1 daher grau umrahmt.

Die drei Spezifikationen, das REFEDS (Identity) Assurance Framework, das REFEDS Single Factor Authentication Profile sowie das REFEDS Multi Factor Authentication Profile sind dabei Teil der übergreifenden REFEDS Assurance Suite.

4.2.3 Funktionsmodell

Gemäß [HAN99] teilt das Funktionsmodell den Gesamtaufgabenkomplex in Funktionsbereiche und legt somit die Basis für ein Baukastenprinzip fest. Folglich ist das Ziel dieses Abschnitts die Erfassung und Abbildung der Funktionen des Funktionsbereiches „Authentication Assurance“ in der Architektur. Bei der Analyse dieses Funktionsbereiches wird deutlich, dass hier lediglich vorhandene Funktionen aufzuführen sind, da deren Ausführungsfähigkeit von der Einführung eines Authentication-Assurance-Konzepts abhängt.

Im Folgenden wird ein Überblick über die zu diesem Funktionsbereich zugehörigen Funktionen gegeben. Die Funktionen repräsentieren dabei sowohl manuelle Tätigkeiten, d.h. diejenigen, die von Menschenhand durch die jeweilige Rolle durchzuführen sind, als auch Funktionen, die automatisiert stattfinden und daher einer entsprechenden Softwarekomponente zugeordnet sind. Des Weiteren werden die gängigen CRUD[2]-Funktionen berücksichtigt. Die Zuordnung der Funktionen zu Komponenten kann der Abbildung 4.1 entnommen werden.

- **setAAL()**: Oder gemäß CRUD auch *createAAL()* repräsentiert die Funktion, um auf Basis der Stärke der bereitgestellten Authentifizierungsfaktoren und den authentifizierungsbezogenen Verfahren das korrekte Authentication Assurance Level auszuwählen und zu setzen. Dazu wird ein Authentication-Assurance-Konzept, das verschiedene Level bzw. Profile festlegt, benötigt, welches in Abschnitt 5.2 spezifiziert wird.
- **readAAL()**: Repräsentiert das Auslesen des eigenen Authentication Assurance Levels.
- **updateAAL()**: Repräsentiert das Aktualisieren des eigenen Authentication Assurance Levels.
- **deleteAAL()**: Repräsentiert das Löschen des eigenen Authentication Assurance Levels.
- **requestAAL()**: Diese Funktion repräsentiert das Anfragen eines Authentication Assurance Levels seitens des Service Providers.
- **respondWithAAL()**: Diese Funktion wird verwendet, um auf eine Anfrage des Service Providers zu antworten.

[2] *create, read, update, delete*

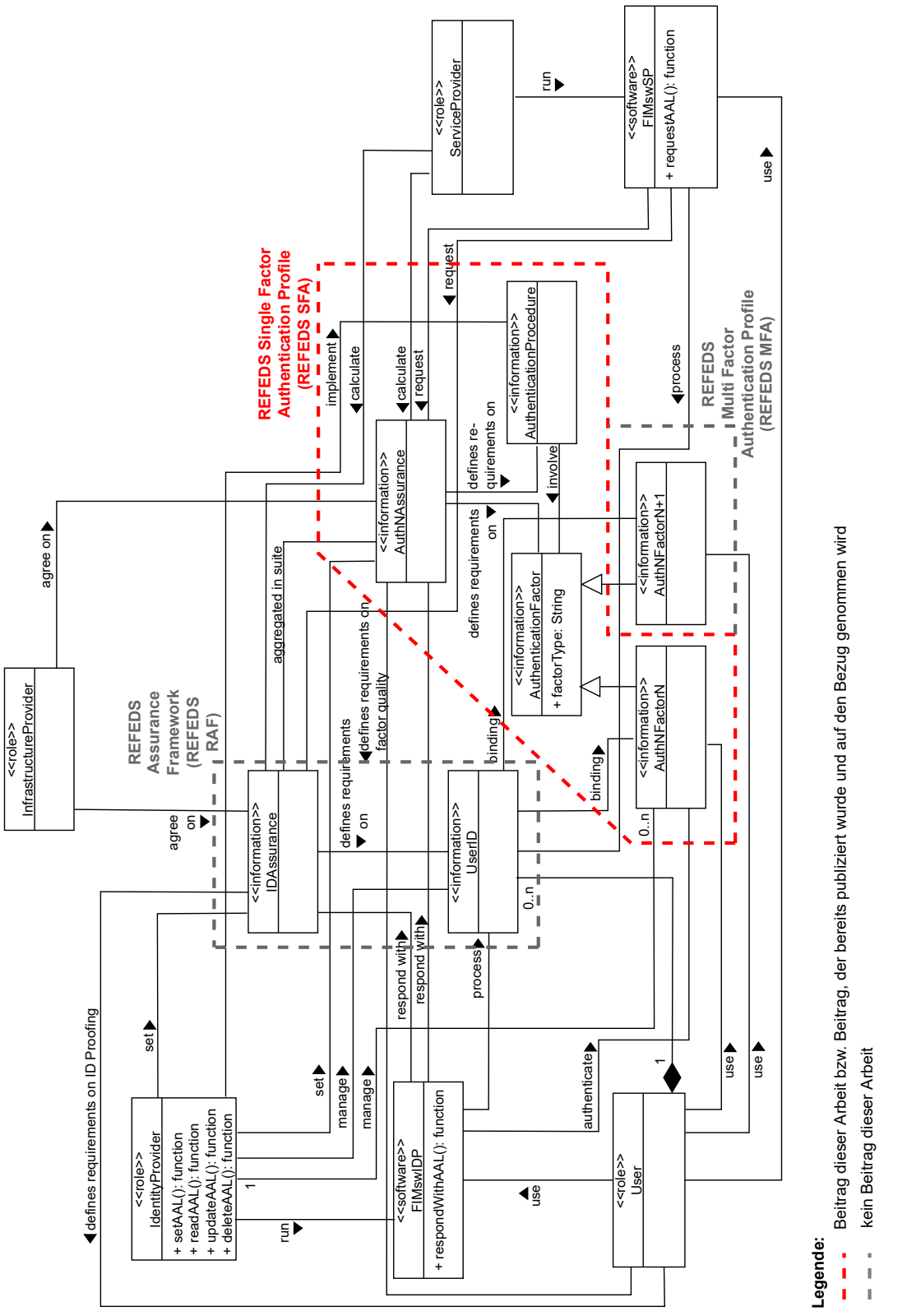


Abbildung 4.1: Resultierender Architekturteil AK

4.2.4 Kommunikationsmodell

Das Kommunikationsmodell gemäß [HAN99] betrachtet die Art und Weise, wie Informationen zwischen den involvierten Akteuren bzw. Rollen ausgetauscht werden, was u.a. durch die Interaktion mit den identifizierten Softwarekomponenten geschieht. Im Folgenden werden daher die durch die föderierten Protokolle SAML und OIDC bereitgestellten Mechanismen zum Austausch von (Authentication-) Assurance-Information vorgestellt und aufgezeigt, welche Mechanismen bei den publizierten Assurance-Spezifikationen [Zie18, REF18c, Zie17, REF17] Anwendung finden.

Bei der Entscheidung welche Variante zur Kommunikation von Informationen allgemein, d.h. unabhängig von der Identity und Authentication Assurance, geeignet ist, kommt es grundsätzlich auf die Art von Informationen an, die übermittelt bzw. ausgetauscht werden soll.

Informationen bezogen auf Benutzer werden üblicherweise in SAML in Form von Attributen und in OIDC in Form von Scopes bzw. Claims in einer Antwortnachricht kommuniziert. In R&E wird dazu bspw. auf das eduPerson-Attributschema [Int16] zurückgegriffen, generell kann aber ein beliebiges Attributschema verwendet werden. Eine weitere Variante, insbesondere für Informationen über durchgeführte Authentifizierungen, ist die Verwendung des SAML Authentication Context [KCM+05] bzw. des OIDC ACR[3] oder AMR[4] [SBJ+14b]. Informationen bezogen auf das (Trust) Management zwischen Entitäten, bspw. zur Etablierung technischen Vertrauens, wie Zertifikate, sind üblicherweise innerhalb der Metadaten festgehalten. Auch Spezifikationen die von einem IDP bzw. SP zu allgemeinen Praktiken behauptet werden, wie SIRTFI [BBG+15] zu einem koordinierten Austausch im Fall eines Security Incidents zwischen Entitäten wird in SAML ebenfalls innerhalb der Metadaten, aber anhand einer Assurance Certification innerhalb der Entity Attribute, kommuniziert. Da in SAML i.d.R. ein statisches Metadatenfile existiert in dem alle teilnehmenden Entitäten enthalten sind, lassen sich Entitäten prinzipiell auch anhand verschiedener Metadaten-Streams gruppieren. Dieses Vorgehen wird in der DFN-AAI zum Recherchezeitpunkt für die verschiedenen Verlässlichkeitsklassen (vgl. Abschnitt 3.6.2.1) verwendet, sodass jeweils ein separater Metadaten-Stream für die Klassen basic bzw. advanced (und test) existiert.

Im Folgenden werden die erläuterten Varianten übersichtlich aufgelistet und hinsichtlich ihrer Eignung diskutiert:

1. **Repräsentation von Assurance-Information in den Metadaten (z.B. SAML Metadatenfile)**: Intuitive Variante. Assurance-Information ist im Fall von SAML direkt in der Metadatendatei enthalten. Die Assurance-Information bezieht sich jedoch auf den gesamten IDP, d.h. die dort enthaltene Information muss für alle Nutzer eines IDPs gleichermaßen gelten. Nutzer-bezogene Assurance-Information ist anhand von Metadaten nicht möglich.
2. **Kommunikation mittels (multi-valued) SAML-Attributs oder OIDC Claim**: Attribute bzw. Claims werden im Vergleich zum zuvor erläuterten Metadatenansatz

[3] Authentication Context Class Reference
[4] Authentication Methods References

herangezogen, um Informationen über einen konkreten Nutzer zu kommunizieren. Sie besitzen die Eigenschaft, dass sie entweder *single-valued* oder *multi-valued* sein können. Im ersten Fall wird mittels eines bestimmten Attributes nur ein einziger Wert kommuniziert (z.B. Name = Alice) während im anderen Fall anhand eines Attributes mehrere Werte übermittelt werden können. Zur Kommunikation von Assurance-Information sieht das eduPerson-Attributschema [Int16] bereits das multi-valued Attribut *eduPersonAssurance* vor. Anhand diesem können mehrere URIs kommuniziert werden, um die Compliance mit einem Assurance-Standard zu behaupten. Hier wird die Assurance-Information erst nach einem Authentication Request in der Response übermittelt. Der Nachteil an dieser Variante ist, dass Nutzer zunächst zu ihrer Heimatorganisation weitergeleitet werden und nach der Authentifizierung möglicherweise vom SP abgewiesen werden. Dadurch sinkt die Benutzerfreundlichkeit. Ferner wird, aufgrund der oben genannten Eigenschaft, dass Attribute i.d.R. Informationen über einen Benutzer darstellen, die Kommunikation von Assurance-Information innerhalb eines Attributes oftmals falsch interpretiert bzw. missverstanden.

3. **Kommunikation mittels Authentication Context Class**[5]: In SAML wird der sogenannte Authentication Context seit SAML 2.0 unterstützt. Er wird dazu angewendet, um einem Service Provider nach einer gestellten Authentifizierungsanfrage zusätzliche Informationen bereitzustellen, sodass dieser in der Lage ist die Assurance einer SAML Assertion zu bewerten [KCM+05]. Aufgrund der möglichen vielzähligen Variationen, stellt die SAML-Spezifikation [KCM+05] sogenannte Authentication Context Classes bereit. Diese lassen sich anhand einer eindeutigen URI identifizieren und stellen bereits einige gängige Kategorien basierend auf konkreten Authentifizierungsmethoden dar. Die URI *urn:oasis:names:tc:SAML:2.0:ac: classes:MobileTwoFactorUnregistered* reflektiert bspw. den Anwendungsfall wenn die ID des Kunden an einen mobil bereitgestellten Zwei-Faktor-Authentifizierungsdienst durch die Erfassung von Mobilfunkdaten bei der Registrierung geknüpft wird [KCM+05]. Ein Vorteil des SAML Authentifizerungskontextes ist, dass dieser auch als Filter eingesetzt werden kann, sodass ein SP bereits in der Anfrage seine präferierte(n) Authentifizierungskontext(e) mittels RequestedAuthnContext anfragen und diesen mit dem Authentifizierungskontext der Antwort vergleichen kann. Der Authentifizierungskontext ist sowohl in SAML als auch in OpenID Connect definiert. In SAML ist die Authentication Context Class ein XML-Fragment und Teil der SAML Attribute Assertion. In OIDC als acr claim im ID Token [SBJ+14b]. Die OIDC Spezifikation verweist hier auf die ISO/IEC 29115, es kann jedoch auch ein anderer, kontext-spezifischer Wert verwendet werden auf dessen Bedeutung sich die involvierten Parteien zunächst einigen müssen. Der Authentifizierungskontext kann somit nutzerbezogen Authentication-Assurance-Information kommunizieren.

Zusammenfassend lassen sich die oben genannten Ansätze weiter aggregieren: Der Kommunikation innerhalb der Metadaten, sodass die Information IDP- bzw. SP-bezogen vorliegt. Oder der Kommunikation in der SAML Assertion bzw. OIDC ID Token für eine nutzerbasierte Assurance-Information.

[5] Im Folgenden als *Authentifizierungskontext* bezeichnet

Im Hinblick auf die Authentication Assurance und den in Abschnitt 5.2 vorgestellten, enthaltenen Kriterien kann nicht davon ausgegangen werden, dass die dort definierten Kriterien für alle Nutzer einer Institution gleichermaßen gelten. Betrachtet man bspw. größere Institutionen wie Universitäten gibt es hier meist unterschiedliche Nutzergruppen. Es gibt Studenten, aber auch Angestellte und Forscher und je Nutzergruppe können hier verschiedene Authentifizierungsfaktoren und Prozeduren zum Tragen kommen. Es ist denkbar, dass für Studenten eine Authentifizierung mit Benutzername und Passwort ausreichend ist, wohingegen Angestellte z.T. mehrere Authentifizierungsfaktoren benötigen. Zur Kommunikation von Authentication-Assurance-Information greifen die publizierten Versionen [Zie18, REF18c, Zie17, REF17] daher auf die Verwendung des nutzerspezifischen SAML Authentication Context bzw. OIDC acr zurück, wohingegen Identity-Assurance-Information anhand des Attributs *eduPersonAssurance* kommuniziert wird.

Das UML-Sequenzdiagramm in Abbildung 4.2 verdeutlicht hier exemplarisch anhand des Protokolls SAML, wie ein Identity Provider das Ein-Faktor-Authentifizierungs-Profil im Authentifizierungskontext setzt und mit dem entsprechenden Wert auf eine Anfrage des Service Providers antwortet.

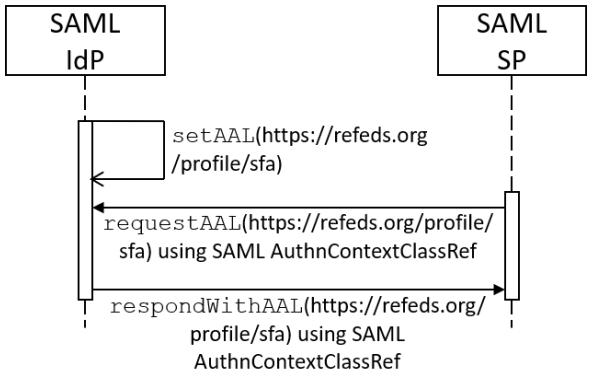


Abbildung 4.2: Anfragen eines Authentication-Assurance-Profils

Im nachfolgenden Abschnitt wird die Architektur hinsichtlich eines Konzeptes für Service Provider zur Auswahl eines angemessenen Authentication Assurance Levels bzw. Profils erweitert. Hier werden Service Provider unter Verwendung eines risikobasierten Ansatzes bei der Wahl, welches der oben erläuterten Profile, d.h. SFA oder MFA, zum Schutz des durch den Service Provider bereitgestellten Dienstes benötigt wird, unterstützt. Dazu werden weitere Komponenten, im Besonderen Informationsobjekte, eingeführt.

4.3 Architekturteil RM: Konzept zur Auswahl eines angemessenen Authentication-Assurance-Profils

Ein weiteres Teilziel dieser Arbeit (Hauptanforderung RM) stellt ein Konzept für Service Provider zur Auswahl eines angemessenen Authentication-Assurance-Profils dar. Das Grundge-

rüst der erforderlichen Authentication-Assurance-Profile (d.h. SFA- und MFA-Profil) wurde dazu bereits in Abschnitt 4.2 vorgestellt.

Die Tatsache, ob ein Service Provider ein stärkeres Authentication-Assurance-Profil (z.B. MFA-Profil) für den Zugriff auf dessen Dienst bzw. Ressourcen benötigt oder nicht, sollte dem Prozess des Risikomanagements unterliegen und regelmäßig re-evaluiert werden. Die Herausforderung an dieser Stelle ist jedoch, dass Service Provider u. U. keinen formalen Risikomanagement-Prozess etabliert haben (wie er bspw. in der ISO/IEC 27001 definiert ist) und daher bei der Evaluation eines angemessenen Authentication-Assurance-Profils Unterstützung benötigen. Da ein umfassender Risikomanagement-Prozess außerhalb des Fokus dieser Arbeit ist und eine eigene Problemstellung in (inter-) föderierten Szenarien darstellt, wird an dieser Stelle, kompatibel und in Abstimmung mit den Authentication-Assurance-Profilen aus Abschnitt 4.2, ein **risikobasierter Ansatz für Service Provider** zur Auswahl eines angemessenen Authentication-Assurance-Profils gewählt. Dieser dient als praxisbezogene Hilfestellung und Anleitung und wird in Abschnitt 5.3 anhand von veranschaulichenden Beispielsszenarien untermauert.

Dazu wird in Abschnitt 4.3.1 das Organisationsmodell aus Architekturteil AK aufgegriffen. Ferner wird dargestellt, um welche Komponenten das Informations-, das Funktions- und das Kommunikationsmodell (vgl. Abschnitte 4.3.2 bis 4.3.4) zu erweitern ist, sodass alle involvierten Komponenten der Architekturteile AK und RM vollständig erfasst sind.

4.3.1 Erweiterung des Organisationsmodells

Bei Betrachtung des Organisationsmodells, d.h. der in Abschnitt 4.2.1 eingeführten, involvierten Rollen und Software zeigt sich, dass die für den Architekturteil RM erforderlichen, zentralen Rollen und Softwarekomponenten bereits in Architekturteil AK erfasst wurden. Die UML-Klasse `ServiceProvider` mit dem Stereotyp *«role»* repräsentiert einen Service Provider, der gemäß des Schutzbedarfes seines FIM-fähigen Dienstes bzw. seiner Dienste ein angemessenes Authentication-Assurance-Profil wählt. Da, wie bereits beschrieben, ein risikobasierter Ansatz Anwendung findet, wird die Klasse `ServiceProvider` um das Attribut `riskManager` ergänzt (siehe Abbildung 4.3). Der Risk Manager ist eine Sub-Rolle des Service Providers, wobei dessen Namensgebung aus dem IT Service Management stammt. Gemäß IT Service Management besitzt ein Risk Manager die Verantwortung des Prozesses Risikomanagement, der sich mit der Identifikation, Bewertung und Behandlung von Risiken befasst. Während im klassischen IT Service Management alle Risiken innerhalb eines definierten Anwendungsbereiches, z.B. innerhalb einer Organisation, zu managen sind, liegt der Fokus dieser Sub-Rolle, aufgrund des Kontextes dieser Arbeit, auf dem authentifizierungsbezogenen Risiko des unberechtigten Zugriffs auf einen FIM-Dienst. Um das Risiko eines unberechtigten Zugriffs auf einen FIM-Dienst zu mindern, kommen idealerweise verschiedene Maßnahmen zum Tragen, wovon eine der Maßnahmen die Auswahl eines angemessenen Authentication-Assurance-Profils darstellt. Die Sub-Rolle `Risk Manager` befasst sich somit, wie man nach der Einführung der Informationsobjekte in Abschnitt 4.3.2 noch sehen wird, mit der Auswahl eines angemessenen Authentication-Assurance-Profils unter Berücksichtigung der involvierten Assets und potentiellen Schadenskategorien.

Die SP-seitige Softwarekomponente `FIMswSP`, die das ausgewählte Authentication-Assurance-Profil anfrägt (vgl. Funktion `requestAAL()` in Abschnitt 4.2.3) und verarbeitet, wurde dazu bereits im Architekturteil AK erfasst.

4.3.2 Erweiterung des Informationsmodells

Im nächsten Schritt wird das in Architekturteil AK erarbeitete Informationsmodell um die Informationsobjekte zur Auswahl eines angemessenen Authentication-Assurance-Profils ergänzt. Die dafür erforderlichen Informationsobjekte sind in Abbildung 4.3 visualisiert.

Wie bereits im vorherigen Abschnitt erläutert, stellt der Fokus dieses Konzeptes bzw. Teillösung, das Mindern des Risikos des unberechtigten Zugriffs durch Auswahl eines angemessenen Authentication-Assurance-Profils dar. Das Risiko des unberechtigten Zugriffs wird dazu in Abbildung 4.3 durch die Klasse `AuthenticationRisk` repräsentiert. Risiken wirken dabei stets auf einen Wert des Unternehmens (engl. *Asset*) [ISO13a], wobei ein Asset bspw. durch einen FIM-fähigen Dienst zugreifbar wird. Aus diesem Grund wird ebenfalls die Klasse `Asset` eingeführt, die durch den Service Provider bzw. durch die Sub-Rolle Risk Manager in Zusammenarbeit mit dem jeweiligen Asset Owner zu schützen ist. Assets können verschiedene Ausprägungen annehmen (z.B. Daten, Software, Hardware) weswegen die Klasse `Asset` ebenfalls mit dem Attribut `category` versehen ist.

Ein Risiko entsteht, wenn eine Schwachstelle eines Wertes durch eine Bedrohung ausgenutzt werden kann [ISO13a]. Aus diesem Grund werden der Klasse `AuthenticationRisk` die beiden Attribute `threat` und `weakness` hinzugefügt. Welche möglichen Kombinationen einer Bedrohung und Schwachstelle zu diesem Risiko führen, ist nicht Teil der Arbeit und wird an dieser Stelle abstrahiert. Im Kontext von Authentifizierungen und des unberechtigten Zugriffs sind Bedrohungen jedoch häufig willentlicher Natur, z.B. durch Impersonation, Social Engineering oder durch das Verwenden nicht rechtzeitig deaktivierter Benutzeraccounts. Schwachstellen können u.a. Mensch, Maschine sowie die authentifizierungsbezogenen Verfahren sein. Bei Betrachtung des Beispiels eines unberechtigten Zugriffs durch Social Engineering versucht ein Angreifer (hier: Bedrohung) einem Nutzer (hier: Schwachstelle) das Passwort zu entlocken. Durch das Erfordern des MFA-Profils kann an dieser Stelle das Risiko gemindert werden, da ein Angreifer zwar (bei einem erfolgreichen Angriff) das Passwort erhalten würde, ein Angreifer aber nicht direkt auf den Dienst zugreifen könnte, da er auch den zweiten Faktor kennen und kompromittieren müsste.

Es ist jedoch zu berücksichtigen, dass nicht alle Bedrohungen und Schwachstellen durch die Auswahl eines angemessenen Authentication-Assurance-Profils gemindert werden, weswegen noch weitere Maßnahmen zum Einsatz kommen sollten, welche nicht im Fokus dieser Arbeit sind. Dazu zählen bspw. Authentifizierungsfehler, wobei das Risiko des unberechtigten Zugriffs aufgrund veralteter Systeme (hier: Schwachstelle Maschine) entsteht. In diesem Kontext sind weitere Maßnahmen erforderlich, wie bspw. das Aktuellhalten der Software durch regelmäßige Sicherheitsupdates, was außerhalb eines Authentication-Assurance-Profils zu adressieren ist.

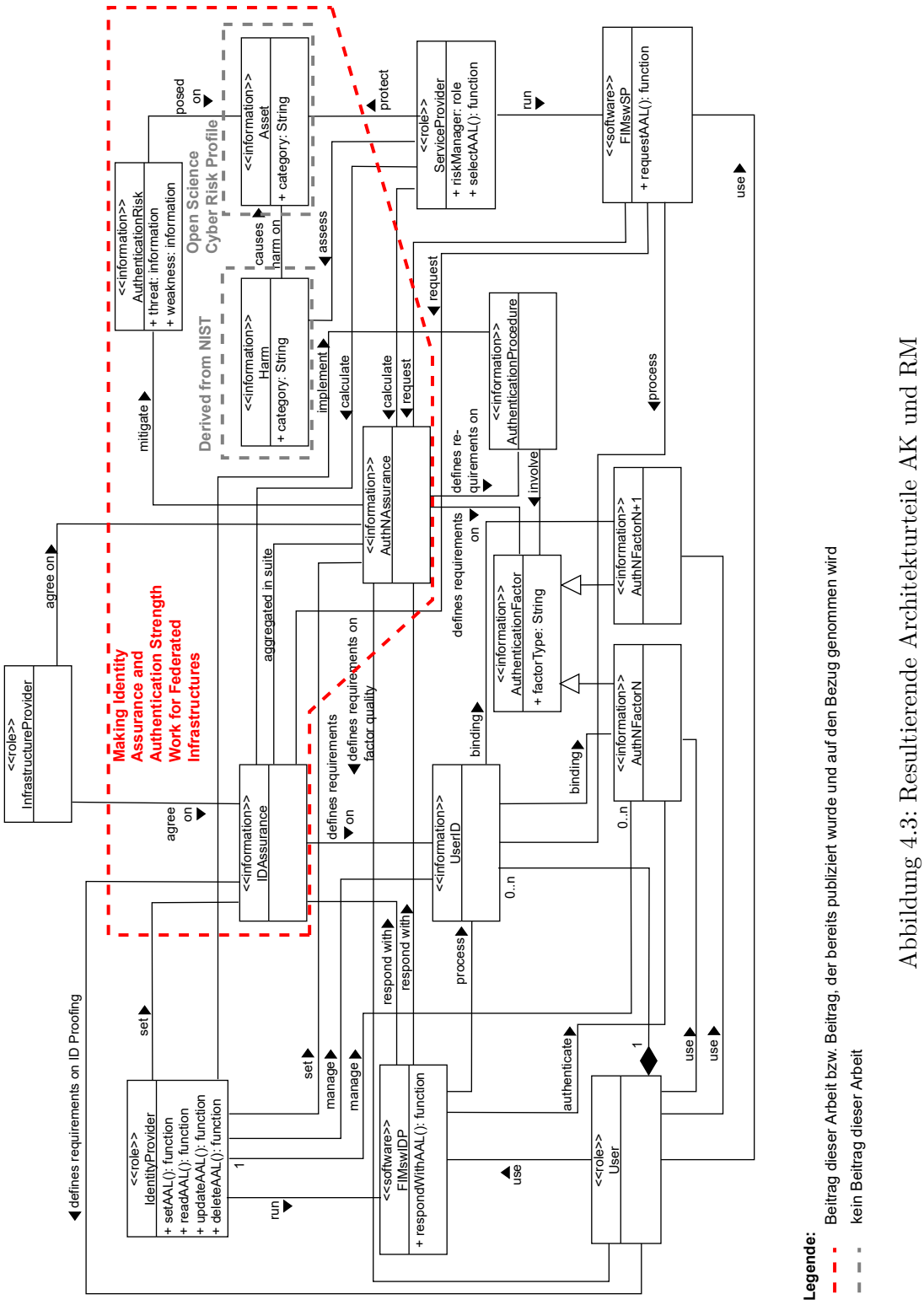


Abbildung 4.3: Resultierende Architekturteile AK und RM

Zusätzlich zu den beiden Klassen `AuthenticationRisk` und `Asset` wird die Klasse `Harm` mit dem Attribut `category` eingeführt. `Harm` repräsentiert potentielle Schäden, die durch den unberechtigten Zugriff auf ein Asset entstehen können (z.B. Reputationsverlust, finanzieller Schaden), sodass die Schadensklassen folglich bei der Auswahl eines angemessenen Authentication-Assurance-Profils zu berücksichtigen sind.

Nach der Einführung der zentralen Informationsobjekte im Rahmen des Architekturteils RM zeigt Abbildung 4.3, welche Komponenten und Konzepte wie kombiniert werden, um zur Erfüllung der Hauptanforderung RM beizutragen. Dazu wurde, analog zu dem Vorgehen in Abschnitt 4.2.2, die Abbildung 4.3 um farbliche Markierungen erweitert.

Die rote Box umsäumt dabei alle zur Erfüllung der Hauptanforderung RM benötigten Informationsobjekte. Hierbei wird das in Abschnitt 4.2 erläuterte Authentication-Assurance-Konzept berücksichtigt sowie das authentifizierungsbezogene Risiko des unberechtigten Zugriffs. Ferner wird auf die beiden bestehenden Konzepte (siehe graue Markierungen), das Open Science Cyber Risk Profile [PVWB+20] zur Klassifikation von Assets sowie auf abgeleitete Schadenskategorien von NIST [GGF17b] zurückgegriffen. Die Vorgehensweise, zusammen mit Anwendungsbeispielen, wurde bereits in dem Paper *Making Identity Assurance and Authentication Strength Work for Federated Infrastructures* [ZSG+21a] veröffentlicht, weswegen in Kapitel 5 auf die bereits publizierten Ergebnisse Bezug genommen wird.

Im nächsten Schritt wird das Funktionsmodell des Architekturteils AK erweitert.

4.3.3 Erweiterung des Funktionsmodells

Der Funktionsbereich zur Auswahl eines angemessenen Authentication-Assurance-Profils unter Verwendung eines risikobasierten Ansatzes steht, wie in den vorherigen Abschnitten ersichtlich wurde, in engem Zusammenhang mit dem Funktionsbereich Authentication Assurance aus Abschnitt 4.2.3. Da durch den Funktionsbereich Authentication Assurance somit bereits ein Großteil der Funktionen erfasst wurde, wird an dieser Stelle nur die SP-seitige Funktion zur Auswahl eines Authentication-Assurance-Profils, hier und in Abbildung 4.3, ergänzt.

- **selectAAL()**: Diese Funktion repräsentiert die Auswahl eines passenden Authentication-Assurance-Profils (d.h. SFA oder MFA) basierend auf der Kritikalität der zugreifbaren Assets. Zur Erfüllung der Funktion und dem darauffolgenden Anfragen eines Authentication-Assurance-Profils (d.h. `requestAAL()`) wird ein pragmatisches Vorgehen benötigt, welches in Abschnitt 5.3 unter Verwendung der Informationsobjekte beschrieben wird.

Die Abschnitte 4.2.3 und 4.3.3 zusammenfassend zeigt sich, dass bisher keine neuen Funktionen eingeführt werden mussten, da viele der dargestellten Funktionen bereits vorhanden sind (z.B. `setAAL()`, `selectAAL()`), deren Erfüllung bzw. Ausführung in den Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen aus Kapitel 2 aber häufig aufgrund des Mangels einheitlicher und unterstützender Konzepte scheitert.

4.3.4 Erweiterung des Kommunikationsmodells

Wie aus den Abschnitten 4.3.1 bis 4.3.3 ersichtlich wurde, ist eine Erweiterung des Kommunikationsmodells an dieser Stelle nicht notwendig, da die in dem vorherigen Abschnitt eingeführte Funktion `selectAAL()` durch den Service Provider und dessen Sub-Rollen selbst zu erbringen ist und daher keine Interaktion mit einer der anderen (externen) Rollen erfordert.

4.4 Architekturteil WF: Konzeption eines Fallback MFA-Workflows

Neben dem Authentication-Assurance-Konzept und dem risikobasierten Ansatz zur Auswahl eines angemessenen Authentication-Assurance-Profils stellt ein weiteres Teilziel dieser Arbeit die Konzeption eines MFA-Workflows dar (vgl. Hauptanforderung WF in Abschnitt 2.5), sodass Benutzer deren Heimatorganisation über keine Multi-Faktor-Authentifizierung verfügen, anhand eines Fallback MFA-Workflows trotzdem auf Dienste zugreifen können, die MFA erfordern. Da ein derartiger Workflow für proxy-basierte Föderationen bzw. Infrastrukturen bereits existiert (vgl. Abschnitt 2.4), konzentriert sich diese Arbeit auf die Unterstützung vollvermaschter Föderationsarchitekturen (i.S.v. Full Mesh). Jedoch sind die hier erarbeiteten Erweiterungen auch auf Proxy-Szenarien übertragbar bzw. integrierbar (vgl. Abbildung 4.4).

Die Herausforderung bei der Etablierung einer Multi-Faktor-Authentifizierung in FIM-Szenarien ist, dass meist ein Henne-Ei-Problem besteht. Identity Provider stellen üblicherweise kein MFA für FIM bereit, solange dies nicht von Service Providern gefordert wird. Umgekehrt besteht jedoch die Problematik, dass sobald Service Provider MFA verpflichtend einführen, potentiell Nutzer, deren Heimatorganisation über keine MFA-Implementierung verfügt, ausgeschlossen werden. Das hier erarbeitete Konzept eines Fallback-MFA Workflows unter Verwendung eines externen Zweitfaktor-Prüfers versucht daher IDP-seitig kaum technische Anpassungen vorzunehmen, indem die Faktoren SP-seitig zusammengeführt werden.

Der Fokus an dieser Stelle ist jedoch nicht das Design einer Softwarekomponente oder eines Servers für MFA, da es hier bereits eine Vielzahl an kommerziellen sowie Open Source Produkten gibt, sondern vielmehr wie, v.a. unter Berücksichtigung der Anforderungen [NFA_Integrierbarkeit], [FA_Koexistenz] und [NFA_Skalierbarkeit], ein externer Zweitfaktor-Prüfer in einen existierenden 1FA-Workflow einer vollvermaschten Infrastruktur integriert werden kann. Aus diesem Grund ist an dieser Stelle v.a. das Kommunikationsmodell, das in Abschnitt 4.4.4 betrachtet wird, relevant. Dazu muss der existierende 1FA-Workflow (vgl. Beschreibung in Abschnitt 2.2 und Abbildung 3.2) erweitert sowie Anpassungen an den bereits vorhandenen Komponenten vorgenommen werden. Zur Realisierung des MFA-Workflows mit externem Zweitfaktor-Prüfer wird an späterer Stelle (vgl. Abschnitt 6.3) auf Open Source Software zurückgegriffen (vgl. Anforderung zur Realisierbarkeit mit Standard-Software [NFA_Realisierbarkeit]).

Der Architekturteil WF zur Konzeption eines MFA-Workflows schlägt vor, dass der erste Authentifizierungsfaktor (hier repräsentiert durch die Klasse `AuthNFactorN`) nach wie vor IDP-seitig[6] bereitgestellt wird, während ein zweiter bzw. weiterer Faktor (`AuthNFactorN+1`) durch einen externen Faktorprüfer, hier als Two-Plus Provider (`TwoPlusProvider`) bezeichnet, bereitgestellt wird. Der Vorteil aus Perspektive der Security ist, dass im Falle eines kompromittierten IDPs (`FIMswIDP`), die dort abgesetzten, unrechtmäßigen Authentifizierungen aufgrund der Einführung eines externen Faktorprüfers nicht zu einem erfolgreichen Zugriff auf die Ressourcen des Service Providers führen.

Jedoch soll nicht, wie bei der in Abschnitt 3.5.3 beschriebenen SP-seitigen Realisierung, jeder Service Provider selbst eine Two-Plus Instanz implementieren, da sonst ein Nutzer eine Vielzahl von Zweitfaktoren registrieren und verwalten müsste (vgl. Anforderung [NFA_Unabhängigkeit]). Die Idee an dieser Stelle ist, dass `FIMswSP` unter Berücksichtigung der [FA_Benutzbarkeit] derart erweitert wird, dass SP-seitig lediglich die Faktoren aus mehreren Quellen zusammenführt bzw. aggregiert werden, wobei der zweite bzw. weitere Faktor durch einen beliebigen Two-Plus Provider betrieben und gewartet wird. Aus Sicht eines Nutzers wählt dieser (je nach Policy-Modell) entweder einen beliebigen TPP aus oder registriert einen Faktor bei einem durch die Heimatorganisation oder Service Provider befürworteten TPP.

Die Abbildung 4.4 verdeutlicht beispielhaft, wie das gemäß der Szenarien von nationalen Identitätsföderationen und deren Zusammenschluss zu einer Interföderation aussehen könnte.

Zusätzlich zu den bereits vorhandenen Identity Providern und Service Providern kommen ebenfalls dedizierte Zweitfaktor-Prüfer hinzu (vgl. Kreise mit „TPP“). Aufgrund des strukturellen Aufbaus der Interföderation, sind diese, analog zu den Identity Providern und Service Providern, in einer der nationalen Föderationen registriert. Die Nutzung eines TPPs aus einer Föderation, z.B. der Föderation B, ist jedoch nicht zwangsweise auf die Teilnehmer der Föderation B beschränkt, sondern kann prinzipiell auch von Teilnehmern anderer Föderationen in Anspruch genommen werden.[7] Die Sinnhaftigkeit der Nutzung hängt dabei aber auch von den durch die TPP implementierten, individuellen Verfahren ab. Stellt ein TPP bspw. nur eine persönliche, vor-Ort Bindung des Zweitfaktors zur Verfügung, wäre dies für Nutzer einer anderen Föderation aufgrund der räumlichen Distanz eher ungünstig. Es wäre jedoch denkbar, dass sich ein Nutzer aufgrund eines Projekttreffens oder einer Konferenz zufällig an diesem Ort befindet und er somit Zweitfaktoren verschiedener TPPs mit unterschiedlich starker Assurance „sammelt“, sodass ein Nutzer bei einem MFA-fordernden Dienst einen beliebigen TPP wählen kann (vgl. Anforderung [FA_Dynamik]).

[6] Der Begriff *IDP-seitig* bezeichnet den Sachverhalt, dass, aus dem Blickwinkel eines Service Providers, der erste Faktor aus der Domäne einer Heimatorganisation bzw. Identity Providers stammt, unabhängig davon ob der `IdentityProvider` den ersten Faktor tatsächlich selbst authentifiziert oder nicht. Es ist ebenfalls denkbar, dass ein SAML IDP (`FIMswIDP`) von einem `IdentityProvider` betrieben wird, der lediglich die Stammdaten seiner Nutzer verwaltet, während an `FIMswIDP` ein beliebiges (externes) Authentifizierungsverfahren angeschlossen ist. Aus Sicht des SPs stammt der erste Authentifizierungsfaktor jedoch in beiden Fällen von Seiten des IDPs.

[7] Dies hängt jedoch davon ab, ob der TPP den Dienst der gesamten Interföderation zur Verfügung stellt oder ob er nur für einen eingeschränkten Adressatenkreis (z.B. Föderationsmitglieder) konzeptioniert wurde.

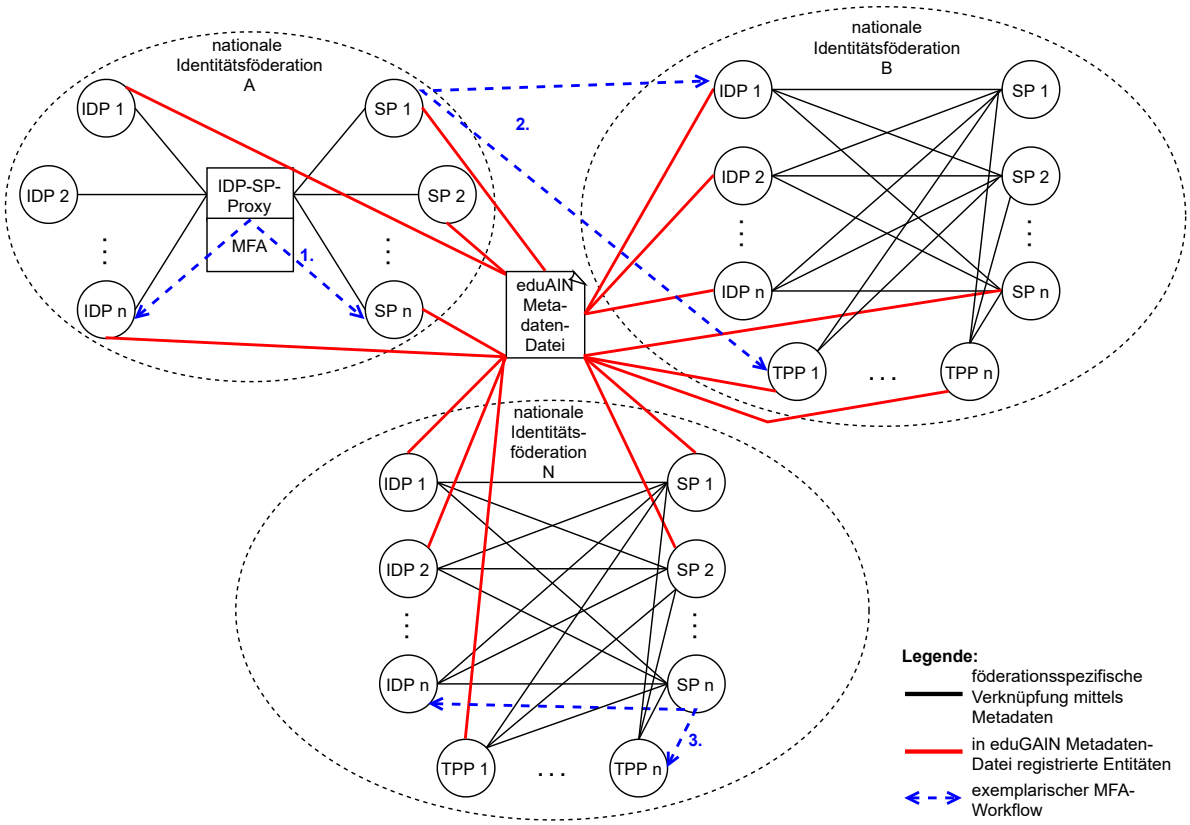


Abbildung 4.4: Konzeption eines Fallback MFA-Workflows verdeutlicht anhand der Szenarien nationales FIM und Inter-FIM

Der exemplarische MFA-Workflow Nummer 1 in Abbildung 4.4 verdeutlicht, das die föderationsspezifischen MFA-Implementierungen (hier: MFA unter Verwendung eines IDP-SP-Proxies) nach wie vor genutzt werden können. MFA-Workflow Nummer 2 zeigt, dass der Fallback MFA-Workflow ebenfalls von SPs einer Hub&Spoke Föderation angewendet werden kann, sofern dieser die entsprechende Erweiterung implementiert. MFA-Workflow Nummer 3 stellt klar, dass analog zu den IDPs und SPs einer Föderation nicht alle TPPs zwangsweise an der Interföderation teilnehmen müssen. Somit kann es auch TPPs geben, die nur Teilnehmern einer bestimmten Föderation eine Zweitfaktor-Prüfung zur Verfügung stellen.

Es sei an dieser Stelle nochmals darauf hingewiesen, dass das Konzept eines Two-Plus Providers als Fallback-Lösung anzusehen ist, da durch das Auslagern von Authentifizierungsfaktoren an externe Two-Plus Provider neue Herausforderungen entstehen, z.B. wie weitere Faktoren mittels Identitätsfeststellung an Personen gebunden werden können. Je länger die Vertrauensketten werden, desto größer werden potentielle Angriffsflächen.

Anhand des skizzierten MFA-Workflow Konzeptes hat der Nutzer auch die Kontrolle wo seine Daten verarbeitet und gespeichert werden. Ferner berücksichtigt das Funktionsmodell in Abschnitt 4.4.3 die Anforderung [DSA_Datenminimalisierung], sodass seitens der TPP nur möglichst wenig personenbezogene Daten verarbeitet und gespeichert werden müssen.

Zur Realisierung des MFA-Workflows wird größtenteils auf bereits vorhandene Konzepte aus föderierten Protokollen zurückgegriffen, die jedoch zum Zwecke einer Multi-Faktor-Authentifizierung, soweit bekannt, auf eine derartige Weise noch nicht miteinander kombiniert wurden, sodass folglich der gesamtheitliche Workflow als neu zu erachten ist. Obwohl bspw. die Security Assertion Markup Language (SAML) nicht nur ein Protokoll, sondern ein umfassendes Framework basierend auf mehreren Dokumenten ist, vgl. „*The Security Assertion Markup Language (SAML) standard defines a framework for exchanging security information between online business partners.*“[RHP+08], und die Kombination der verschiedenen Dokumente bzw. Spezifikationen verschiedene Anwendungsfälle abdeckt, fehlt bzgl. MFA der Aspekt der Interoperabilität, der beschreibt, wie die verschiedenen Elemente (wie bspw. Metadaten, Authentifizierungskontext, Attribute, Discovery) für verschiedene Multi-Faktor-Szenarien sinnvoll miteinander kombiniert werden können. Selbiges ist auch bei dem relativ jungen OpenID Connect Standard der Fall, da sich hier die Spezifikation zur Etablierung von multilateralen (n:m) Föderationen während der Entstehung dieser Arbeit noch im Draft-Status befindet.

Der in Abschnitt 3.5.4 skizzierte PoC unter Verwendung einer Attribute Authority ähnelt dem hier skizzierten Ansatz zwar, da Authentifizierungs- bzw. Assurance-Informationen SP-seitig zusammengeführt werden, jedoch leitet in dem PoC der SP einen Nutzer zu einem fest verdrahteten Zweitfaktor-Prüfer weiter und ermöglicht nicht die oben beschriebene Flexibilität unter Berücksichtigung mehrerer TPPs. Das hier skizzierte Konzept eines MFA-Workflows leistet daher einen wertvollen Beitrag indem:

- Er von Identity Providern in der Transitionsphase angewendet werden kann, bis MFA selbst IDP-seitig implementiert wird.
- Er für Identity Provider deren Ressourcenplanung auf lange Sicht keine eigenständige MFA-Implementierung vorsieht eine verlässliche und dauerhafte Lösung zur Multi-Faktor-Authentifizierung liefert.
- Er als Fallback verwendet werden kann, wenn eine IDP-seitige Implementierung (die bspw. in der Cloud gehostet wird) ausfällt.

Zur Konzeption des skizzierten MFA-Workflows werden neue Komponenten benötigt. Abschnitt 4.4.1 startet daher, analog zu Abschnitt 4.3.1, mit der Erweiterung des Organisationsmodells. Darauffolgend werden in den Abschnitten 4.4.2 - 4.4.4 das Informationsmodell, das Funktionsmodell sowie das Kommunikationsmodell erweitert.

4.4.1 Erweiterung des Organisationsmodells

Damit der oben skizzierte Fallback MFA-Workflow realisiert werden kann, wird zuerst die Rolle des sogenannten Two-Plus Providers eingeführt. Der Name „Two-Plus“ leitet sich daraus ab, dass ein IDP-seitig bereitgestellter Faktor durch einen zweiten bzw. weiteren Faktor eines externen Faktorprüfers erweitert wird.[8]

[8] Hier ist prinzipiell auch denkbar, dass eine Zwei-Faktor-Authentifizierung durch einen dritten Faktor eines Two-Plus Providers erweitert wird.

Der Abbildung 4.5 wird somit die folgende Rolle hinzugefügt:

- **Two-Plus Provider** (UML-Klasse `TwoPlusProvider`) Übergeordnete Rolle zur Aggregation eines externen Faktorbereitstellers bzw. -prüfers.

Die UML-Klasse `TwoPlusProvider` erhält dabei dieselben Funktionen, wie diejenigen der Klasse `IdentityProvider`. Hier wird z.T. bereits deutlich, dass es sich um eine Art spezialisierter Identity Provider handelt (siehe auch Anforderung [FA_Konformität], die die technische Konformität beschreibt). Während eine Attribute Authority ebenfalls ein spezialisierter Identity Provider ist, liegt der feine Unterschied beim Two-Plus Provider jedoch darin, dass dessen primäres Ziel die Authentifizierung von Zweitfaktoren (bzw. weiteren Faktoren) und nicht die Bereitstellung zusätzlicher Benutzerattribute ist.[9] Er lässt sich somit eher als eine „Authentication Authority“ beschreiben.

In Bezug auf die Assoziationen, mit denen der `TwoPlusProvider` in Abbildung 4.5 versehen ist, wird ebenfalls deutlich, dass diese fast deckungsgleich mit den Assoziationen der Klasse `IdentityProvider` sind. Der Unterschied besteht darin, dass die Klasse `IdentityProvider` auf `AuthNFactorN` Bezug nimmt, während der `TwoPlusProvider` die Klasse `AuthNFactorN+1` referenziert.

Ein weiterer Unterschied im Hinblick auf die Assoziationen ist, dass die Klasse `TwoPlusProvider` im Vergleich zur Klasse `IdentityProvider` nicht zwangsweise eine eigene `UserID` verwalten muss (vgl. Assoziation zwischen der Klasse `IdentityProvider` und `UserID`), da der `TwoPlusProvider` idealerweise die bereits existierende `UserID` wiederverwendet. Dazu muss jedoch vorab die `UserID` zwischen `IdentityProvider` und `TwoPlusProvider` ausgetauscht werden, sodass der Zweitfaktor an den korrekten Nutzer gebunden wird (siehe Kommunikationsmodell in Abschnitt 4.4.4). Alternativ kann der Two-Plus Provider auch einen eigenen User Identifier verwenden, dies hat allerdings zur Folge, dass die Verarbeitung auf Service Provider Seite komplizierter wird, da dieser dann eine Tabelle speichern muss, um die verschiedenen User Identifier eines Nutzers aufeinander abzubilden. Streng genommen ließe sich in letzterem Fall auch diskutieren, ob es sich noch um eine valide Multi-Faktor-Authentifizierung handelt oder ob es eher zwei Ein-Faktor-Authentifizierungen unterschiedlicher Identitäten desselben Benutzers sind.

Ferner wird die Architektur um die UML-Klasse `FIMswTPP` erweitert, die analog zu `FIMswIDP` eine authentifizierungsbezogene Softwarekomponente darstellt. Auch hier sind die eingefügten Assoziationen nahezu deckungsgleich mit denjenigen der Klasse `FIMswIDP`.

Hinzu kommt außerdem die UML-Klasse `FIMswDiscovery`, die die Softwarekomponente eines Lokalisierungsdienstes repräsentiert. Hierbei zeigt sich, dass einige Service Provider Implementierungen (siehe `FIMswSP`) bereits einen sogenannten *embedded discovery service* integrieren, sodass diese Klasse auch als Attribut der Klasse `FIMswSP` angesehen werden könnte. Da `FIMswDiscovery` an späterer Stelle jedoch noch von Relevanz sein wird, wird die Klasse aus Gründen der Übersichtlichkeit explizit und von `FIMswSP` getrennt modelliert.

[9] Natürlich müssen bei der Authentifizierung eines Zweitfaktors auch ein paar wenige Benutzerattribute übertragen werden, wie bspw. der User Identifier oder das o.g. eduPersonAssurance Attribut zur Kommunikation von Identity-Assurance-Information, jedoch stehen diese nicht im Vordergrund.

4.4.2 Erweiterung des Informationsmodells

Da durch den MFA-Workflow Informationsobjekte übertragen werden, die bereits im Architekturteil AK eingeführt wurden, kommen an dieser Stelle keine neuen Informationsobjekte hinzu.

Aus diesem Grund werden nachfolgend direkt die erforderlichen Funktionalitäten zur Erweiterung des existierenden 1FA-Workflows betrachtet.

4.4.3 Erweiterung des Funktionsmodells

Wie in Abschnitt 4.4.1 beschrieben, muss, bevor ein Nutzer den durch den TPP bereitgestellten Zweitfaktor nutzen kann, ein Austausch der UserID stattfinden, um den Authentifizierungsfaktor an die vorhandene, föderierte Identität des Nutzers zu binden.[10] Ein Austausch findet dabei durch die beiden Funktionen `requestUID()` und `respondWithUID()` statt, während die Bindung des Zweitfaktors an den Nutzer bzw. die UserID der föderierten Identität durch die Funktion `createBinding()` geschieht. In der Auflistung am Ende des Abschnitts sind die Funktionen, zusammen mit den anderen Funktionen, nochmals übersichtlich aufgelistet. In Abschnitt 4.4.4 wird dann im Rahmen des Kommunikationsmodells das Zusammenspiel der Funktionen aufgezeigt.

Aus Gründen der Vollständigkeit werden ebenfalls die Funktionen `readBinding()`, `updateBinding()` und `deleteBinding()` aufgelistet, obwohl diese nicht unmittelbar für die initiale Bindung benötigt werden. Die drei Funktionen finden eher in späteren Stadien Anwendung, um bspw. eine bestehende Bindung zu aktualisieren oder zu löschen.

Nachdem die Bindung des Authentifizierungsfaktors bei dem TPP an den Nutzer erfolgt ist, kann der Nutzer diesen nun verwenden. Bei der Zugriffsanfrage auf einen MFA-fordernden Dienst durchläuft ein Nutzer (dessen IDP über keine MFA-Implementierung verfügt) zunächst den regulären 1FA-Workflow, d.h. zuerst Auswahl des IDPs beim Lokalisierungsdienst, dann Authentifizierung des ersten Faktors. Aufgrund der nicht stattgefundenen IDP-seitigen Multi-Faktor-Authentifizierung wird der Nutzer dann erneut zum Lokalisierungsdienst geleitet, um den externen Two-Plus Provider auszuwählen, bei dem der Zweitfaktor registriert wurde. Abbildung 4.4 verdeutlicht hier, dass gemäß des hier erarbeiteten Konzepts in einer (Inter-) Föderation prinzipiell beliebig viele TPPs registriert sein können. Somit ist auch denkbar, dass ein Nutzer mehrere Zweitfaktoren bei verschiedenen TPPs registriert hat und diese beliebig verwenden kann.

Um eine dynamische Auswahl eines TPP durch den Benutzer zu ermöglichen, müssen alle TPPs einer (Inter-) Föderation mit einem entsprechenden Flag versehen und veröffentlicht werden. Dazu wird die Funktion `publishEntities()` eingeführt. Anhand dieses Flags grenzen sich TPPs von IDPs ab, sodass beim zweiten Durchlauf des Lokalisierungsdienstes nicht

[10] Der Anwendungsfall bei dem eine eigene, durch den TPP etablierte UserID verwendet wird, die dann später durch den Service Provider aufeinander abgebildet werden, wird hier nicht im Detail betrachtet.

sowohl IDPs und TPPs, sondern nur noch TPPs angezeigt werden. Zum Filtern wird die Funktion `filterEntities()` eingeführt, die auf das entsprechende Flag zugreift.[11]

Zum Zwecke des Filterns ist es zunächst ausreichend, wenn lediglich die TPPs ein derartiges Flag besitzen. Zur Erfüllung der wünschenswerten Anforderung [FA_Messbarkeit] müssten ebenfalls die IDPs um ein Flag, welches angibt ob ein IDP überhaupt MFA unterstützt oder nicht, erweitert werden.[12] Jedoch kann anhand des Flags nicht abgelesen werden, ob MFA tatsächlich bei einer Benutzerauthentifizierung stattgefunden hat, da dies erst zur Laufzeit ersichtlich wird.

Nachdem ein Nutzer den durch MFA erweiterten 1FA-Workflow durchlaufen hat, müssen letztlich noch die durchgeführten Authentifizierungen SP-seitig zusammengeführt werden. Dazu wird die Funktion `aggregateAAL()` eingeführt, die die verschiedenen, mit den Authentifizierungen bzw. Authentifizierungsfaktoren verbundenen Authentication-Assurance-Profile aggregiert.

Die folgende Auflistung gibt einen Überblick über die hier relevanten Funktionen. Diese werden in Abbildung 4.5 den entsprechenden Klassen zugeordnet. Rot markierte Klassen, Assoziationen und Funktionen repräsentieren dabei die für den Architekturteil WF benötigten Komponenten zur Realisierung des Fallback MFA-Workflows.

Wie die Funktionen dann genau zusammenspielen, ist Teil des Kommunikationsmodells.

- **requestUID()**: Anfragen der UserID eines Nutzers.
- **respondWithUID()**: Antworten mit der UserID eines Nutzers.
- **createBinding()**: Stellt das Verknüpfen des Nutzers bzw. dessen User Identifiers mit dem Zweitfaktor dar.
- **readBinding()**: Repräsentiert das Auslesen der Verknüpfung.
- **updateBinding()**: Repräsentiert das Aktualisieren der Verknüpfung, bspw. bei Verlust des Authentifizierungsfaktors.

[11] Das Filtern von Entitäten ist innerhalb der Community ein Diskussionsthema, da deren Kritiker negativ anmerken, dass die dem Benutzer zur Verfügung stehende Auswahl nicht eingeschränkt werden sollte, da dies zu einer Verschlechterung der Benutzbarkeit führt. Hier ist jedoch zu betonen, dass die Benutzerauswahl zu Beginn (d.h. bei Auswahl des IDPs) nicht einschränkt wird und die Filter-Funktion nur im zweiten Schritt zum Zwecke der Anzeige vorhandener TPPs angewendet wird. Dies wird im Gegensatz zum Filtern von IDPs, bei dem u.U. ein Benutzer seine Heimatorganisation gar nicht angezeigt bekommen würde, als Bedienungserleichterung erachtet. Da die Konzepte zur Discovery in SAML (d.h. statisch, auf Basis einer Metadatendatei) im Vergleich zu OIDC (d.h. dynamische Discovery und Registrierung, vgl. Abschnitt 3.2.2.3) unterschiedlich sind, kann der Workflow, je nach verwendetem Protokoll, an dieser Stelle ggf. unterschiedliche Ausprägungen annehmen.

[12] Als die Autorin dieser Arbeit die Chair-Position der REFEDS Assurance WG übernommen hat, wurde die Diskussion, ob die Authentication-Assurance-Profile ein derartiges Flag für IDPs erfordern sollten, erneut angestoßen. Aufgrund des Implementierungsaufwandes im Vergleich zum Nutzen (d.h. zur Generierung von Statistiken), wird dies durch die aktuellen Authentication-Assurance-Profile momentan nicht erfordert. Jedoch wurde in einem Empfehlungsdokument, das in [REF20a] verlinkt ist, eine regelmäßige Reevaluierung vorgeschlagen.

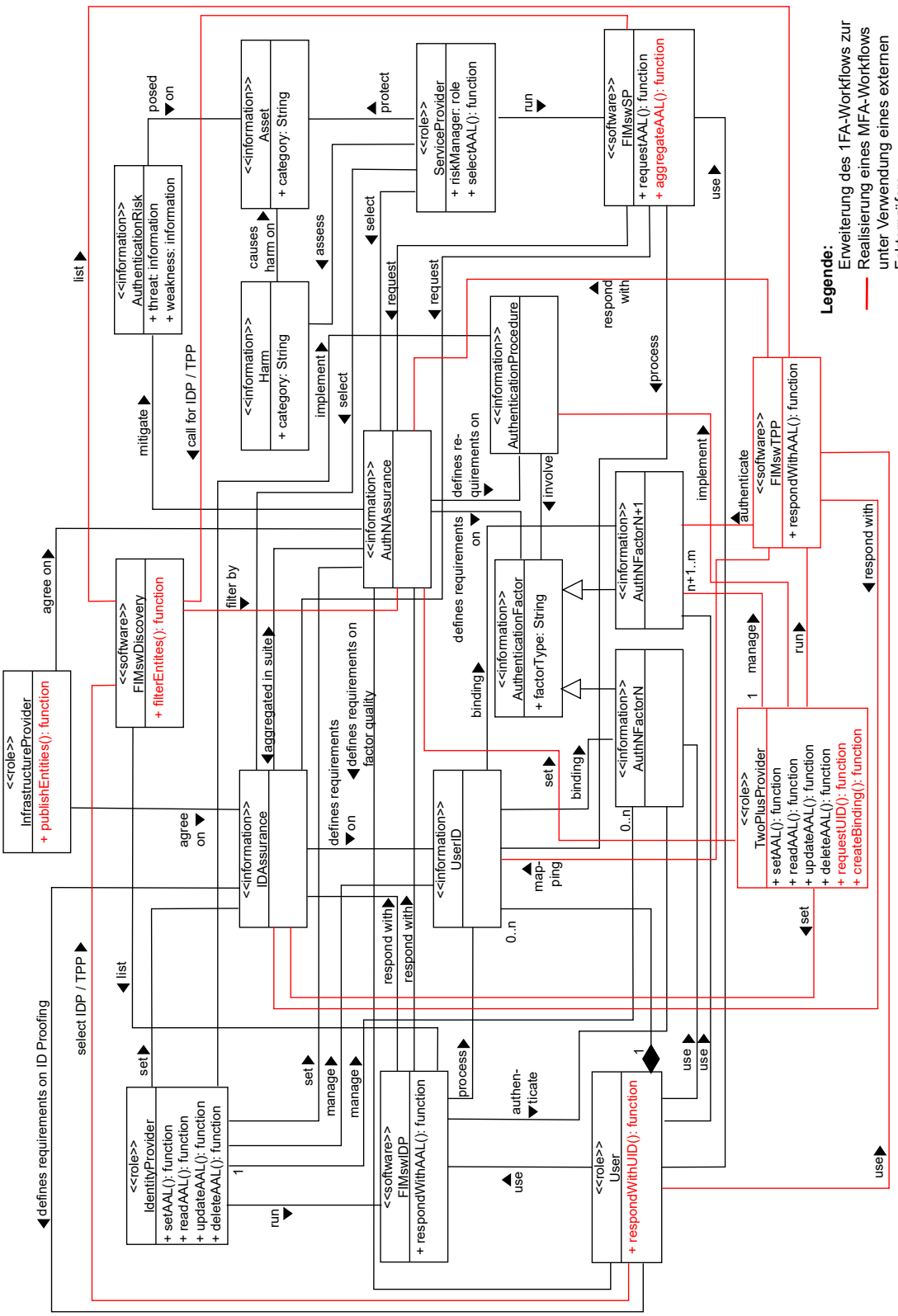


Abbildung 4.5: Resultierende Architekturteile AK, RM und WF

- **deleteBinding()**: Repräsentiert das Löschen bzw. Aufheben der Verknüpfung, bspw. wenn der Dienst nicht mehr genutzt wird.
- **publishEntities()**: Diese Funktion wird benötigt, um zwischen den verschiedenen Arten von Faktorprüfern (i.S.v. *1st factor only IDP*, *Two-Plus Provider*) zu unterscheiden, sodass einem Nutzer im Rahmen des Discovery-Prozesses stets die korrekten auswahlfähigen Faktorprüfer angezeigt werden.
- **filterEntities()**: Diese Funktion dient zum Filtern der Faktorprüfer bzw. Entitäten, sodass beim zweiten Durchlaufen der Discovery ausschließlich TPPs angezeigt werden.
- **aggregateAAL()**: Diese Funktion ist dafür zuständig, die aus potentiell verschiedenen Quellen stammenden Authentifizierungen und die damit verbundenen Authentication-Assurance-Profile zu aggregieren, um darauf basierend (neben anderen Kriterien) eine Zugriffsentscheidung zu treffen.

Die Abbildung 4.5 verdeutlicht, dass durch das SP-seitige Zusammenführen der Faktoren IDP-seitig zunächst keine technischen Anpassungen vorzunehmen sind (vgl. Anforderung [NFA_Einrichtungsauswand]). Der vorgeschlagene MFA-Workflow ist dabei dynamisch, in dem Sinne, dass Benutzer nicht statisch zu einem fest verdrahteten TPP weitergeleitet werden, sondern grundsätzlich zwischen beliebigen TPPs, die potentiell unterschiedliche Faktoren implementieren, wählen können. Dies setzt natürlich voraus, dass Faktoren bei dem/n entsprechenden TPP(s) registriert wurden.

4.4.4 Erweiterung des Kommunikationsmodells

In diesem Abschnitt findet auf Basis der zuvor definierten Funktionen eine Erweiterung des Kommunikationsmodells statt. Dazu wird zunächst der Zusammenhang der Funktionen `requestUID()`, `respondWithUID()` und `createBinding()` betrachtet, die für die initiale Bindung des durch den TPP bereitgestellten (Zweit-)faktors an die föderierte Identität des Benutzers benötigt werden. Dabei kann die UserID entweder vom Benutzer oder dessen Identity Provider bereitgestellt werden. Das UML-Sequenzdiagramm in Abbildung 4.6 verdeutlicht das Zusammenspiel der Funktionen grafisch.

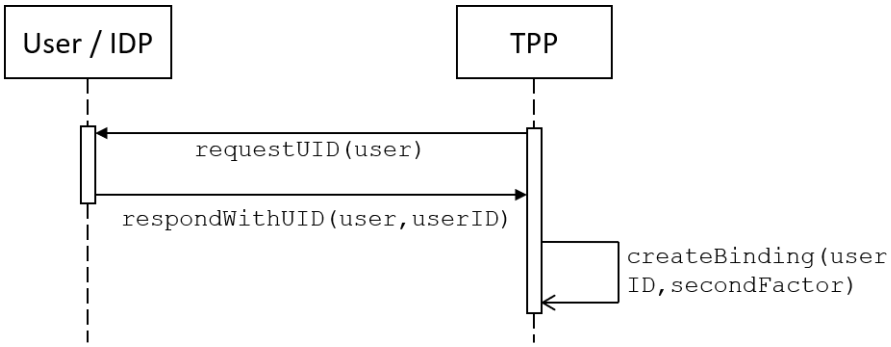


Abbildung 4.6: Bindung des Zweitfaktors an den Nutzer bzw. die UserID der föderierten Identität

Der in Abbildung 4.6 dargestellte Vorgang erfolgt dabei nicht unbedingt unter Verwendung von föderierten Protokollen, sondern kann auf einen beliebigen Kommunikationsmechanismus zurückgreifen. Bspw. kann hier ein durch den TPP bereitgestelltes Self-Service Portal zum Einsatz kommen; denkbar ist auch, dass das Anfragen der UserID via E-Mail erfolgt, während die Bereitstellung der UserID vor-Ort, durch den Nutzer am Service Desk des TPPs geschieht. Der (Zweit-)faktor wird dann nach der Überprüfung der Identität des Nutzers (z.B. Vorzeigen des Mitarbeiter- oder Personalausweises) an den Nutzer gebunden (`createBinding()`).

Nachdem der durch den TPP bereitgestellte Faktor an den Nutzer gebunden wurde, kann dieser für Authentifizierungen bei MFA-fordernden Diensten herangezogen werden. Die Schritte des MFA-Workflows unter Verwendung eines externen Faktorprüfers werden dabei im UML-Sequenzdiagramm in Abbildung 4.7 dargestellt. Da der Nachrichtenaustausch in SAML und OIDC im Groben ähnlich ist (d.h. Request-Response, Verwendung von Attributen bzw. Claims sowie Authentifizierungskontexten, Involvierung eines Lokalisierungsdienstes), wird an dieser Stelle vom konkreten Protokoll abstrahiert. In dieser Abbildung wird, analog zu Abbildung 4.6, zunächst nur das Zusammenspiel der in Abschnitt 4.4.3 erarbeiteten Funktionen betrachtet, während die Art und Weise der Implementierung unter Verwendung eines föderierten Protokolls Teil der Kapitel 5 und 6 ist.

Die Schritte vom Anfragen der Zielressource bis hin zum Zugriff, der wegen fehlender Authentifizierungsstärke hier nicht möglich ist, sind dabei analog zu denjenigen Schritten des 1FA-Workflows aus den Abbildungen 3.2 bzw. 3.3. Da in der Antwort des Identity Providers des Nutzers keine Aussage über eine stattgefundene Multi-Faktor-Authentifizierung enthalten ist, leitet der Service Provider den Nutzer daher zur Auswahl eines TPPs, wobei durch die Funktionen `publishEntities()` und `filterEntities()` IDPs aus der Auswahlliste herausgefiltert wurden.[13]

Nach der Authentifizierung des zweiten bzw. weiteren Faktors durch den TPP werden die Antworten aller Authentifizierungen durch den SP aggregiert (Funktion: `aggregateAAL()`). Entsprechen die durchgeführten Authentifizierungen den Erwartungen des Service Providers (z.B. Einhaltung der Verwendung unterschiedlicher Faktortypen) erhält der Nutzer Zugriff auf den Dienst.[14] Ist dies nicht der Fall erscheint eine Fehlermeldung und es muss u.U. ein anderer Faktortyp oder -prüfer verwendet werden.

Im nächsten Abschnitt wird die Architektur um den letzten Teil, einem Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien, erweitert.

[13] Abhängig von der Art und Weise der Implementierung sowie des verwendeten Protokolls. In SAML sind üblicherweise alle Entitäten (IDPs, SPs und TPPs) in einer zentralen Metadatendatei erfasst, sodass hier ein Filtern erforderlich ist. OIDC hingegen wendet Normalisierungsregeln an, um auf Basis einer Benutzereingabe (z.B. E-Mail-Adresse) den OpenID Endpunkt herauszufinden [SBJJ14].

[14] Zur Unterstützung dieser Funktionalität müssen die bereits publizierten Authentication-Assurance-Profile erweitert werden, was in Abschnitt 5.4 beschrieben wird.

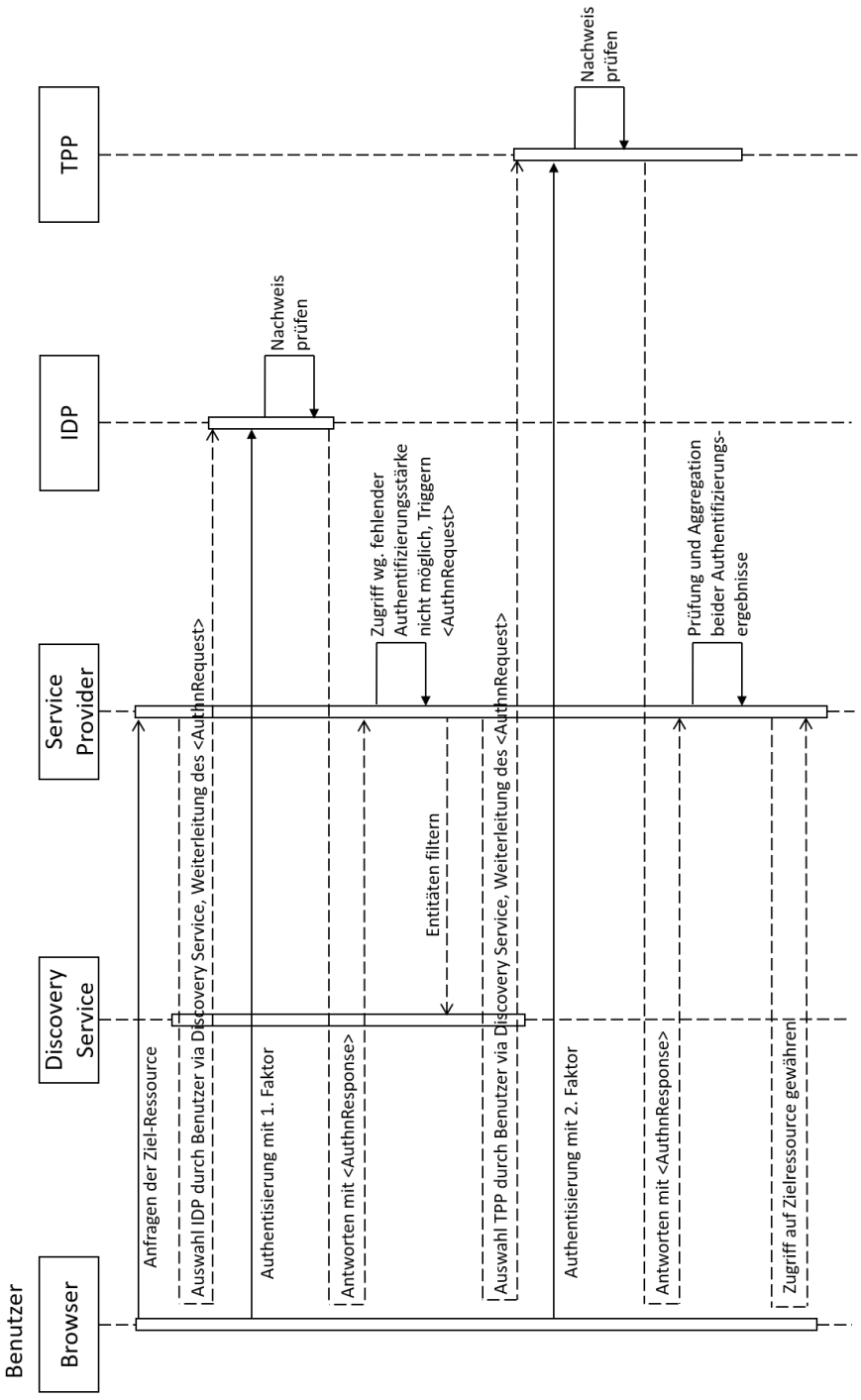


Abbildung 4.7: Fallback MFA-Workflow unter Verwendung eines externen Faktorprüfers

4.5 Architekturteil UM: Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien

Die Notwendigkeit für ein Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien ergab sich primär aus der Tatsache, dass eine bestehende, heterogene Infrastruktur um zusätzliche Komponenten und Konzepte zur Authentication Assurance und Multi-Faktor-Authentifizierung erweitert werden soll. Das Modell dient folglich dazu eine generische Beschreibungs- und Modellierungssprache für Authentifizierungsszenarien zu entwickeln und damit eine Grundlage zu schaffen, um existierende Authentifizierungsinfrastrukturen abzubilden und somit neue Komponenten leichter in eine bestehende Infrastruktur integrieren zu können. Da es sich vor allem in interföderierten Szenarien um hochgradig verteilte Umgebungen handelt, ist eine getreue Abbildung eines vorhandenen Authentifizierungsszenarios umso kritischer.

Ein Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien kann somit, wie oben erläutert, einerseits

- zur Einführung neuer Technologien,
- dem Design zukünftiger Architektur (-muster) und als
- Implementierungsgrundlage für zu integrierende Softwarekomponenten

verwendet werden und andererseits,

- zur Durchführung diverser Analysen (z.B. Security Analyse),
- als Grundlage für Simulationen als auch
- zur formalen Verifikation

herangezogen werden.

Anhand der Abbildung 2.9 wurden ebenfalls exemplarisch verschiedene Anwendungsfälle visualisiert, in denen ein derartiges Modell hilfreich sein kann.

Für eine *vollständige* Beschreibung von Authentifizierungsszenarien (vgl. v.a. die Anforderungen [FA_Service_Orientierung], [FA_Managementaspekte] und [FA_Nutzungsaspekte]) wurden in Abschnitt 3.7 verschiedene, existierende Modelle untersucht, wobei sich zeigte, dass das *MNM Service Model* [GHH+01, GHK+01, GHH+02] zur Beschreibung und Modellierung von Authentifizierungsszenarien erweitert werden kann, da dieses den gesamten Lebenszyklus eines Services berücksichtigt und verschiedene Sichten auf Services definiert. Zu diesem Zweck werden bei der Konzeption des hier vorliegenden Architekturteils Authentifizierungen nicht mehr als ein rein technischer Austausch von Authentifizierungsinformationen zwischen zwei Entitäten angesehen, da die Authentifizierung, v.a. unter dem Aspekt der *Service-Orientierung*, Qualitäten eines *Services* aufweist, der verschiedene Rollen, Prozesse, Funktionalitäten und Abhängigkeiten vereint (vgl. Abbildung 4.5, die v.a. die Rollen, Funktionalitäten und Abhängigkeiten der in der Architektur involvierten

Komponenten visualisiert). Ein weiterer, nicht zu vernachlässigender Punkt ist, dass zunehmend verschiedene Protokolle, Technologien, Rahmenwerke und Standards bei Authentifizierungen zum Einsatz kommen, weswegen bei der Konzeption dieses Architekturteils ebenfalls das Ziel der *Vergleichbarkeit* unter Verwendung einer einheitlichen Terminologie (vgl. [FA_Terminologie]) eine zentrale Rolle spielt. [ZS18]

Bei Betrachtung der oben aufgegriffenen Ziele bzw. Anforderungen an ein Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien zeigt sich, dass diese Anforderungen nicht direkt in Komponenten, gemäß der verwendeten Teilmodelle, transformierbar und in die Architektur integrierbar sind. Das Konzept zur Beschreibung und Modellierung von Authentifizierungsszenarien greift vielmehr bereits vorhandene Komponenten der Architektur auf und versucht diese, unter Verwendung eines vollständigen und vergleichbaren Modells auf eine generische, service-orientierte sowie protokoll-/technologie-/rahmenwerk- und standard-agnostische Art und Weise zu beschreiben und abzubilden [ZS18].

Aus diesem Grund werden in den Abschnitten 4.5.1 und 4.5.2 keine neuen Rollen, Softwarekomponenten und Informationsobjekte eingeführt. In Abschnitt 4.5.3 wird dann die CRUD-Funktionalität aufgegriffen und denjenigen Rollen zugeordnet, die idealerweise das Konzept zur Beschreibung und Modellierung anwenden. Eine Erweiterung des Kommunikationsmodells (vgl. Abschnitt 4.5.4) ist ebenfalls nicht notwendig, da eine Beschreibung und Modellierung der eigenen Authentifizierungsumgebung keinen Austausch mit anderen Rollen der Architektur erfordert.

Der Architekturteil UM in Abbildung 4.8 verdeutlicht daher neben der hinzugekommenen Funktionalität lediglich anhand farblicher Markierungen, für welche Komponenten auf das MNM Service Model zurückgegriffen werden kann und für welche Komponenten die Erweiterung des MNM Service Models zur Beschreibung und Modellierung von Authentifizierungsszenarien (in Kapitel 5 als *Universelles Service Modell für Authentifizierungsszenarien (UASM)* bezeichnet) herangezogen werden kann. Als *Work in Progress* wurden in [ZS18] bereits die Grundlagen von UASM geschaffen. Der Abschnitt 5.1 baut darauf auf und konkretisiert UASM.

4.5.1 Erweiterung des Organisationsmodells

Wie zuvor ersichtlich wurde, sollen anhand eines Konzeptes zur Beschreibung und Modellierung von Authentifizierungsszenarien existierende Strukturen vollständig und vergleichbar beschrieben und abgebildet werden. Aus diesem Grund ist eine Einführung neuer Rollen und Softwarekomponenten als Teil des Organisationsmodells nicht erforderlich.

4.5.2 Erweiterung des Informationsmodells

Analog zur Argumentation hinsichtlich des Organisationsmodells in Abschnitt 4.5.1, ist auch hier eine Erweiterung des Informationsmodells um neue Informationsobjekte nicht erforderlich. Im nächsten Schritt werden daher direkt die für diesen Teil der Architektur erforderlichen Funktionen betrachtet.

4.5.3 Erweiterung des Funktionsmodells

Dieser Funktionsbereich befasst sich mit der Analyse, der Beschreibung und der Modellierung einer Authentifizierungsumgebung und sollte idealerweise von jeder Rolle der Architektur (ausgenommen der Rolle *Nutzer*, vgl. dazu Abbildung 4.8) adressiert werden. Wie zu Beginn des Abschnitts 4.5 bereits erläutert, können derartige Modelle im Rahmen eines kontinuierlichen Vorgehens u.a. als Wegbereiter (*engl. Enabler*) genutzt werden, indem sie bei der Identifikation neuer Dienst (typen) oder der Deprovisionierung nicht mehr benötigter Authentifizierungsdienste unterstützen.

Der Funktionsbereich umfasst dabei die CRUD-Funktionen zum Erstellen, Lesen, Aktualisieren und Entfernen eines Modells:

- **createModel()**: Das erstmalige Analysieren, Beschreiben und Modellieren eines Authentifizierungsszenarios bzw. einer Authentifizierungsumgebung.

Zur detaillierten Beschreibung eines beliebigen Services bzw. Service Providers kann das in Abschnitt 3.7.2 beschriebene, allgemeingültige MNM Service Model [GHH+01, GHK+01, GHH+02] herangezogen werden. Zur vollständigen und vergleichbaren Beschreibung von Diensten, die Authentifizierungsinformationen bereitstellen sowie deren Abhängigkeiten zu Diensten, die Authentifizierungsinformationen konsumieren, wird ein erweitertes Modell benötigt, welches in Abschnitt 5.1 spezifiziert wird.

Gemäß CRUD-Funktionalität kommen noch die folgenden Funktionen hinzu:

- **readModel()**: Das Auslesen von Informationen aus einem Modell.
- **updateModel()**: Das Aktualisieren eines Modells.
- **deleteModel()**: Das Auflösen bzw. Löschen eines Modells.

Die Funktionen werden in Abbildung 4.8 den entsprechenden Rollen der Architektur zugeordnet.

4.5.4 Erweiterung des Kommunikationsmodells

Auf eine Erweiterung des Kommunikationsmodells kann an dieser Stelle ebenfalls verzichtet werden, da die im vorherigen Abschnitt eingeführten Funktionen durch die jeweilige Rolle bzw. deren Sub-Rollen zu erbringen ist und daher keine Interaktion mit einer der anderen Rollen der Architektur erfordert.

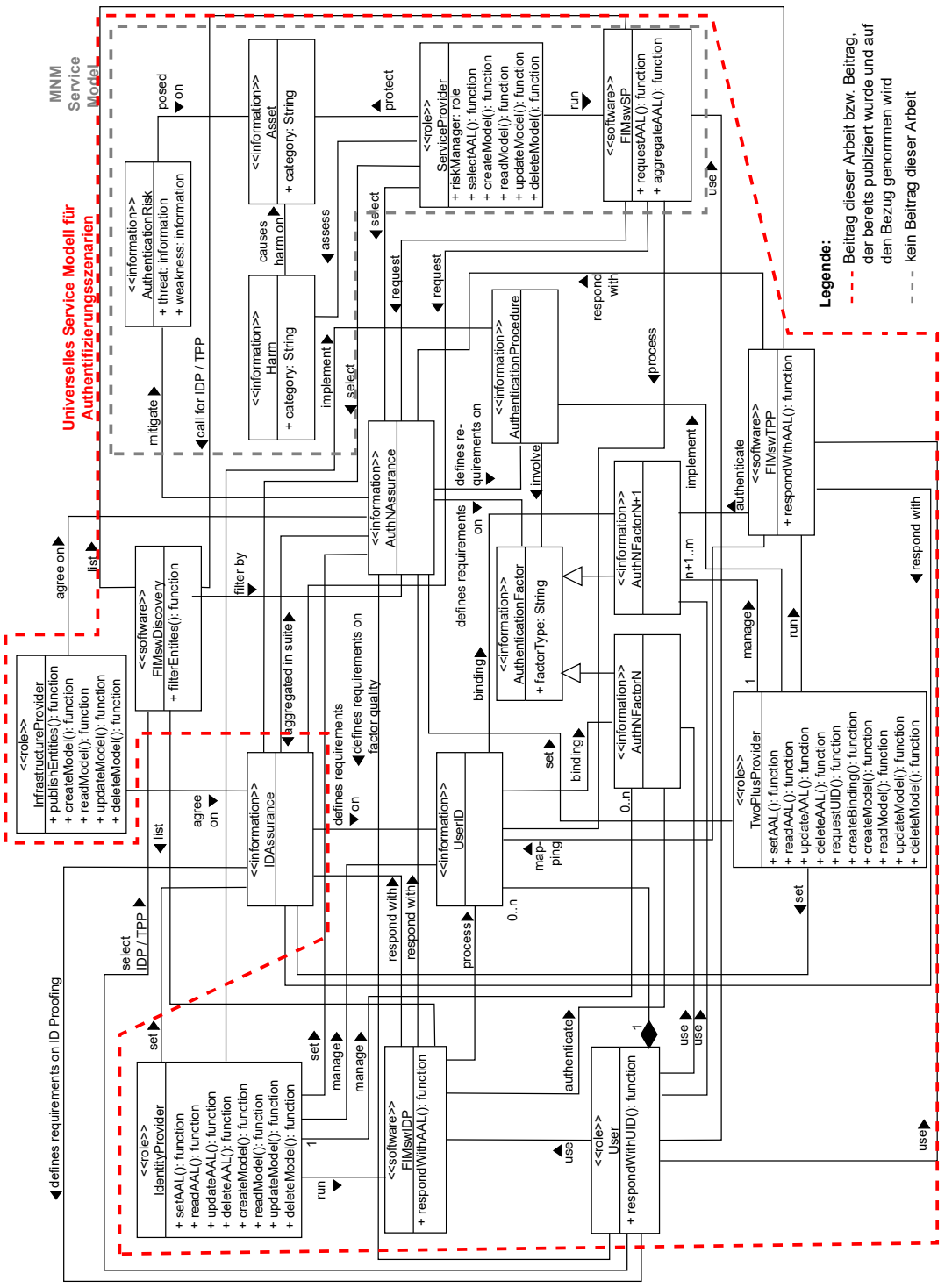


Abbildung 4.8: Resultierende Architekturteile AK, RM, WF und UM

4.6 Resultierende Gesamtarchitektur und Zusammenfassung

Ziel des Kapitels 4 war es, aufbauend auf den Szenarien nationales FIM, Inter-FIM und Forschungsinfrastrukturen sowie den Anforderungen des Kapitels 2 eine Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM zu erarbeiten. Ein Überblick über die resultierende Gesamtarchitektur ist dabei in Abbildung 4.9 gegeben.

Zur Konzeption einer Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM wurden dazu zunächst im Rahmen einer **strukturierten Ableitung des Idealzustandes** (vgl. Abschnitt 4.1), die **vier Teilmodelle für Managementarchitekturen** [HAN99] eingeführt, um die verschiedenen, in die Architektur involvierten Komponenten zu definieren und zu klassifizieren. Gemäß [HAN99] sind hierzu die folgenden vier Teilmodelle von Relevanz. Des Weiteren gibt die Tabelle 4.1 einen Überblick über die gemäß der Teilmodelle zu spezifizierenden Komponenten.

- Organisationsmodell
- Informationsmodell
- Funktionsmodell
- Kommunikationsmodell

Die Teilmodelle wurden dann jeweils auf die vier zentralen Hauptanforderungen aus Kapitel 2 angewendet. Somit ergaben sich vier zu erarbeitende Teile der Architektur, d.h. die Architekturteile AK, RM, WF und UM, die jeweils durch die Abschnitte 4.2 bis 4.5 widergespiegelt werden.

In Abschnitt 4.2 (Architekturteil AK) wurden somit die durch die Teilmodelle vorgegebenen Typen von Komponenten für ein Authentication-Assurance-Konzept erarbeitet. Da ein Großteil der dort skizzierten Komponenten auch für den Architekturteil RM relevant sind (Abschnitt 4.3), wurden die in Abschnitt 4.2 erarbeiteten Modelle, d.h. Organisations-, Informations-, Funktions- und Kommunikationsmodell, aufgegriffen und entsprechend erweitert. Selbiges Vorgehen findet auch bei den Architekturteilen WF und UM in den Abschnitten 4.4 und 4.5 Anwendung, sodass jeweils die Teilmodelle des vorherigen Abschnittes um die Komponenten des aktuellen Architekturteils erweitert werden.

Im folgenden Kapitel 5 werden auf Basis der Architektur die erforderlichen Konzepte systematisch erarbeitet und konkretisiert. Da die Entwicklung eines Konzepts zur Beschreibung und Modellierung von Authentifizierungsszenarien, welches in Abschnitt 4.5 als UASM bezeichnet wird, eine hervorragende Ausgangslage für ein tiefergehendes Verständnis der Zusammenhänge und Abhängigkeiten liefert, steht dieses in Kapitel 5 an erster Stelle.

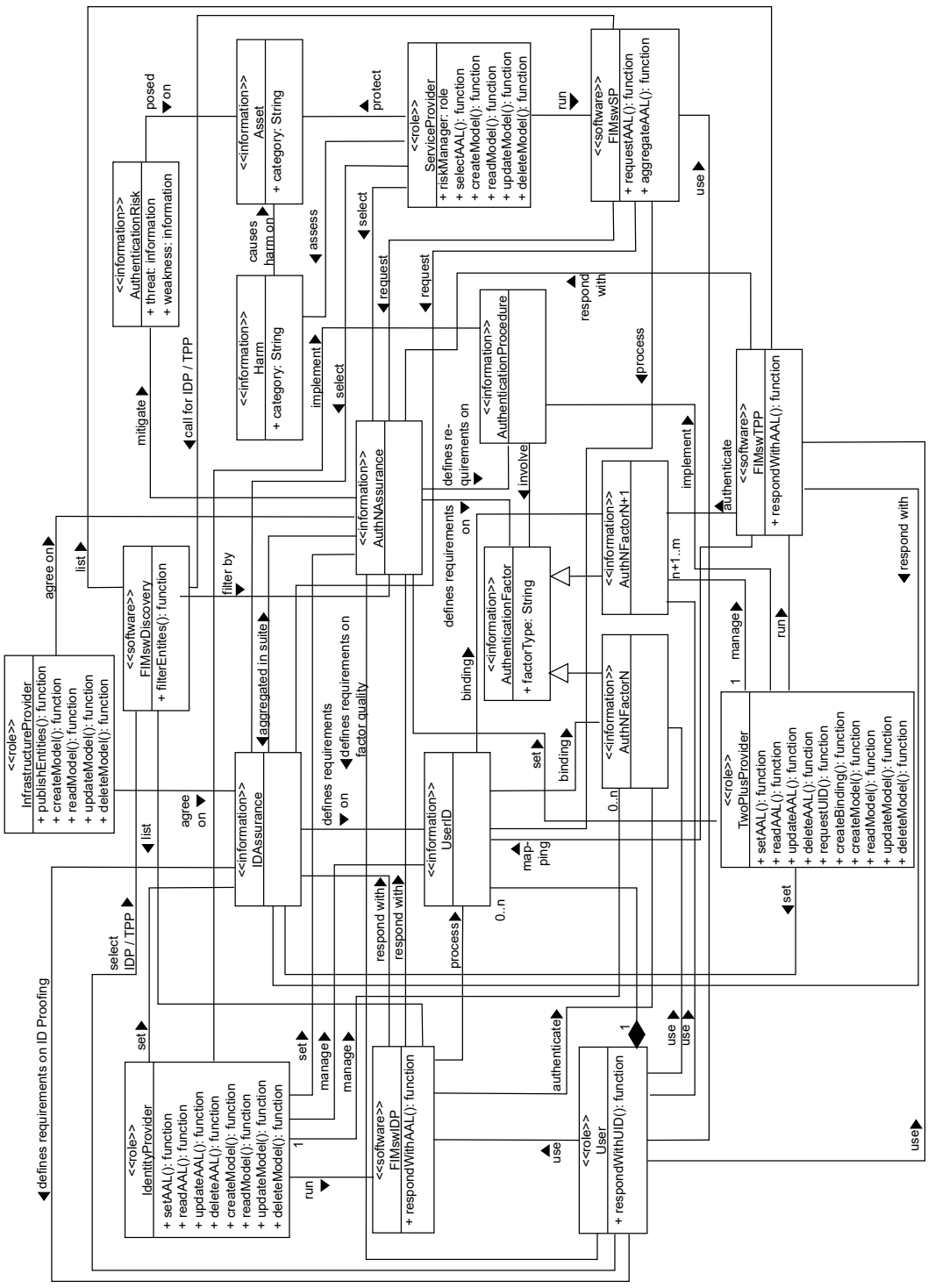


Abbildung 4.9: Überblick über die resultierende Gesamtarchitektur

Kapitel 5

Spezifikation erforderlicher Konzepte

Inhalt dieses Kapitels

In diesem Kapitel werden die aus der Architektur (vgl. Kapitel 4 sowie Abbildung 4.9) resultierenden, erforderlichen Konzepte detailliert erarbeitet.

Das Kapitel beginnt dazu in Abschnitt 5.1 mit der Spezifikation des **Universellen Modells für Authentifizierungsszenarien**. Hier werden Entitäten, Rollen und Services sowie deren Abhängigkeiten und Interaktionen auf generische Art und Weise, jedoch stets mit repräsentativen Authentifizierungsszenarien untermauert, eingeführt und verschiedene Sichten bereitgestellt.

Darauf aufbauend wird in Abschnitt 5.2 ein **leichtgewichtiges Authentication-Assurance-Konzept** eingeführt. Da die gesamtheitliche, in [ZSL19, Zie18, REF18c, Zie17, REF17, LAB+18, REF18a] publizierte Assurance Suite (inkl. Identity Assurance, die keinen Beitrag dieser Dissertation darstellt) neben dem SFA-Profil (vgl. Abschnitt 5.2.1) und dem

MFA-Profil (vgl. Abschnitt 5.2.2) auch Identity-Assurance-Komponenten umfasst, wird in Abschnitt 5.2.4 für ein gesamtheitliches Verständnis der Zusammenhang der Spezifikationen aufgezeigt.

In Abschnitt 5.3 wird das in Abschnitt 5.2 erarbeitete Authentication-Assurance-Konzept erneut aufgegriffen und beleuchtet dieses hinsichtlich des Risikomanagement-Prozesses. Diese Teillösung dient zur **Unterstützung der Service Provider hinsichtlich der Bewertung von Risiken und potentiellen Schäden**, um eine angemessene Entscheidung fällen zu können, ob eine Multi-Faktor-Authentifizierung erforderlich ist oder nicht.

Zuletzt wird in Abschnitt 5.4 der existierende 1FA-Workflow zum Zwecke der Multi-Faktor-Authentifizierung erweitert. Dazu werden die Komponenten aus dem vorherigen Kapitel referenziert und aufgezeigt, inwiefern das SFA-Profil zu erweitern ist, damit der **Fallback MFA-Workflow** unterstützt wird.

Das Kapitel endet mit einer abschließenden Bewertung.

5.1 Universelles Service Modell für Authentifizierungsszenarien

In Abschnitt 3.7 wurden bereits verschiedene Modelle zur Beschreibung und Abbildung von Informationen und Services unter Betrachtung des gesamten Lebenszyklus evaluiert. Dabei hat sich gezeigt, dass das MNM Service Model (MSM) [GHH+01, GHK+01, GHH+02] ein geeignetes Ausgangsmodell zur Erweiterung und Verfeinerung für authentifizierungsbezogene Szenarien ist. In diesem Abschnitt werden daher Rollen und Funktionalitäten (vgl. Abschnitt 5.1.1), Entitäten bzw. Akteure (vgl. Abschnitt 5.1.2), Services (Abschnitt 5.1.3) sowie verschiedene Sichten (Views) auf Basis von MSM eingeführt und erweitert, um ein universelles Modell für Authentifizierungsszenarien zu schaffen. Als Hilfestellung zur Anwendung in Multi-Faktor-Authentifizierungsszenarien werden verschiedene, gebräuchliche MFA-Templates erarbeitet.

„Universell“ bedeutet an dieser Stelle, dass das Modell Protokoll-, Standard-, Technologie- und Rahmenwerk-agnostisch ist und Authentifizierungsszenarien somit davon unabhängig modelliert und vor allem auch kombiniert oder verkettet werden können. Ferner wird aufgrund des zugrundeliegenden MNM Modells der gesamte Lebenszyklus eines Services berücksichtigt und kann daher in den verschiedenen Phasen des Lebenszyklus eines Services angewendet werden. Bspw. beim Design neuer, zukünftiger Architekturen, um zunächst vorhandene Abhängigkeiten zu identifizieren und darauf aufbauend, neue Technologien, z.B. MFA, leichter in eine bestehende Infrastruktur zu integrieren. Oder aber auch während der Nutzungsphase zur Durchführung spezieller Analysen, z.B. GAP-Analysen oder Security-Analysen (vgl. Abschnitt 2.9).

Um eine Verfeinerung von MSM zu erzielen, muss zunächst von konkreten Authentifizierungsprotokollen/-standards/-technologien/-rahmenwerken abstrahiert werden, sodass Authentifizierungsszenarien auf eine unabhängige Art und Weise beschrieben und modelliert werden können (vgl. [FA_Terminologie]). Darüber hinaus soll auch die Modellierung von

bspw. mehreren Protokollen innerhalb eines Szenarios möglich sein, was nur durch eine einheitliche Terminologie erreicht werden kann. Somit resultiert die Einführung verfeinerter Klassen auf Basis von MSM und darauf basierend verfeinerte Assoziationen/Beziehungen in den verschiedenen Sichten von MSM. [ZS18]

Die Erweiterung bzw. Verfeinerung von MSM wird als **Universal Authentication Service Model (UASM)** bezeichnet, dessen Grundlagen bereits in [ZS18] veröffentlicht wurden, wobei das generische Konzept der **Authentifizierungsinformation (AuthN Information, kurz: AuthNI)** verkörpert wird. Als Authentifizierungsinformation wird all jene Information bezeichnet, die sich auf die Authentifizierung eines Subjektes der realen Welt bezieht. Beispiele hierzu sind die Folgenden:

- AuthNI bereitgestellt durch den Benutzer, wie bspw. Anmeldeinformationen (*first factor credentials*)
- AuthNI, die innerhalb einer Entität auftreten und verarbeitet werden, z.B. der Vergleich von Benutzer bereitgestellter Information mit Werten eines LDAP Directories zur Verifikation.
- AuthNI, die zwischen zwei Entitäten auf vertrauenswürdige Art und Weise ausgetauscht werden, um eine vertrauenswürdige und vertrauensvolle Aussage über das digitale Gegenstück eines realen Subjekts zu erhalten.

Authentifizierungsinformationen treten somit an unterschiedlichen Stellen einer Interaktion auf und werden dort verarbeitet bzw. kommuniziert.

Da es sich bei dem Konzept der Authentifizierungsinformation um ein generisches Konzept handelt, wird nicht konkret eingegrenzt, welche Ausprägungen AuthNI annehmen darf bzw. muss. Es ist dabei unerheblich, ob AuthNI bspw. in Form eines Passworts oder eines Passworthashes auftritt oder ob, wie in föderierten Szenarien, nur eine Aussage über eine stattgefundene Authentifizierung kommuniziert wird. Darüber hinaus wird nicht konkret spezifiziert in welcher Form AuthNI (statisch versus dynamisch, als Attribut oder Teil der (Meta-) daten) vorliegt oder auftritt.

Exemplarische Authentifizierungsinformationen sind:

- Statische Attribute wie Benutzername oder E-Mail-Adresse
- Dynamische Attribute wie die Anzahl der Faktoren oder verwendete Faktoren
- Meta-Attribute wie Uhrzeit der Authentifizierung, maximale Gültigkeit oder Sessionlänge

Dabei ist zu berücksichtigen, dass Authentifizierungsinformationen nicht zwangsweise personenbezogene Daten darstellen, sondern wie aus obiger Auflistung hervorgehend auch Metadaten über z.B. verwendete Methoden (Assurance zur Stärke des Faktors) sein können.

AuthNI wird als **vertrauenswürdige Authentifizierungsinformation (Trustworthy AuthNI, kurz: TAuthNI)** bezeichnet, sobald Maßnahmen (meist kryptographisch, z.B. Verschlüsselung des Kommunikationskanals, Zertifikate) angewendet werden, um die Vertrauenswürdigkeit zwischen den involvierten Entitäten herzustellen und zu untermauern.

Dies setzt voraus, dass Vertrauen zwischen den Entitäten vorab etabliert und gemanagt wird.

In den folgenden Abschnitten werden Hauptkonzepte von UASM (Rollen, Funktionalitäten, Entitäten, Services) basierend auf MSM eingeführt, um die Interaktion und Kommunikation mit (vertrauenswürdigen) Authentifizierungsinformationen zu verdeutlichen.

5.1.1 UASM Rollen und Funktionalitäten

Die Rollen und Funktionalitäten von UASM basieren auf den von MSM beschriebenen Rollen und Interaktionsklassen (Funktionalitäten), weswegen diese zunächst kurz erläutert werden.

MSM unterscheidet hierbei zwischen drei zentralen Rollen, die nach Analyse der verschiedenen Lebenszyklus-Phasen und der Interaktionsklassen abgeleitet und abstrahiert wurden:

- Customer
- User
- Provider

Die Rollen Customer und User werden dabei der **Customer-Seite** zugeordnet, wohingegen die Rolle Provider der **Provider-Seite** zugeordnet ist.

Ferner unterscheidet MSM zwischen allgemeinen **Nutzungs- und Management-Interaktionsklassen bzw. -funktionalität**. Diese sind in MSM aus der Notwendigkeit heraus entstanden, Interaktionen zu abstrahieren, da es unmöglich wäre, alle auftretenden Interaktionen während eines Service-Lebenszyklus abzubilden.

Auf der Customer-Seite sind somit unter der Rolle User sämtliche Interaktionen zusammengefasst, um einen Service zu nutzen **(Nutzungsfunktionalität)**, wohingegen ein Customer für die Managementaktivitäten eines von ihm abonnierten Dienstes verantwortlich ist **(Managementfunktionalität)**.

Auf der Provider-Seite sind Aktivitäten zur Bereitstellung und Aufrechterhaltung der Nutzungs- und Managementfunktionalität notwendig. Aufgrund der Schwierigkeit, diese Funktionalitäten strikt zu trennen, subsumiert die Provider-Rolle sowohl Nutzungs- als auch Managementaspekte.

Somit leiten sich neben den Rollen und Interaktionen bzw. Funktionalitäten auch verschiedene **Seiten** für ein gemeinsames Verständnis über Aspekte eines Services ab. Pro Service-Interaktion kommt jede Rolle i.d.R. genau einmal vor, wobei eine Verkettung von Interaktionen (Subservice-Beziehungen) möglich bzw. vorgesehen ist (vgl. [FA_Rekursion]).

Zusammenfassend ergibt sich somit ein dreischichtiges Modell: Die **Customer-Seite** inkl. den Rollen Customer und User sowie eine **Provider-Seite** (mit Provider Rolle). Daneben

existieren gemäß MSM noch **seitenunabhängige Aspekte**, die den Service auf eine implementierungsunabhängige Art und Weise aus Sicht der Kunden beschreiben. Die Beschreibung der Services aus Blickwinkel der Kunden lässt sich darauf zurück schließen, dass wir inzwischen in einer kundenzentrierten Gesellschaft leben (i.S.v. *Customer Centricity*, *Customer Experience Programs*). Die seitenunabhängigen Aspekte eines Services sind dabei zwischen den beiden anderen Domänen angesiedelt.

5.1.2 Ableitung der UASM Entitäten

Um eine Verfeinerung von MSM zu erzielen (und da MSM keine generischen Entitäten definiert), werden nachfolgend generische Akteure bzw. Entitäten für UASM eingeführt. Diese dienen dazu, Authentifizierungsszenarien auf protokoll-/standard-/technologie-/rahmenwerk-agnostische Art und Weise zu beschreiben und abzubilden, weswegen UASM Entitäten *nicht* mit den bereits eingeführten Rollen gleichzusetzen sind.

Dazu wird zunächst zwischen zwei Typen von Subjekten unterschieden:

- **Real-World Authentication Subject (RAS)**: RAS stellt eine Identität bzw. ein Subjekt der realen Welt dar, das authentifiziert wird. Bei Betrachtung der klassischen Benutzerauthentifizierung handelt es sich hierbei typischerweise um Personen; potentiell denkbar sind aber auch gesamte Organisationen oder Untereinheiten, i.S.v. technischen Accounts. Reale „Things“ im Hinblick auf Internet of Things (IoT) sind ebenfalls denkbar.
- **Trustworthy Authentication Subject (TAS)**: Ist das digitale Pendant eines RAS, das bei einer Authentifizierung an einem Dienst bzw. System das reale Subjekt bei einer Authentifizierung widerspiegelt. Ein TAS ist vertrauenswürdig (trustworthy), wenn es durch einen entsprechenden Identitätsfeststellungs- und Bindungsprozess mit dem RAS verknüpft wurde. Kann ein ausreichend vertrauenswürdiges TAS nicht garantiert werden, kann das „trustworthy“ entfernt werden.

Rückblickend auf die Definition von Authentifizierungsinformation bezeichnet die Abkürzung AuthNI somit die *Information über die Authentifizierung eines digitalen Subjekts (TAS).*

Unter Berücksichtigung der MSM Customer- und Provider-Rollen sind für UASM die folgenden spezialisierten Entitäten abgeleitet. Anstatt der Analogie zur Rolle „Customer“ wird für Entitäten in Authentifizierungsszenarien der aussagekräftigere Begriff **Consumer** verwendet:

- **Trustworthy AuthNI Provider (TAP)**: Repräsentiert eine Entität, die einen Dienst betreibt, der Authentifizierungsinformationen über ein Subjekt zur Verfügung stellt bzw. kommuniziert.
- **Trusworthy AuthNI Consumer (TAC)**: Repräsentiert eine Entität, die Authentifizierungsinformationen, bspw. zum Zwecke der Zugriffskontrolle, konsumiert und verarbeitet.

Zusammenfassend sind somit in UASM alle Entitäten konsistent mit einer Abkürzung aus drei Buchstaben versehen (TAP, TAC sowie die Subjekte RAS und TAS), während Services einheitlich mit vier Buchstaben abgekürzt sind (s.u.).

5.1.3 Ableitung der UASM Services

Nach Einführung der zentralen Entitäten in Abschnitt 5.1.2 für UASM werden in diesem Abschnitt zwei Klassen generischer UASM Services spezifiziert. Nach Analyse zahlreicher Use Cases zur Authentifizierung wurden die folgenden zwei Serviceklassen für UASM [ZS18] abstrahiert:

Die generische Serviceklasse **TAAS**, **Trustworthy AuthNI Administration Service**, stellt den Ursprung bzw. (Haupt-) Quelle von Authentifizierungsinformationen dar, indem insbesondere reale Subjekte auf digitale Subjekte gemappt und registriert werden. Darüber hinaus dient TAAS zur Administration von Authentifizierungsinformationen (auch durch den Nutzer), wie bspw. das Ändern eines Passworts und die daraus resultierende Aktualisierung und Speicherung zugehöriger (dynamischer) (Meta-) daten.

Zusätzlich dazu beschreibt die generische Serviceklasse **Trustworthy AuthNI Provisioning Service (TAPS)** Services, die (vertrauenswürdige) Authentifizierungsinformationen bereitstellen bzw. kommunizieren. (T)AuthNI erhält diese Subklasse bspw. von einer (lokalen) Ressource, die Funktionalität zur Authentifizierung realisiert und dazu Informationen von einem TAAS erhält, welche dann wiederum von einem TAPS in ein entsprechendes Format/Protokoll zur Kommunikation transferiert wird (vgl. Beispiel 1, s.u.). Da das Konzept von Subservice-Beziehungen (Rekursion bzw. Verkettung) weiter oben bereits erwähnt wurde, kann (T)AuthNI auch rekursiv von einem low-level TAPS an einen high-level TAPS (oder umgekehrt) kommuniziert werden (vgl. Beispiel 2).

Hierzu dienen die folgenden zwei Beispiele aus FIM zur Verdeutlichung des Konzeptes:

1. Ein SAML IDP mit all seiner Nutzungs- und Managementfunktionalität repräsentiert eine Instanz der generischen Subklasse TAPS, während ein Identitätsmanagement-Portal bspw. eine TAAS-Instanz darstellt. Der TAPS erhält vertrauenswürdige Authentifizierungsinformationen von einem angeschlossenen LDAP oder Active Directory (Ressource), die er nach Transformation (in bspw. SAML-Attribute) in Form einer SAML-Antwortnachricht an einen TAC kommuniziert.

2. Ein SAML IDP-SP-Proxy inklusive seiner Nutzungs-/Managementfunktionalität agiert als (high-level) TAPS. Er führt selbst keine Authentifizierungen durch, sondern erhält TAuthNI von einem oder mehrerer low-level TAPS, aggregiert und/ oder mappt diese und leitet vertrauenswürdige Authentifizierungsinformationen an einen TAC weiter.

Wie in Abschnitt 5.1.1 eingeführt, wird bei den beiden konkretisierten Diensten (gemäß MSM) zwischen **Nutzungsfunktionalität** und **Managementfunktionalität** unterschieden. Die Nutzungsfunktionalität repräsentiert hier Interaktionen mit einem Dienst, die zur Erfüllung des Zweckes eines entsprechenden Dienstes erforderlich sind. Im Fall von TAPS,

sind das bspw. Authentifizierungen bzw. die Kommunikation der resultierenden Authentifizierungsinformationen. Interaktionen zum Managen eines Services, wie bspw. das Etablieren von Vertrauen oder Incident Mangement, werden an dieser Stelle als Managementfunktionalität bezeichnet (vgl. [FA_MANAGEMENTASPEKTE] und [FA_NUTZUNGSASPEKTE]).

Der Fokus von UASM liegt im Besonderen auf der Serviceklasse TAPS, wohingegen die Service-Subklasse TAAS eingeführt wurde, um eine gesamtheitliche Sicht auf Authentifizierungsinformationen bereitzustellen. Die Serviceklasse TAAS ist in den nachfolgenden Abbildungen stets enthalten, jedoch wird diese zunächst nicht weiter verfeinert, sondern der hier vorliegende Detaillierungsgrad beibehalten.

5.1.4 UASM Basic Views

Neben den wesentlichen, bereits eingeführten Aspekten stellen die verschiedenen Sichten (*engl. views*) ein weiteres zentrales Konzept in MSM dar. Diese spiegeln diverse seitenbezogene Aspekte wider, die in Abschnitt 5.1.1 gemäß MSM als *Customer-Seite*, *Provider-Seite* und *seitenunabhängige Aspekte* bezeichnet wurden.

MSM führt anhand einer systematischen Methodologie insgesamt drei verschiedene Arten von Sichten ein, um Akteure, Services und deren inter- und intraorganisatorische Beziehungen zu identifizieren und abzubilden. Die grundlegendste der drei Sichten ist das MSM Basic Service Model, die im Folgenden für eine konsistente Bezeichnung in UASM als **UASM Basic View** bezeichnet wird.

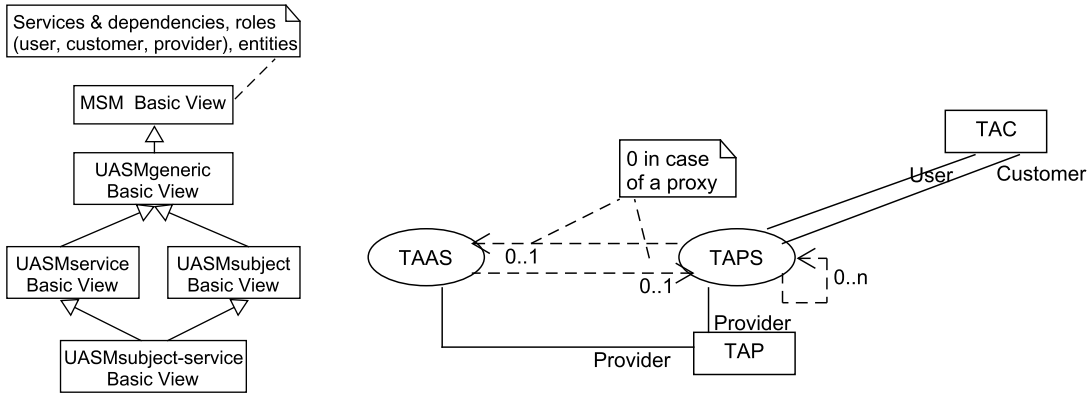
UASM Basic View, abgeleitet von den Konzepten des MSM Basic Service Model, dient zur grundlegenden Identifikation teilnehmender Rollen (Customer, User, Provider) und deren Beziehungen innerhalb eines Authentifizierungsszenarios. Während MSM an dieser Stelle lediglich Konzepte basierend auf UML-Diagrammen zur Erzeugung eines Basic Service Models bereitstellt, zeigte sich in UASM die Notwendigkeit zur schrittweisen Verfeinerung der UASM Basic View, um verschiedene Szenarien, auch außerhalb der IT, durch ein konsistentes Vorgehen abbilden zu können (vgl. Abbildung 5.1a).

Die Vorgehensweise ist in [ZS18] im Detail beschrieben, weswegen an dieser Stelle die verschiedenen Verfeinerungsschritte und die daraus resultierenden, verschiedenen UASM Basic Views nur grundlegend erläutert werden (vgl. Abbildungen 5.1, 5.2 und 5.3).

Abbildung 5.1a verdeutlicht, dass die $\text{UASM}_{\text{generic}}$ Basic View zunächst von der MSM Basic View bzw. Basic Model abgeleitet ist und darauf folgend zwei weitere Verfeinerungsschritte durchlaufen werden, wobei deren jeweilige Eigenschaften in der finalen $\text{UASM}_{\text{subject-service}}$ Basic View zusammengeführt werden. Die verschiedenen UASM Basic Views können somit als initiale Templates herangezogen werden.

Abbildung 5.1b zeigt die $\text{UASM}_{\text{generic}}$ Basic View im Detail, wobei (legale) Entitäten als Rechtecke, Services als Ellipsen, Rollen als UML-Assoziationen und Abhängigkeiten als gestrichelte Linien dargestellt sind. In der $\text{UASM}_{\text{generic}}$ Basic View werden Subjekte (i.S.v. RAS und TAS) zunächst nicht als aktiv agierende Entitäten betrachtet, weswegen sie hier noch nicht dargestellt sind. Es werden lediglich die Zusammenhänge zwischen den Entitäten

TAP und TAC sowie den Services (TAPS und TAAS) betrachtet, ohne auf potentielle, vom TAPS abhängige, Dienste einzugehen.

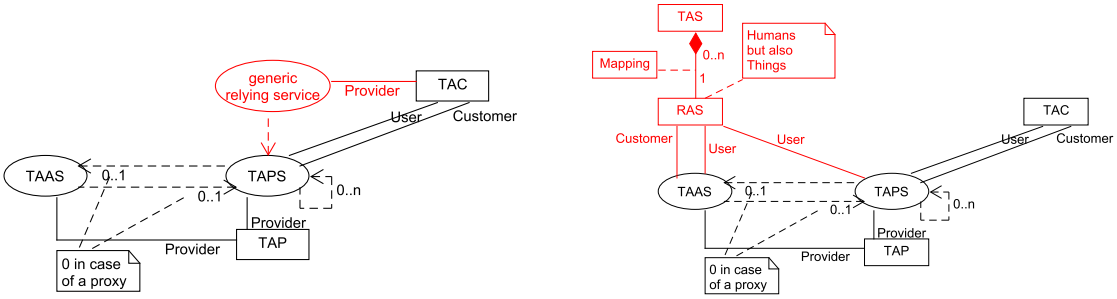


(a) Resultierende UASM Basic Views nach schrittweiser Verfeinerung

(b) $\text{UASM}_{\text{generic}}$ Basic View

Abbildung 5.1: UASM Basic Views. Abbildungen aus [ZS18]

Ein abhängiger Dienst, der von einem TAC bereitgestellt wird und folglich Authentifizierungsinformationen eines TAPS konsumiert, ist in der $\text{UASM}_{\text{service}}$ Basic View in Abbildung 5.2a in rot dargestellt. Aktiv agierende Subjekte werden mit der $\text{UASM}_{\text{subject}}$ Basic View in Abbildung 5.2b eingeführt (ebenfalls rot dargestellt).



(a) $\text{UASM}_{\text{service}}$ Basic View

(b) $\text{UASM}_{\text{subject}}$ Basic View

Abbildung 5.2: $\text{UASM}_{\text{service}}$ Basic View und $\text{UASM}_{\text{subject}}$ Basic View. Abbildungen aus [ZS18]

Somit ergeben sich aus den beiden verfeinerten Sichten (vgl. Abbildung 5.2) die in Abbildung 5.3 dargestellte, aggregierte $\text{UASM}_{\text{subject-service}}$ Basic View.

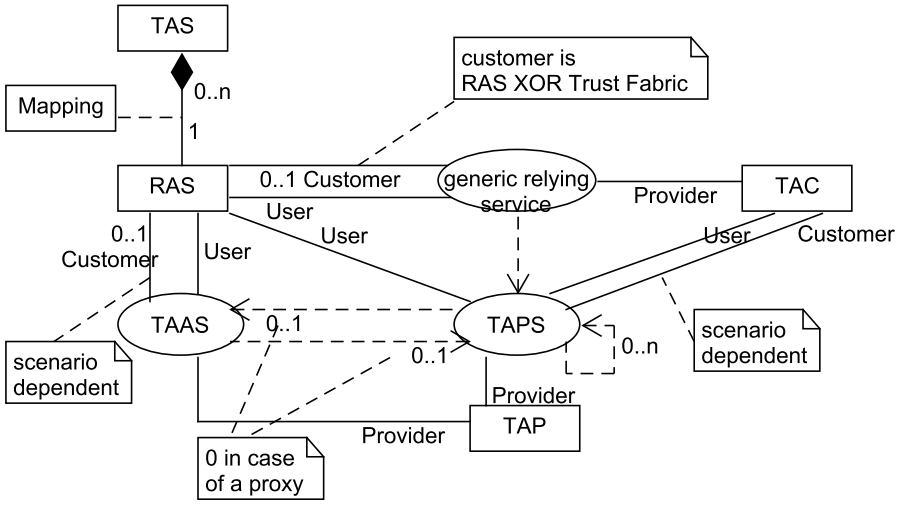


Abbildung 5.3: $\text{UASM}_{\text{subject-service}}$ Basic View. Abbildung aus [ZS18]

Anhand einer Assoziationsklasse werden zusätzliche Informationen zum Mapping zwischen realem Subjekt (RAS) und digitalem Subjekt (TAS) bereitgestellt. Jedes RAS kann prinzipiell auf beliebig viele TAS gemappt sein, im Fall von föderierten Szenarien wäre an dieser Stelle optimalerweise eine 1:1 Beziehung präsent (eine digitale Identität zum Zugriff auf mehrere Services).

Ein RAS nimmt, abhängig vom Szenario, die Rolle des User (und Customer) beim abhängigen Dienst (generic relying service) ein, der wiederum von einem TAPS abhängt. Somit ist ein RAS auch rekursiv User des davon abhängigen TAPS, da das RAS die Intention verfolgt, Authentifizierungsinformationen über sich bereitzustellen, um einen generischen Dienst nutzen zu können (d.h. RAS als Input-liefernde Entität). Ein TAC konsumiert die Authentifizierungsinformationen (bspw. zum Zwecke der Zugriffskontrolle)[1] und ist folglich (neben dem RAS) ebenfalls User des TAPS, da er Informationen nutzt, die durch ein Subjekt angestoßen und durch einen TAPS bereitgestellt werden (d.h. TAC als Output-nutzende Entität). Da MSM normalerweise nur eine (User-) Rolle pro Interaktion vorsieht, zeigt sich bei genauerer Betrachtung der User-Rolle des TAC, dass es sich hierbei nicht um einen User im klassischen Sinne (wie bspw. eine Person, die die eingehenden Authentifizierungsinformationen verarbeitet) handelt, sondern dass es sich aufgrund der technisch geprägten Natur eines Authentifizierungsszenarios auch um etwas technisches, das das Verhalten eines Nutzers nachbildet (wie z.B. einen Agenten), handeln kann. Eine weitere Konkretisierung der User-Rolle (d.h. „realer“ versus „technischer“ User) wäre hier für UASM anhand von Stereotypen denkbar (vgl. Abschnitt 5.1.4.1), jedoch wird an dieser Stelle zunächst darauf verzichtet.

Abb. 5.1, Abb. 5.2 und Abb. 5.3 von Ziegler/Schmitz, lizenziert unter CC BY-SA, Farbe und Beschriftung z.T. abgeändert.

[1] Er „spart“ sich somit die Implementierung einer eigenen Benutzerverwaltung.

Darüber hinaus wird, zur Vermeidung von Komplexität, davon ausgegangen, dass der TAP sowohl Provider des TAPS als auch des TAAS ist. In realen Szenarien ist das nicht zwangsweise der Fall, sodass auch hier die Einführung einer weiteren Provider-Entität denkbar wäre. Aufgrund der zugrundeliegenden, starken Methodologie von MSM, lassen sich Verfeinerungen unproblematisch ergänzen.

In Abbildung 5.4 ist die generische $\text{UASM}_{\text{subject-service}}$ getreu dem MSM Basic Model dargestellt. Hier wird explizit zwischen Customer- und Provider-Seite des TAPS unterschieden, auch sind die seitenunabhängigen Aspekte erstmals abgebildet. Eine ähnliche, jedoch verfeinerte Darstellungsweise, spiegelt sich auch später in der Service View wider.

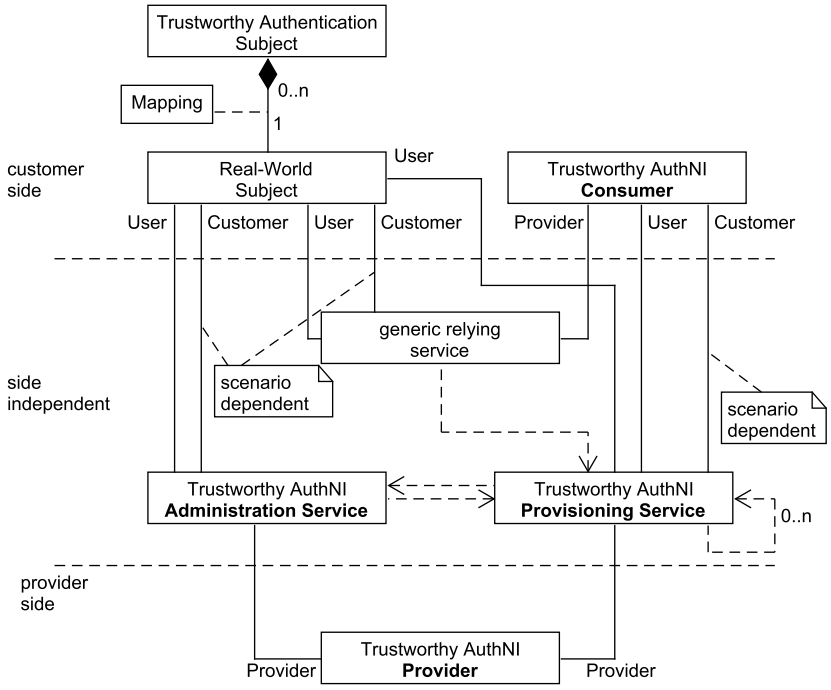


Abbildung 5.4: $\text{UASM}_{\text{subject-service}}$ Basic View auf Basis von MSM [GHH+01, GHK+01, GHH+02]

5.1.4.1 UASM Stereotypen

Während der Analyse verschiedener Authentifizierungsszenarien, insb. deren Beziehungen/-Abhängigkeiten, zeigte sich, dass Beziehungen (d.h. UML-Assoziationen) zwischen Entitäten und Services unterschiedliche Ausprägungen annehmen können. Daher werden als weitere Verfeinerung von MSM in **UASM Stereotypen** eingeführt.

Das Konzept eines Stereotyps leitet sich von UML-Stereotypen ab und dient zur Erweiterung existierender Modellelemente in UASM. Während in UML Stereotypen meist bei der

Verwendung von Klassen (-diagrammen) auftreten und mit «stereotype» markiert werden, lassen sich in UASM (UML) Assoziationen durch Anwendung eines Stereotyps weiter spezifizieren.

Die folgenden beiden Stereotypen werden dazu eingeführt:

«direct»: Wird verwendet, um Beziehungen/Abhängigkeiten zu markieren, die auf *direktem Wege* stattfinden. Dies kann bspw. ein Nutzer sein, der mit einem Interface eines Services agiert und Änderungen vornimmt.

«indirect»: Bezeichnet *indirekte* Beziehungen/Abhängigkeiten zwischen Entität und Service, wo entweder die Beziehung nicht direkt ersichtlich ist oder über Umwege stattfindet. Im Szenario eduGAIN kann ein Service Provider (UASM TAC) bspw. indirekter Customer eines TAPS sein, wenn kein bilateraler Vertrag ausgehandelt wurde, eine Interaktion jedoch anhand des (Inter-) Föderationskonstruktes möglich ist.

Assoziationen, die weder mit «direct» noch «indirect» markiert sind, sind implizit stets «direct», wohingegen «indirect» stets explizit mit angegeben werden muss.

5.1.4.2 Exemplarische Anwendung der UASM Basic View

Nach der Einführung der zentralen Konzepte von UASM [ZS18] basierend auf MSM, wird im Folgenden zur Verdeutlichung der Zweckmäßigkeit und Anwendbarkeit ein Beispiel unter Verwendung der zuvor eingeführten UASM Basic Views vorgestellt. Das Authentifizierungsbeispiel wird von dem Standpunkt der Lebenszyklus-Phase Betrieb erläutert, sodass die Etablierung des Services (insb. Design-, Verhandlungsphase) bereits stattgefunden hat.

In dem Authentifizierungsbeispiel geht es um einen Sales Service, der von beliebigen Nutzern über das Internet genutzt werden kann. Studenten, die über den Sales Service Produkte erwerben, können vorab ihren Studentenstatus validieren lassen, um einen Rabatt für ausgewählte Produkte zu erhalten. Ein reales Beispiel zur Validierung des Studentenstatus ist inAcademia [GÉ22b].

Die Abbildung 5.5 zeigt eine exemplarische Instanziierung der $\text{UASM}_{\text{subject-service}}$ Basic View, um Entitäten, Services und deren Beziehungen high-level abzubilden. Die zugrundeliegenden Authentifizierungskomponenten (d.h. die generischen Serviceklassen TAPS und TAAS) werden erst in den nächsten beiden Verfeinerungsschritten eingeführt.

Die Nutzer, darunter auch Studenten (in UASM als RAS bezeichnet), agieren somit als User und Customer des Sales Service, der von einem Verkäufer bzw. Dealer (UASM TAC) bereitgestellt wird. Die Rolle User (vgl. UML-Assoziation) subsumiert dabei jede Interaktion mit dem Service, um diesen zu nutzen (Nutzungsfunktionalität), wohingegen die Rolle Customer die Managementfunktionalitäten auf Kundenseite zusammenfasst. Zu den Managementfunktionalitäten zählen bspw. das Vertragsmanagement und auch das Melden von Anliegen (Service Requests) und Störungen in Form von Tickets (Incident Management).

Die Validierung des Studentenstatus wird dem Verkäufer (UASM TAC) als Subservice, betrieben durch den Validation Provider, zur Verfügung gestellt (d.h. Customer i.S.v. Ma-

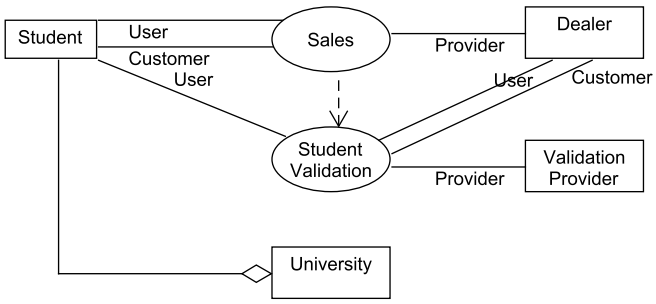


Abbildung 5.5: Exemplarischer Sales Service zur Verdeutlichung der UASM Konzepte

nagementfunktionalität, User i.S.v. Nutzer der durch Studenten angestoßenen Authentifizierungsinformationen zur Gewährung des Rabatts). Studenten (UASM RAS) agieren ebenfalls als User des Service Student Validation, da sie sich bei diesem authentifizieren, um ihren Studentenstatus validieren zu lassen.

Die Abbildung 5.6 zeigt die Einführung und Instanziierung der generischen Serviceklasse TAPS, die entsprechende Authentifizierungsinformationen an den Student Validation Service kommuniziert. Aufgrund der Abhängigkeitsbeziehung ist auch hier der Student (RAS) rekursiv User des Authentifizierungsdienstes (TAPS), betrieben durch seine Universität (in Abbildung 5.6 stellt der SAML IDP den TAPS dar). Bei genauerer Betrachtung des Student Validation Services wird deutlich, dass dieser selbst von der generischen Serviceklasse TAPS abstammt, da der Student Validation Service lediglich Authentifizierungsinformationen (hier: Zugehörigkeit zu Universität ja/nein) von einem SAML IDP weiterleitet.

Ferner verdeutlicht die Assoziation zwischen Validation Provider und SAML IDP die Verwendung der eingeführten UASM Stereotypen. Der Validation Provider ist in diesem Beispiel als Service Provider in einer (Inter-) Föderation registriert und hat keinen bilateralen Vertrag mit jedem Identity Provider unterzeichnet. Die Kundenbeziehung wäre somit indirekt.

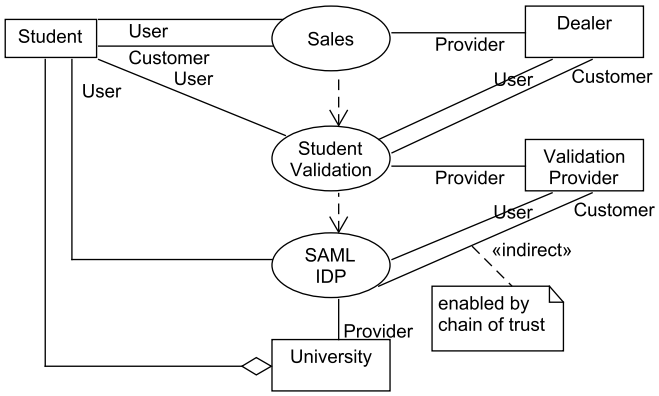


Abbildung 5.6: Einführung und Instanziierung der Serviceklasse TAPS

Zur Vervollständigung der eingeführten Konzepte zeigt Abbildung 5.7 die Einführung und Instanziierung der generischen Serviceklasse TAAS (siehe *IDM Portal* in Abbildung 5.7). Wie bereits erläutert, stellt diese den Ursprung der Authentifizierungsinformationen dar, da hier reale und digitale Subjekte initial registriert und gemappt werden.

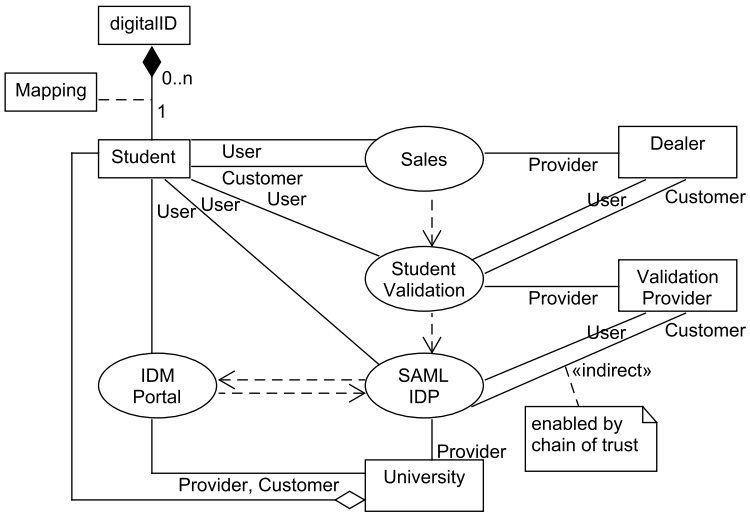


Abbildung 5.7: Einführung und Instanziierung der Serviceklasse TAAS

Wie in Abbildung 5.1b durch die $\text{UASM}_{\text{generic}}$ Basic View eingeführt, besteht eine gegenseitige Abhängigkeit zwischen den generischen Serviceklassen TAAS und TAPS, was auch in Abbildung 5.7 zwischen dem IDM Portal (TAAS) und dem SAML IDP (TAPS) ersichtlich ist. Eine solche Abhängigkeit ist bei dem als high-level agierenden Student Validation Service (TAPS) nicht vorzufinden, da sich dieser als eine Art Proxy verhält und somit üblicherweise nur Authentifizierungsinformationen aus verschiedenen Quellen aggregiert und weiterleitet.

In diesem Beispiel, jedoch stets abhängig vom konkreten Szenario, agieren unterschiedliche organisatorische Einheiten der Universität als Provider und Customer des IDM Portals. Der Student ist User des IDM Portals. Es zeigt sich somit, dass die in Abschnitt 5.1.4 eingeführten, generischen UASM Basic Views und deren Assoziationen eine erste Modellierungsgrundlage bilden, die für verschiedene Authentifizierungsszenarien flexibel adaptierbar und veränderbar ist.

5.1.4.3 UASM Basic View MFA Templates

Nachdem eine Vielzahl von Authentifizierungsszenarien mit MFA analysiert wurden und häufig auftretende, föderierte MFA-Ansätze in Abschnitt 3.5 diskutiert wurden, werden in diesem Abschnitt zwei UASM Templates zur Abbildung föderierter MFA-Szenarien erarbeitet. Zur Verdeutlichung der Anwendbarkeit in komplexen Szenarien wird die $\text{UASM}_{\text{subject-service}}$ Basic

View herangezogen. Das dritte Pattern bildet die in Abschnitt 4.4 spezifizierte Architektur bzw. den MFA-Workflow unter Verwendung eines TPPs ab.

Die UASM Basic View Templates dienen einerseits als Hilfestellung, um involvierte Entitäten, Rollen, Dienste und deren Abhängigkeiten in komplexen Authentifizierungsszenarien leichter zu identifizieren sowie abzubilden; andererseits wird durch eine einheitliche Terminologie und ein systematisches Vorgehen die Wiederverwendbarkeit der Templates für beliebige Authentifizierungsszenarien unterstützt.

Je nach Notwendigkeit, auch außerhalb von FIM, können noch weitere, generische Templates entwickelt werden. Zur Verdeutlichung des Konzepts und deren Anwendbarkeit sind jedoch zunächst die folgenden drei Templates ausreichend. Diese lassen sich auf die später erläuterte Service View und Realization View übertragen.

Ferner wurden bereits TAPS auf verschiedenen Ebenen (high-level bzw. low-level) eingeführt. Zur Unterscheidung werden diese im folgenden mit Zahlen versehen, deren Nummerierung *bottom up* erfolgt. Der Service T1APS beschreibt daher einen low-level TAPS auf unterer Ebene. Existieren mehrere T1APS auf unterer Ebene erhalten diese noch eine Zahl am Ende, z.B. T1APS 1, T1APS 2 usw. High-level TAPS (i.d.R. Proxies) auf oberer Ebene werden mit T2APS bezeichnet. Die Nummerierung erfolgt analog für die Provider-Entitäten des TAPS.

MFA Subservice Template:

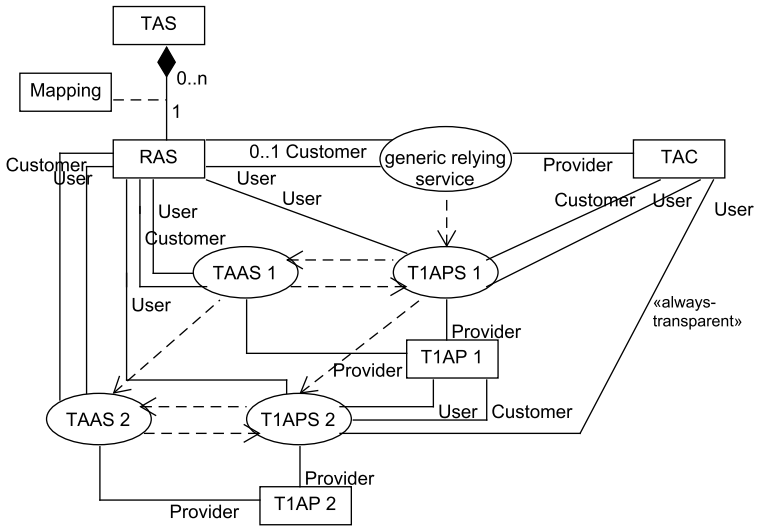


Abbildung 5.8: UASM Basic View MFA Subservice Template

Dieses Template (vgl. Abbildung 5.8) realisiert den in Abschnitt 3.5.1 beschriebenen MFA-Ansatz. Hier existiert ein beliebiger, (generischer) abhängiger Service, der Authentifizierungsinformationen von einem Subservice (T1APS 1) konsumiert. MFA wird hier in Form

eines weiteren Subservices (T1APS 2) realisiert (Prinzip der Verkettung/Rekursion). In diesem Fall stellt der T1APS 1 Authentifizierungsinformationen über den ersten Faktor eines Subjektes und der T1APS 2 AuthNI über den zweiten bzw. weitere Faktoren bereit. Sowohl T1APS 1 als auch T1APS 2 sind daher von einem TAAS 1 bzw. TAAS 2 abhängig, da jeweils Funktionalität notwendig ist, um Faktoren zu registrieren und diese mit realen Subjekten (RAS) zu mappen. Das RAS ist daher User (und ggf. Customer) von TAAS 1 und TAAS 2. Die Abhängigkeit zwischen TAAS 1 und TAAS 2 realisiert bspw. den Austausch einer UserID, sodass die Faktoren dem richtigen Subjekt zugeordnet werden können.

Wie bereits erläutert, ist der TAC, abhängig vom Szenario, entweder direkter oder indirekter Customer des T1APS 1. Aufgrund der Subservice-Beziehung (Verkettung) ist der Provider T1AP 1 nun sowohl User und Customer des T1APS 2. Da der TAC Authentifizierungsinformationen beider Services (T1APS 1 und T1APS 2) konsumiert, ihm dies aber i.d.R. aufgrund der internen Subservice-Realisierung nicht bekannt ist, ist die Assoziation zwischen TAC und T1APS 2 mit dem Stereotyp «always-transparent» markiert.

MFA Proxy Template:

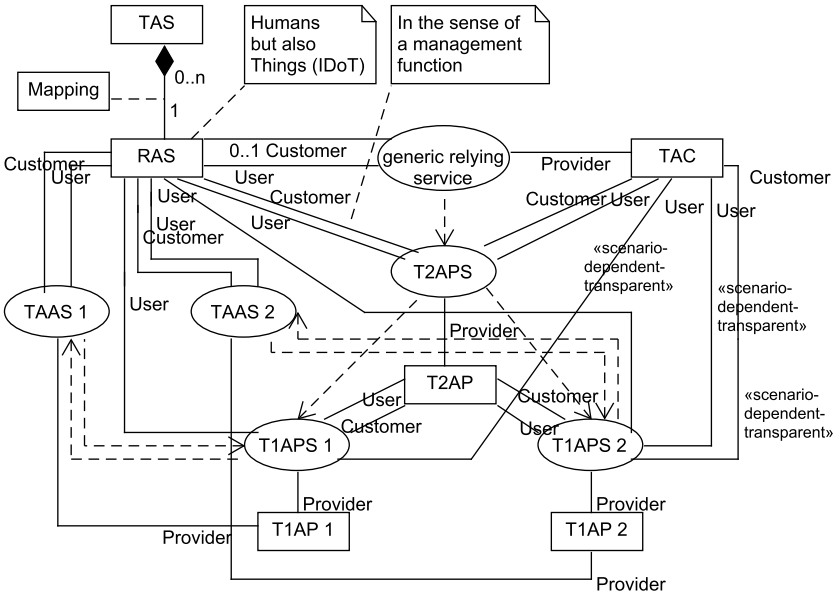


Abbildung 5.9: UASM Basic View MFA Proxy Template

Abbildung 5.9 zeigt das MFA Proxy Template. Hier existiert ein high-level TAPS (T2APS), der Proxy-Funktionalität implementiert, indem er Authentifizierungsinformationen von zwei low-level T1APS (T1APS 1 und T1APS 2) aggregiert und kommuniziert. Der T2APS ist daher selbst von keinem TAAS abhängig, greift jedoch auf zwei low-level T1APS zurück, die eine Abhängigkeitsbeziehung zu jeweils einem TAAS aufweisen. Das reale Subjekt (RAS) ist wieder User (und ggf. Customer) der beiden TAAS (TAAS 1 und TAAS 2).

Es besteht jeweils eine Subservice-Beziehung zwischen dem high-level T2APS und den zwei low-level T1APS, sodass der Provider T2AP (des high-level Services T2APS) wieder jeweils die Rolle des User und Customer (i.S.v. Managementfunktionalität) bei den beiden low-level T1APS einnimmt. Aus Darstellungsgründen werden in diesem Template nur Authentifizierungsinformationen von zwei T1APS zusammengeführt, prinzipiell sind aber 1..n viele Subservice-Beziehungen denkbar.

Abhängig vom Szenario ist die User Rolle des TAC beim T1APS 1 und T1APS 2 offensichtlich oder nicht, weswegen die Assoziationen im generischen Template mit dem Stereotyp «scenario-dependent-transparent» markiert sind. Der TAC ist ebenfalls ((in)direkter) Customer des high-level T2APS und eventuell sogar, abhängig vom Szenario, auch rekursiv Customer der low-level T1APS. Hier ist jedoch nochmals anzumerken, dass die Managementfunktionalität in FIM-Szenarien (v.a. in Forschung & Lehre) im Gegensatz zu MSM eher weniger formale, strikt definierte Prozesse umfasst und stattdessen auf lose gekoppelte Interaktionen (bspw. im Incident Management) basierend auf Vertrauen zurückgreift.

MFA Two-Plus Template:

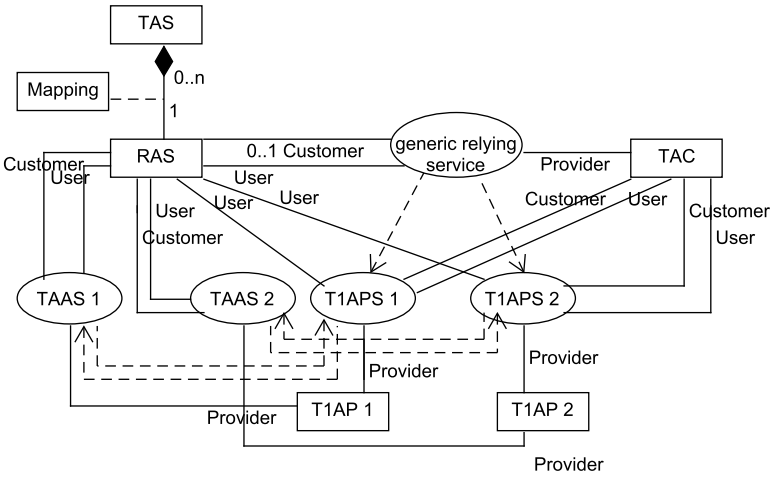


Abbildung 5.10: UASM Basic View MFA Two-Plus Template

Und letztlich zeigt die Abbildung 5.10 das MFA Template zweier unabhängiger Faktorprüfer gemäß der spezifizierten MFA-Architektur aus Abschnitt 4.4. Anstatt eines Proxies existieren hier zwei individuelle Subservice-Beziehungen zwischen dem (generischen) abhängigen Service sowie dem T1APS 1 und dem T1APS 2. Der TAC ist somit sowohl User und ((in)direkter) Customer des T1APS 1 als auch des T1APS 2. In dem konkreten Fall, dass eine Koordination zwischen TAAS 1 und TAAS 2 (bspw. zum Zwecke des Austausches einer gemeinsamen digitalen ID (TAS)) stattfindet, ist zwischen den beiden Services ebenfalls eine Abhängigkeitsbeziehung hinzuzufügen. Diese ist jedoch nicht notwendig, wenn der abhängige Dienst eigene Mechanismen implementiert, um bspw. verschiedene digitale Subjekte desselben realen Subjekts aufeinander zu mappen.

5.1.5 UASM Service View

Die UASM Basic View zeigt somit die in einem Authentifizierungsszenario involvierten Entitäten, Rollen, Services und deren inter- und intraorganisatorische Beziehungen. Mit Anwendung der UASM Service View, abgeleitet von der MSM Service View, werden im Folgenden die in Abschnitt 5.1.1 erläuterten seitenunabhängigen Aspekte weiter spezifiziert. Dazu wird hinsichtlich der Vollständigkeit die $\text{UASM}_{\text{subject-service}}$ Basic View, die maximale Ausprägung der verschiedenen, abgeleiteten Basic Views, herangezogen, wobei das Konzept der UASM Service View analog auch für die anderen Basic Views anwendbar ist.

In der UASM Service View werden alle notwendigen Details eines Services abgebildet, um ein gemeinsames, seitenunabhängiges Verständnis zwischen Customer-Seite und Provider-Seite herzustellen. Stets abhängig von der Lebenszyklus-Phase eines Services, in der man sich befindet, können die Details bei Anwendung der Service View eher grobkörnig (z.B. Service Design Phase) oder schon sehr feingranular (z.B. Nutzungsphase) ausgearbeitet sein. Da MSM und somit UASM das Prinzip der Service-Orientierung verfolgen, umfasst die Service View daher sämtliche Nutzungs- und Managementfunktionalitäten auf eine implementierungsunabhängige Art und Weise. Sie kann dabei für alle in UASM eingeführten Services angewendet werden, der Fokus liegt hier jedoch auf den (generischen) TAPS.

Zur Erläuterung der neu eingeführten Konzepte und Klassen zeigt die Abbildung 5.11 die $\text{UASM}_{\text{subject-service}}$ Service View im Detail.

Während in der generischen MSM Service View auf Customer- und Provider-Seite nur die Rollen anhand von Stereotypen abgebildet sind, sind in der UASM Service View, analog zur UASM Basic View, sowohl die Rollen als auch alle Akteure bzw. Entitäten abgebildet. Dies wurde zur einfacheren Zuordnung so gewählt, da Entitäten verschiedene Rollen bei verschiedenen Services einnehmen können. Ferner ist MSM derart konzipiert, dass pro Modell nur ein Service modelliert wird. In UASM wird analog nur ein konkreter Service modelliert (hier: TAPS); da das vollständige Bild jedoch erhalten bleiben soll, sind die Abhängigkeiten zu den anderen Services jedoch ebenfalls dargestellt. Darüber hinaus wäre in der UASM Service View bspw. das MSM Konzept der Verkettung (Rekursion) zwischen TAAS und TAPS nicht anwendbar, da dieser kein Subservice des TAPS ist.

Neben den bereits bekannten Entitäten und Rollen auf Customer-Seite werden, analog zu MSM, **zwei Clients** eingeführt, um auf die bereitgestellte Funktionalität eines Services zugreifen zu können. Es existiert daher jeweils eine Client-Klasse die den Zugriff auf verschiedene Nutzungsfunktionalitäten bzw. Managementfunktionalitäten eines Services aggregiert. In einer SAML-basierten Föderation ist dies bzgl. der Nutzungsfunktionalität bspw. der Webbrowser eines realen Subjekts (RAS).

Zur Nutzung bzw. zum Management des TAPS greift der entsprechende Client auf das jeweils entsprechende Interface des TAPS zu. Auch hier wird, gemäß MSM, zwischen Nutzungs- und Managementfunktionalität unterschieden, sodass sowohl ein **Interface zur Nutzung (Service Access Point, kurz: SAP)** als auch ein **Interface zum Management (Customer Service Management (CSM) Interface)** des Services existiert. In einer SAML-basierten Föderation kann der SAP bspw. die Shibboleth Login-Seite sein, die einem realen Subjekt

nach der Lokalisierung (Discovery) zur Verfügung gestellt wird. Die Lokalisierung kann dabei ebenfalls als Service modelliert werden.

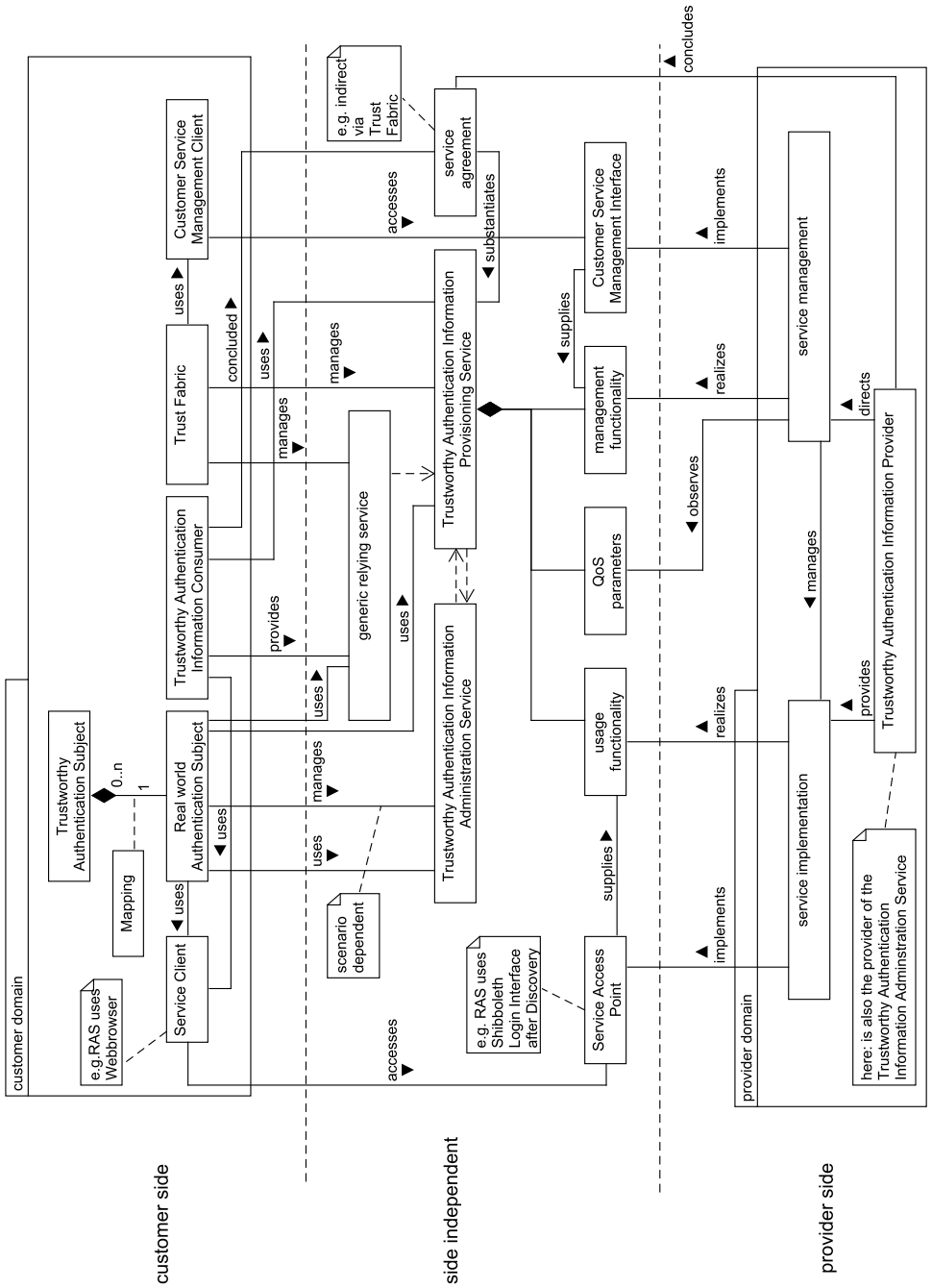


Abbildung 5.11: $\text{UASM}_{\text{subject-service}}$ Service View. Basierend auf MSM [GHH+01, GHK+01, GHH+02]

Die zwei Haupt-Interaktionsklassen (Nutzung/Management) des TAPS sind ebenfalls abgebildet und fassen sämtliche Service-Funktionalitäten zusammen. Dabei genügen die Funktionalitäten gewissen **Quality of Service (QoS) Parametern**, die in einer **Service-Vereinbarung** (Service Agreement) niedergeschrieben sind. QoS-Parameter können sowohl qualitative als auch quantitative Parameter sein, die dazu dienen, die minimale Service-Qualität der bereitgestellten Nutzungs- und Managementfunktionalität zu definieren. Dies kann bspw. die maximale Bereitstellungszahl von Authentifizierungsinformationen pro Zeitintervall (z.B. pro Monat) sein.

Normalerweise werden Service-Vereinbarungen (und somit QoS-Parameter) bilateral zwischen UASM TAC und TAP festgelegt. Im Fall von eduGAIN (vgl. Szenario Inter-FIM in Abschnitt 2.3) ist das nicht zwangsweise der Fall, da GÉANT im Namen der Teilnehmer Verträge mit neu hinzugekommenen Föderationen schließt, wobei eine Föderation wiederum selbst Verträge mit Identity Providern und Service Providern abgeschlossen hat. Sofern es dann nicht explizit eine Vereinbarung zwischen Identity Provider (TAP) und Service Provider (TAC) gibt, ist ein TAC indirekter Customer des TAPS. Somit ist auch der Föderationsbetreiber (Trust Fabric) primär Customer des TAPS (und verwendet damit den CSM Client), da dieser initial einen Vertrag mit einem Identity Provider zur Teilnahme an der Föderation geschlossen hat. Dieses komplexe Konstrukt ist in generischer Form in Abbildung 5.11 modelliert, wobei das Durchführen von Managementaktivitäten an dieser Stelle nicht unbedingt hundertprozentig trennscharf ist, da bspw. in der Praxis die Aushandlung erforderlicher Attribute zwischen TAP und TAC (auch ohne Föderation als Vermittler) unter Verwendung des Clients „Mail“ stattfinden kann. Im Beispiel hier zeigt sich auch, dass die Managementfunktionalität oft auf das Trust Management zurückgreift und weniger auf vollständig formal definierte, ausgereifte Prozesse. In einem derartigen komplexen Konstrukt ist dann analog nicht mehr das reale Subjekt Customer des abhängigen Services sondern die Trust Fabric, die den Vertrag mit einem abhängigen Service ausgehandelt hat (hier z.B. Föderationsbetreiber). Zur Managementfunktionalität zählen dann bspw. das Vertragsmanagement oder Änderungen an den Metadaten damit der Service für das reale Subjekt nutzbar bleibt.

Um den Service verfügbar zu machen, werden auf Provider-Seite, gemäß MSM, die **Service-Implementierung** und das **Service-Management** eingeführt. Die Service-Implementierung dient zur Realisierung der Nutzungsfunktionalität sowie zur Implementierung des Service Access Point und umfasst somit sämtliches Wissen, die dazu erforderlichen Mitarbeiter und die benötigte Soft-/Hardware. Das Service-Management hingegen dient zur Einhaltung der Service-Vereinbarung, der Service-Erfüllung gemäß den festgelegten QoS-Parametern sowie der Implementierung des CSM-Interfaces, um die Managementfunktionalität dem Customer zur Verfügung zu stellen. Zum Service-Management zählt bspw. das Incident Management (d.h. Bereitstellung eines Interfaces zum Melden von Störungen), um den Service nach einer Störung schnellstmöglich wiederherzustellen, sodass dieser innerhalb der definierten QoS-Grenzen bleibt; und das Change Management, um Änderungen, bspw. nach Eingang einer Störung, durchzuführen.

Die erweiterte UASM Service View inklusive exemplarischer Nutzungs-/ Managementfunktionalität und QoS-Parametern ist in Abbildung 5.12 dargestellt.

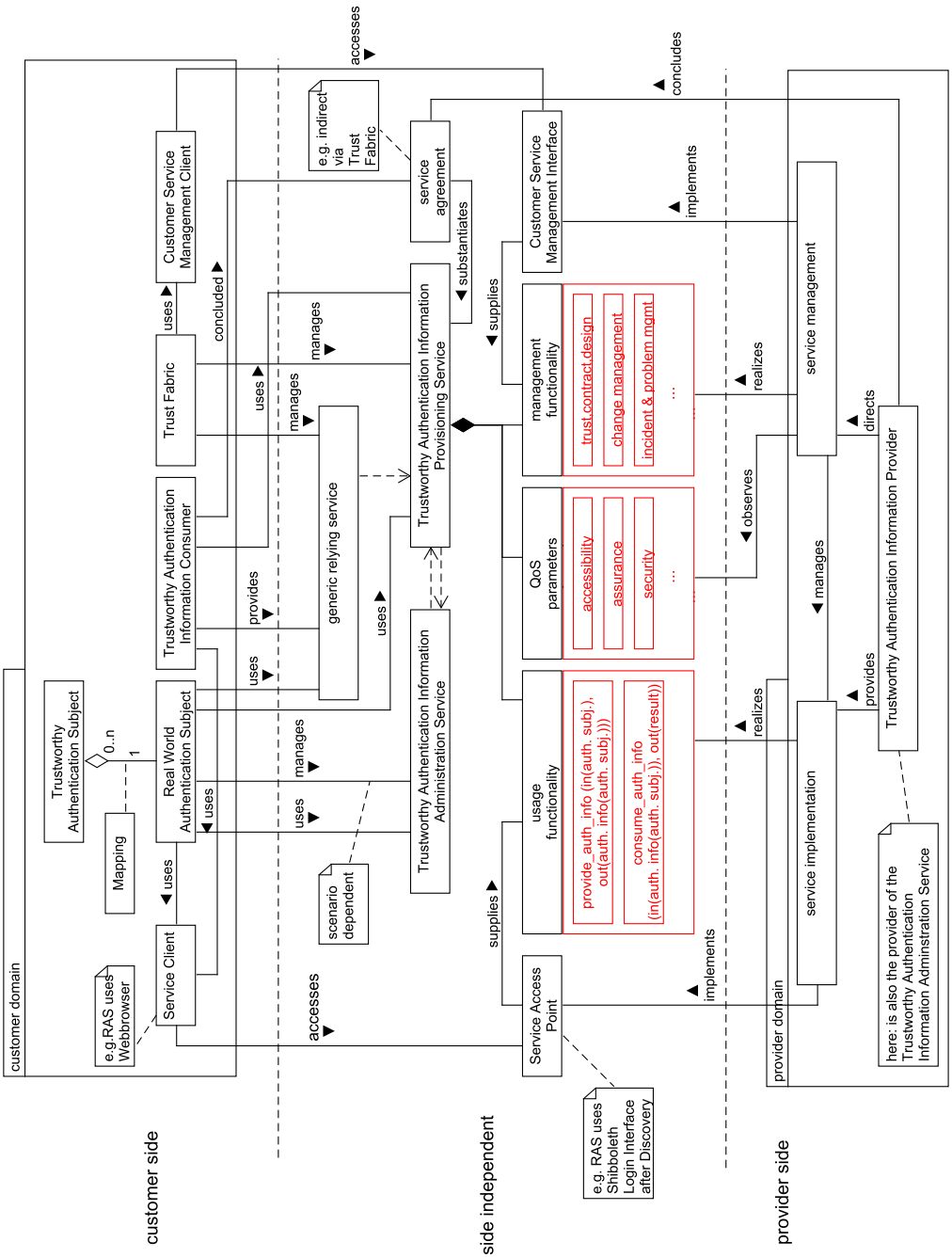


Abbildung 5.12: UASM$_{\text{subject-service}}$ Service View mit erweiterter Funktionalität. Basierend auf MSM [GHH$^+$01, GHK$^+$01, GHH$^+$02]

Zu den QoS-Parametern zählt bspw. die Authentication Assurance, die mittels Assurance-Konzept (vgl. Abschnitt 5.2) realisiert wird. Hier werden minimale Anforderungen an die Authentifizierungsqualität gestellt, sodass ein Service Provider Rückschlüsse über durchgeführte Authentifizierungen ziehen kann, um diese bei einer Zugriffsentscheidung zu berücksichtigen.

5.1.5.1 UASM Service View MFA Templates

Wie bereits erläutert, sind die in Abschnitt 5.1.4.3 erarbeiteten MFA Templates auch auf die UASM Service View bzw. UASM Realization View übertragbar. Aufgrund der wachsenden Größe der Modelle werden zum Zwecke der Veranschaulichung die drei MFA Templates nur stark vereinfacht dargestellt (vgl. Abbildungen 5.13, 5.14 und 5.15).

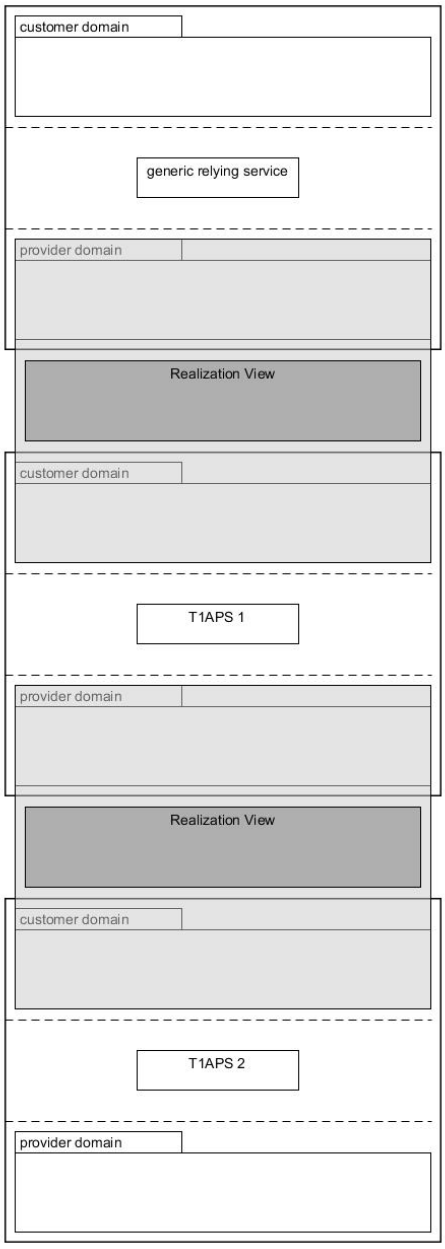


Abbildung 5.13: UASM Service View MFA Subservice Template

Da in den Abbildungen 5.13, 5.14 und 5.15 das Konzept der Verkettung (Rekursion) angewendet wird, um Subservice-Beziehungen zu modellieren, dient das Vorgehen gleichzeitig dazu, die fehlenden Komponenten zu identifizieren, die dann letztlich die UASM Realization View (abgeleitet von der MSM Realization View) formen. Die Abbildung 5.13 zeigt somit das resultierende UASM Service View MFA Subservice Template.

Hier werden anhand von drei rekursiv angewendeten UASM Service View Modellen (weiße, umrahmende Boxen), die jeweiligen Services (abhängiger Dienst, T1APS1, T1APS2) im Detail abgebildet. Der Provider des abhängigen Services agiert dabei als User/Customer des T1APS 1. Der Provider des T1APS 1 ist wiederum User/Customer des T1APS 2. Die Rolle eines Providers bettet somit auch die Rollen User/Customer des darunterliegenden Modells ein (durch hellgraue Box markiert). Die Lücke zwischen den beiden Seiten wird durch die Provider-interne Realization View geschlossen, welche im nachfolgenden Abschnitt erläutert wird.

Die beiden Grafiken in Abbildung 5.14 und 5.15 zeigen die resultierenden UASM Service View MFA Templates für Proxy-Szenarien und den Two-Plus-Ansatz.

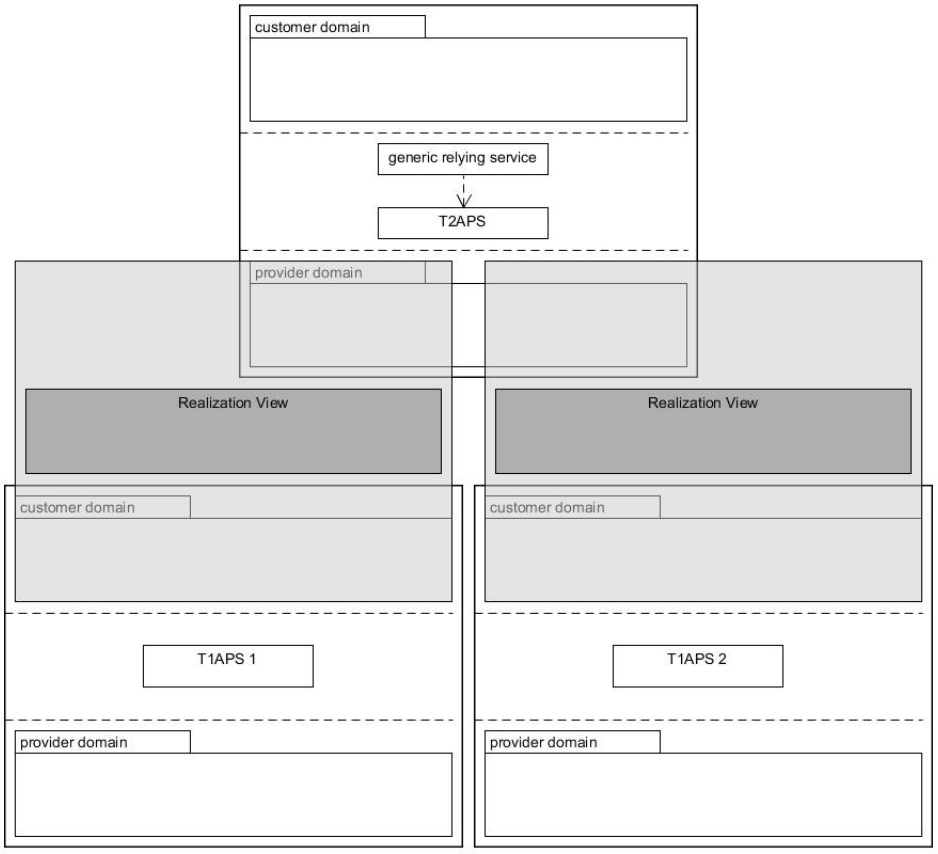


Abbildung 5.14: UASM Service View MFA Proxy Template

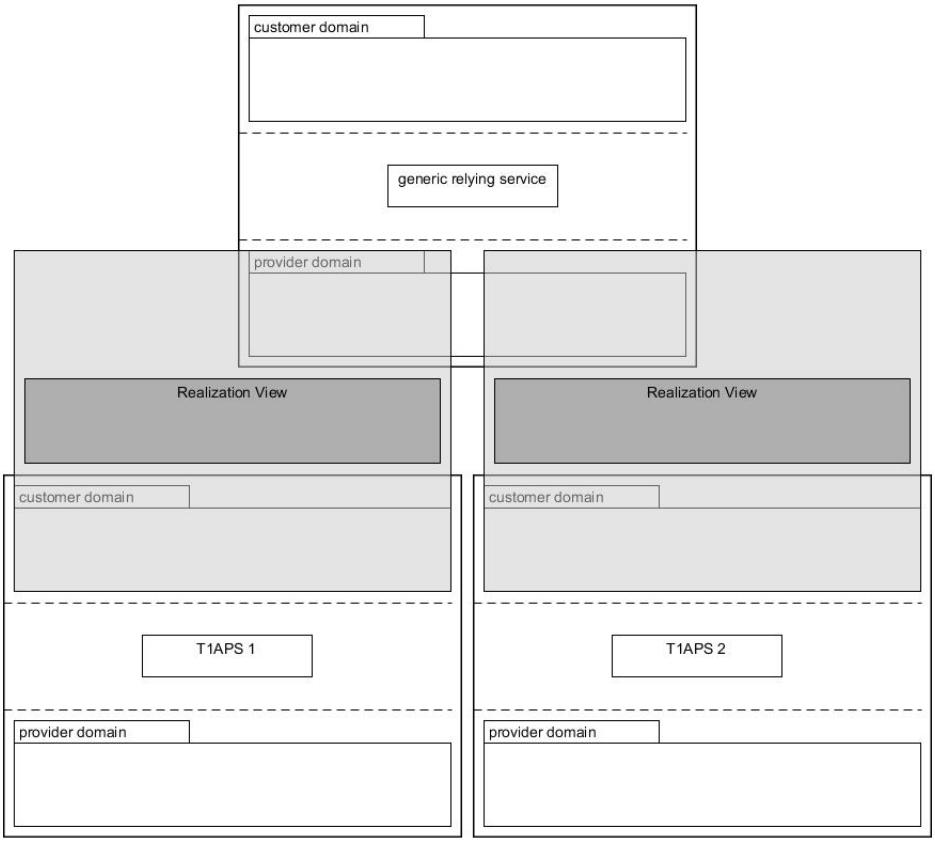


Abbildung 5.15: UASM Service View MFA Two-Plus Template

5.1.6 UASM Realization View

Der vorherige Abschnitt hat auf Basis der erarbeiteten UASM Service View MFA Templates gezeigt, dass die (MSM) Realization View neben der Provider-internen Realisierung dazu herangezogen wird, um bei Subservice-Beziehungen die Lücke zwischen Provider-Seite und Customer-Seite zu schließen (vgl. (hell)graue Boxen). Sie ermöglicht daher die Realisierung von Service-Hierarchien, sodass die Modelle verkettet angewendet werden können.

Die Abbildung 5.16 verdeutlicht anhand eines MFA Subservice Szenarios, welche zusätzlichen Elemente erforderlich sind und wie daraus die UASM Realization View abgeleitet wird.

Fokus ist hier wieder die Serviceklasse T1APS 1, die exemplarisch eine Ein-Faktor-Authentifizierung zur Verfügung stellt; sowie der Provider (des T1APS 1), der zur Realisierung eines zweiten Faktors auf einen Subservice (T1APS 2) zurückgreift. Der Provider agiert somit einerseits als Provider (des T1APS 1) aber auch rekursiv als User und Customer des T1APS 2. Nutzungsinteraktion mit dem T1APS 2 ist hier das Bereitstellen von 1FA-Informationen des weiter zu authentifizierenden Subjekts (z.B. UserID) sowie das Konsumieren von 2FA-Informationen zur Ableitung und Kommunikation einer (aggregierten) Response.

Diese Subservice-Beziehung ist in der Grafik 5.16 abgebildet, wobei auf die Modellierung der Assoziationen des realen Subjekts und des TAAS verzichtet wird, da der Fokus an dieser Stelle auf der provider-internen Realisierung des entsprechenden Services liegt.

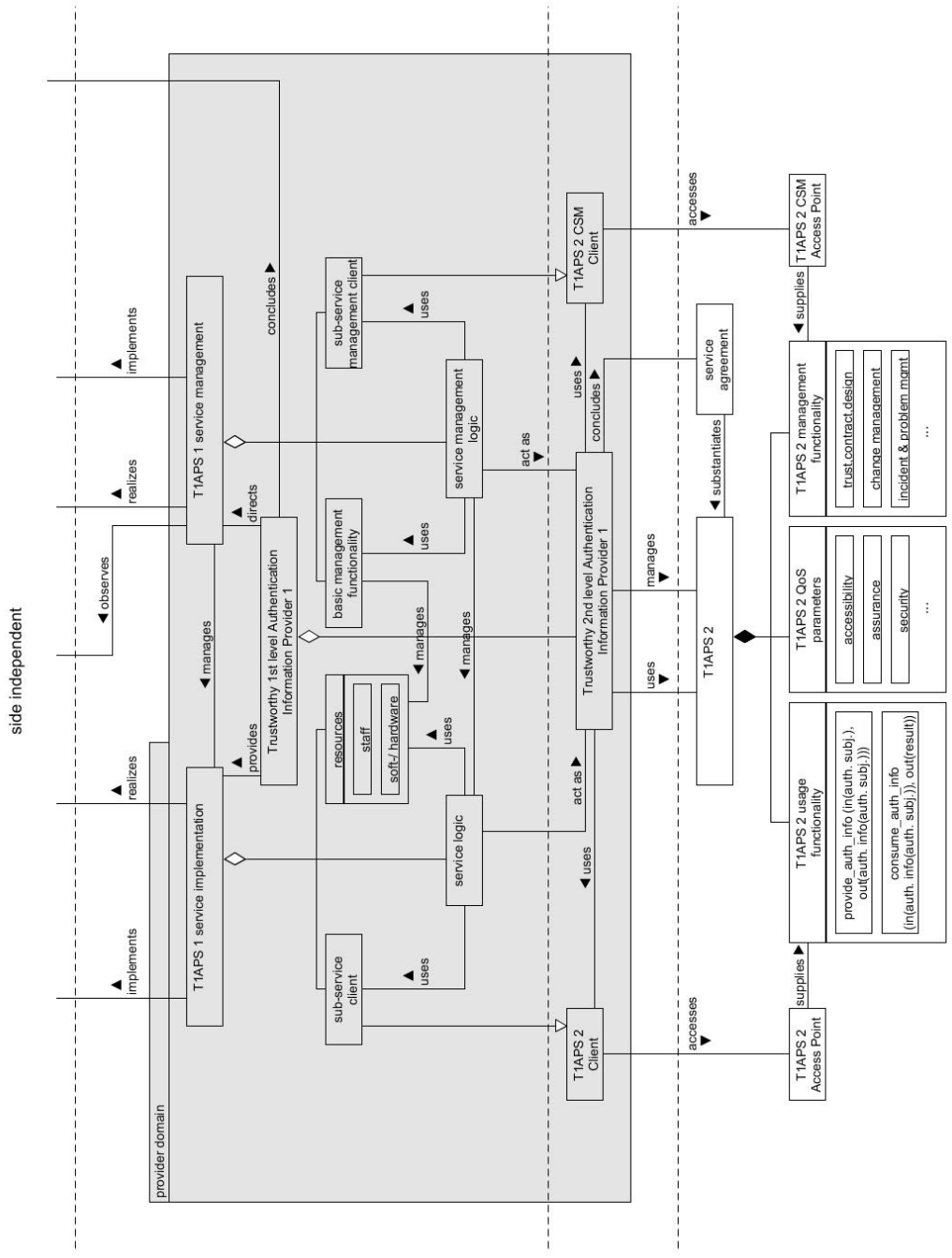


Abbildung 5.16: UASM Realization View am Beispiel eines MFA Subservices. Basierend auf MSM [GHH+01, GHK+01, GHH+02]

Die linke Seite der Grafik verdeutlicht, analog zu den vorherigen Modellen, die Service-Implementierung (Nutzungsaspekt) des T1APS 1. Als Verfeinerung der T1APS 1 Service-Implementierung (gemäß MSM) kommen diverse Ressourcen bereitgestellt durch den Provider des T1APS 1, wie bswp. virtuelle Maschinen auf denen entsprechende Software läuft oder personelle Ressourcen, hinzu. Der Subservice-Client, zum Zugriff auf den Subservice, ist ebenfalls Teil der Service-Implementierung. Zur Service-Logik zählt z.B. die Entscheidung, wann MFA (d.h. Kontaktieren des Subservices) notwendig ist und wann nicht. Dies kann bspw. auf Basis von Assurance-Anforderungen im einkommenden Request geschehen. Die Management-Seite ist analog aufgebaut.

5.2 Authentication-Assurance-Konzept

Im vorherigen Abschnitt wurde an der ein oder anderen Stelle Authentication-Assurance-Information bereits erwähnt oder referenziert. In diesem Abschnitt werden die Kriterien des Authentication-Assurance-Konzepts konkret erläutert. Dazu wird auf bereits veröffentlichte Konzepte zurückgegriffen [Zie18, REF18c, Zie17, REF17].

Die Kriterien orientieren sich dabei gemäß der Architektur aus Abschnitt 4.2 an der Anzahl verwendeter Authentifizierungsfaktoren, weswegen an dieser Stelle zwischen zwei Profilen unterschieden wird:

Das in Abschnitt 5.2.1 skizzierte **Ein-Faktor-Authentifizierungs-Profil** (kurz: SFA-Profil), welches das Hauptaugenmerk des hier präsentierten Authentication-Assurance-Konzepts darstellt, definiert Kriterien für Authentifizierungen mit einem Faktor (vgl. [FA_LoA_1FA]), während das in Abschnitt 5.2.2 erläuterte **Multi-Faktor-Authentifizierungs-Profil** (MFA-Profil) Kriterien für Authentifizierungen mit zwei oder mehr Faktoren spezifiziert (vgl. [FA_LoA_MFA]).

Das SFA-Profil wurde federführend von der Autorin dieser Arbeit zusammen mit Michael Schmidt anhand vielzähliger Feedback-Iterationen im Rahmen der REFEDS Assurance Working Group erarbeitet und wurde daher in Architekturteil AK der Architektur in Abbildung 4.1 als Teilleistung dieser Dissertation eingeordnet. Das MFA-Profil hingegen stammt ursprünglich aus der amerikanischen Föderation InCommon und wurde später von der REFEDS Assurance Working Group für die föderationsübergreifende Nutzung angepasst. Jedoch ist das MFA-Profil mit nur drei Kriterien zu high-level und trifft keine expliziten Aussagen über die Qualität der jeweiligen Faktoren. Daher wird im Rahmen dieser Arbeit das bereits existierende MFA-Profil aufgegriffen (vgl. Abschnitt 5.2.2 und in Abschnitt 5.2.3 ergänzende Kriterien eingeführt.

Da, wie bereits in Abschnitt 4.2.2 erläutert, die Authentication-Assurance-Profile und das Identity Assurance Framework [LAB+18, REF18a] teil einer gemeinsamen Assurance Suite sind, werden in Abschnitt 5.2.4 deren Zusammenhänge kurz aufgezeigt.

5.2.1 Kriterien des Ein-Faktor-Authentifizierungs-Profils

Das SFA-Profil [Zie18, REF18c, ZSL19] legt Minimalanforderungen zur Qualität einer durchgeführten Authentifizierung mit einem Faktor fest. *Minimal* bedeutet hier einerseits, i.S.v. Leichtgewichtigkeit (vgl. Anforderung [NFA_LoA_Minimalität]), dass Schlüsselkriterien aus existierenden LoA-Rahmenwerken wiederverwendet wurden und auf nicht-essentielle Anforderungen verzichtet wurde. Andererseits bezieht sich *minimal* auf die Tatsache, dass die im SFA-Profil definierten Anforderungen als Minimum zu erfüllen sind und, sofern anderweitige, striktere Anforderungen (z.B. organisationsspezifische Richtlinien) vorhanden sind, von diesen übertroffen werden können [ZSL19].

Das SFA-Profil unterscheidet zwischen zwei Hauptkriterien welche in den nachfolgenden beiden Abschnitten weiter konkretisiert werden.

1. Kriterien für Authentifizierungsfaktoren
2. Kriterien für Prozeduren zum Ersetzen eines Authentifizierungsfaktors

5.2.1.1 Kriterien für Authentifizierungsfaktoren

Dieses Hauptkriterium definiert wiederum vier Anforderungen für Authentifizierungsfaktoren, die für alle darin festgelegten Faktoren unabhängig ihres Typs gelten. Lediglich Authentifizierungsfaktoren, die die Biometrie betreffen sind hier ausgenommen, da diese gemäß NIST [GFN+17] aufgrund der probabilistischen Fehlerrate nicht zur Einfaktorauthentifizierung geeignet sind.

1. **Faktortypen, Geheimnisbasis und Minimale Länge:** Hier werden verschiedene Authentifizierungsarten, die aus dem NIST-Standard [GFN+17] abgeleitet sind, zu Klassen zusammengefasst. Diese sind:

   - Memorized Secret
   - Time-based OTP Device, Out-of-Band Device
   - Look-Up Secret, Sequence based OTP Device
   - Cryptographic Software/Device

   Pro Klasse wird die Geheimnisbasis angegeben. In der Regel handelt es sich dabei um eine Zeichenmenge. Für Zertifikate wird angegeben, ob diese auf RSA bzw. DSA oder ECDSA basieren. Ferner wird pro Klasse und Geheimnisbasis die minimale Länge des Geheimnisses angegeben (vgl. Tabelle 5.1). Diese entstanden unter Berücksichtigung des zu diesem Zeitpunkt aktuellen Standes der Technik und wurden nach Diskussion mit den Working Group Mitgliedern im Scope von R&E als angemessen festgelegt.

2. **Maximale Lebensdauer eines Geheimnisses**: Die maximale Lebensdauer eines Geheimnisses orientiert sich an der Art und Weise der Übermittlung. Es wird zwischen vier Varianten der Übermittlung für Einmalpasswörter unterschieden. Es ist dabei

Tabelle 5.1: Authentifikatoren, Geheimnisbasis und minimale Länge gemäß [Zie18, REF18c, ZSL19]

Authentifikator Typ	**Geheimnisbasis**	**minimale Länge**
Memorized Secret	$\geq$ 52 Zeichen (z.B. 52 Buchstaben)	12 Zeichen
	$\geq$ 72 Zeichen (z.B. 52 Buchstaben + 10 Zahlen + 10 Sonderzeichen)	8 Zeichen
Time based OTP-Device Out-of-band Device	10-51 Zeichen (z.B. 10 Ziffern)	6 Zeichen
	$\geq$ 52 Zeichen (z.B. 52 Buchstaben)	4 Zeichen
Look-up Secret Sequence based OTP-Device	10-51 Zeichen (z.B. 10 Ziffern)	10 Zeichen
	$\geq$ 52 Zeichen (z.B. 52 Buchstaben)	6 Zeichen
Cryptographic Software/Device	RSA/DSA	2048 bit
	ECDSA	356 bit

unerheblich, ob ein Einmalpasswort für Authentifizierungs-Transaktionen oder bspw. zum Zurücksetzen eines Faktors verwendet wird:

- via TOTP-basiertem Gerät
- via Telefon-/Mobilfunknetz, z.B. per SMS oder Anruf
- per Mail, z.B. Wiederherstellungslink
- per Post

Die maximale Gültigkeit ist jeweils in Tabelle 5.2 dargestellt.

Tabelle 5.2: Maximale Lebensdauer eines Geheimnisses gemäß [Zie18, REF18c]

Art und Weise der Übermittlung	**Maximale Lebensdauer**
Time based OTP Device	5 Minuten
Telefon-/Mobilfunknetz	10 Minuten
E-Mail	24 Stunden
Post	1 Monat

Für Nicht-Einmalpasswörter trifft die Anforderung keine explizite Aussage, ob Passwörter regelmäßig zu ändern sind oder nicht. Zwar besitzen einige LoA-Rahmenwerke noch diese Anforderung, jedoch haben Behörden wie die NIST regelmäßige Passwortwechsel inzwischen revidiert [GFN+17]. Dadurch wird ein Nutzer in regelmäßigen Abständen gezwungen, sein Passwort zu ändern, was dazu führen kann, dass der Nutzer ein eher schwaches, leicht zu merkendes Passwort wählt. Die Anforderung verlangt per se keine eingeschränkte Gültigkeit

von Passwörtern, ist dies jedoch in einer organisatorischen Richtlinie festgelegt, steht das nicht im Konflikt zum SFA-Profil.

Die nächsten beiden (high-level) Anforderungen dienen zum Schutz vor Bedrohungen. Besonders bei Passwort-basierten Authentifizierungssystemen wie es bei Webauthentifizierungen häufig der Fall ist, besteht die Gefahr des Online-Guessings. Hierbei rät ein Angreifer das Passwort des Benutzers, bspw. basierend auf Social Engineering oder aber auch automatisiert, anhand von veröffentlichten Passwortlisten oder Brute Force. Wird von einem Benutzer ein schlechtes Passwort gewählt, ist dies u. U. relativ einfach möglich. Neben der in Punkt 1 definierten minimalen Länge von Geheimnissen ist daher ein Schutz vor Online-Guessing Angriffen erforderlich. Darüber hinaus muss eine sichere Speicherung und Übermittlung von Geheimnissen sichergestellt werden.

3. **Schutz vor Online-Guessing Bedrohungen:** Diese Anforderung legt fest, dass Maßnahmen zum Schutz vor Online-Guessing zu implementieren sind. Wie das konkret zu realisieren ist, wird nicht spezifiziert. Dadurch erhalten Organisationen den notwendigen Freiraum und können selbst entscheiden, ob sie sich bspw. für ein Rate-Limiting oder andere Maßnahmen entscheidet.

4. **Kryptografischer Schutz (bei Speicherung/bei Übermittlung):** Analog zu Anforderung 3 wird hier lediglich spezifiziert, dass Maßnahmen zum Schutz von Authentifizierungsgeheimnissen bei Speicherung und Übermittlung getroffen werden müssen (z.B. mittels Hashing). Die Umsetzung der Maßnahme bleibt der jeweiligen Organisation selbst überlassen.

Neben den in Punkt 1 bis 4 definierten Kriterien für Authentifizierungsfaktoren bzw. Geheimnissen selbst sind zudem Kriterien für die damit verbundenen Prozeduren zum Ersetzen eines Authentifizierungsfaktors notwendig, die nachfolgend erläutert werden.

5.2.1.2 Kriterien für Prozeduren beim Ersetzen eines Authentifizierungsfaktors

1. **Gespeicherte Geheimnisse dürfen nicht an den Benutzer gesendet werden:** Hierdurch soll unterbunden werden, dass gespeicherte Geheimnisse, wie bspw. das von einem Benutzer festgelegte Passwort, im Klartext an den Benutzer übermittelt wird, da dies potentiell von Angreifer abgegriffen werden kann.

2. **Die Prozedur zum Ersetzen erfolgt nicht ausschließlich auf einer wissensbasierten Authentifizierung:** Dies unterbindet, dass das Ersetzen eines Geheimnisses oder Tokens ausschließlich durch die Beantwortung einer einfachen Frage möglich ist (z.B. Name Deines Haustiers). Kennt ein Angreifer den Benutzer bzw. dessen persönlichen Hintergrund und Umfeld (i.S.v. Social Engineering), kann diese Ersetzungsprozedur relativ einfach kompromittiert werden.

3. **Prozeduren, die menschliche Interaktion involvieren, stellen ein vergleichbares Assurance Level wie bei der initialen Identitätsfeststellung sicher:** Bezieht die Prozedur zum Ersetzen eines Authentifizierungsfaktors menschliche Interaktion mit ein, wie bspw. einen Service Desk, muss die Überprüfung der Identität bei

Vergessen/Ersetzen auf eine vergleichbare Art und Weise wie die initiale Überprüfung erfolgen. Wurde bspw. ein Authentifizierungsfaktor zu Beginn durch eine Überprüfung des Personalausweises an eine Person gebunden, darf die Prozedur zur Ersetzung nicht rein auf der Behauptung einer Identität stattfinden.

4. **Um einen Authentifizierungsfaktor wiederherzustellen, kann ein OTP an die registrierte Adresse eines Benutzers gesendet werden. Die Anforderungen an das OTP sind analog der Anforderungen an Look-Up Secrets, mit der Ausnahme das dieses ohne kryptographischen Schutz übermittelt werden kann:** Die maximale Lebensdauer des OTP richtet sich dabei ebenfalls nach Tabelle 5.2. Für einen Recovery-Link via E-Mail ist bspw. die maximale Gültigkeit von 24 Stunden angegeben.
5. **Für Backup-Authentifizierungsfaktoren gelten die Anforderungen gemäß des entsprechenden Faktortyps:** Wird bspw. eine TAN-Liste ausgegeben, richtet sich die Länge der dort niedergeschriebenen Geheimnisse nach den Anforderungen gemäß Look-Up Secret bzw. Sequence based OTP (-Device) in Tabelle 5.1.

5.2.2 Kriterien des Multi-Faktor-Authentifizierungs-Profils

Das MFA-Profil [REF17, Zie17] spezifiziert Anforderungen an Authentifizierungen mit mehr als einem Faktor und greift dazu auf drei high-level Anforderungen zurück:

1. **Die Authentifizierung eines Benutzers setzt sich aus mindestens zwei (von vier) unterschiedlichen Authentifizierungsfaktoren zusammen:** Als Referenzrahmenwerk wird hier ITU-T X.1254 [Int12] angegeben, das zwischen *something you know*, *something you have*, *something you are* und *something you do* unterscheidet. Andere Definitionen (vgl. Kapitel 3) hingegen unterscheiden lediglich zwischen drei verschiedenen Typen von Authentifizierungsfaktoren. Kapitel 3 verdeutlicht ebenfalls, dass eine Authentifizierung mit zwei unterschiedlichen Passwörtern keine gültige Multi-Faktor-Authentifizierung ist.
2. **Die verwendeten Authentifizierungsfaktoren sind voneinander unabhängig, sodass der Zugriff auf einen Faktor keinen Zugriff auf einen anderen Faktor ermöglicht:** Diese Anforderung stellt sicher, dass auf die Faktoren nicht gegenseitig zugegriffen werden kann, da ansonsten eine Multi-Faktor-Authentifizierung nicht stärker als eine Authentifizierung mit einem Faktor ist.
3. **Die Kombination von Faktoren mindert die Risiken einer Ein-Faktor-Authentifizierung:** Dazu zählen bspw. Nicht-Echtzeitangriffe wie Phishing, Offline Cracking, Online Guessing oder Diebstahl.

5.2.3 Erweiterung des Multi-Faktor-Authentifizierungs-Profils

Im vorherigen Abschnitt wurden die drei Hauptkriterien des MFA-Profils vorgestellt. Daraus wird ersichtlich, dass im Gegensatz zum SFA-Profil diese Spezifikation viel grobgranularer

gehalten ist und keine konkreten Qualitätsanforderungen an bspw. die verwendeten Faktoren einer Multi-Faktor-Authentifizierung stellt. Gemäß Konformität mit dem MFA-Profil ließe sich also ein Passwort von schlechter Qualität mit einem als bereits unsicher eingestuften zweiten Authentifizierungsfaktor (z.B. SMS) kombinieren. Es ist an dieser Stelle also fraglich, inwiefern Service Provider tatsächlich von dem Signalisieren der URI *https://refeds.org/profile/mfa* profitieren, wenn ihnen nur mitgeteilt wird, dass zwei unterschiedliche Faktoren verwendet wurden, diese jedoch mit keinen Qualitätsanforderungen assoziiert sind. Da MFA jedoch stets mit einer höheren Sicherheit assoziiert wird, wird hier eine sinnvolle Erweiterung des MFA-Profils vorgestellt.

Um diesem entgegenzuwirken, wird daher als Erweiterung vorgeschlagen, die beiden Spezifikationen SFA und MFA nicht mehr voneinander getrennt zu betrachten, sondern eine hierarchische Kopplung vorzunehmen, sodass jeder verwendete Faktor des MFA-Profils die dem Faktortyp entsprechenden Anforderungen des SFA-Profils zu erfüllen hat. Indem die Erweiterung in die MFA-Spezifikation aufgenommen wird, wird in diesem Zuge gleichzeitig sichergestellt, dass potentielle Versionsupdates an dem SFA-Profil automatisch in das MFA-Profil einfließen, ohne dass zusätzliche Änderungen an dem MFA-Profil erforderlich sind. Da IDPs ohnehin ermutigt werden, zunächst die Anforderungen des SFA-Profils umzusetzen, können die Anforderungen Schritt für Schritt für die eingesetzten Authentifizierungsfaktoren vorgenommen werden.

5.2.4 Zusammenhang der Authentication- und Identity-Assurance-Profile

Da wie bereits in Abschnitt 4.2.2 erläutert, die publizierten Versionen in einer gemeinsamen Assurance Suite zusammengefasst sind, verdeutlicht die Abbildung 5.17 kurz den Zusammenhang des SFA-Profils und des MFA-Profils mit den Komponenten des Identity Assurance Frameworks [LAB+18, REF18a].

Die Authentication Assurance wird dazu in Abbildung 5.17 anhand einer Dimension (d.h. nach außen zeigender Pfeil) mit den zwei Werten SFA und MFA repräsentiert, während die Komponenten des Identity Assurance Frameworks anhand drei, individuell behauptbarer Dimensionen, vgl. *Identifier Uniqueness*, *ID Proofing* und *Attribute Freshness*, abgebildet sind. Das Identity Assurance Framework definiert dabei analog zu den SFA- und MFA-Profilen zwei unterschiedlich starke Profile, die in Abbildung 5.17 durch blau bzw. grün durchgezogene Linien repräsentiert sind.

Das low-risk Profil (vgl. *REFEDS Cappuccino profile*) legt dabei die Verwendung eines eindeutigen, persönlichen und rückverfolgbaren Identifiers mit einer *Attribute Freshness* der Zugehörigkeit (*engl. Affiliation*) eines Nutzers von einem Monat und einem mittleren Identitätsfeststellungsverfahren (vgl. z.B. remote Identitätsfeststellung) fest.

Das high-risk Profil (vgl. *REFEDS Espresso profile*) greift auf einen eindeutigen, persönlichen und rückverfolgbaren Identifier mit einer *Attribute Freshness* von einem Monat und einem hohen Identitätsfeststellungsverfahren (vgl. z.B. persönliche Identitätsfeststellung) zurück.

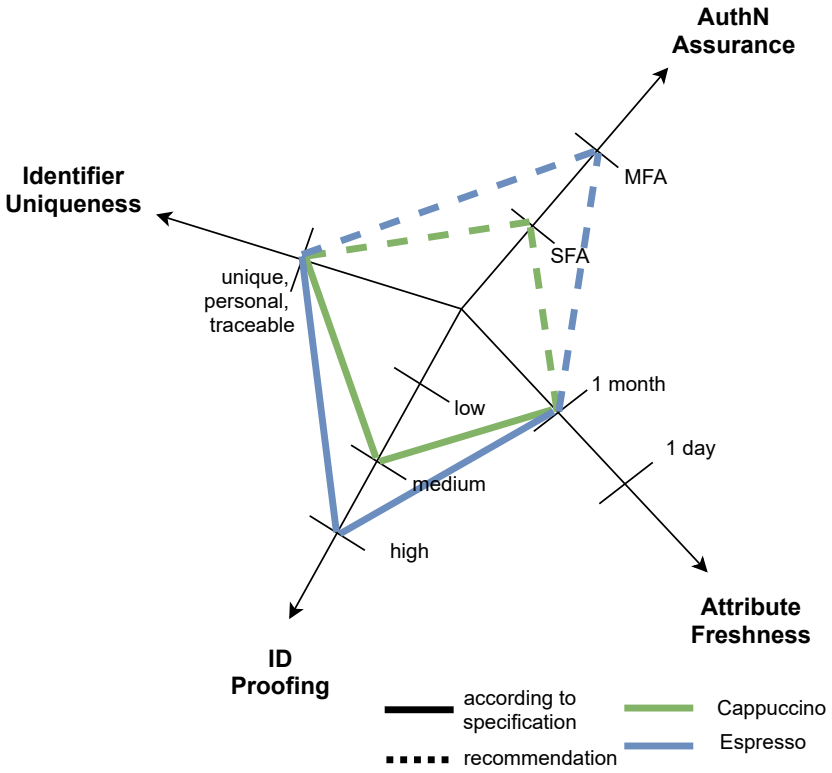


Abbildung 5.17: Assurance-Komponenten. Grafik aus [ZSG+21a]

Aufgrund der Modularität der Authentication Assurance und der Identity Assurance wird keine strikte Kombination der Profile vorgegeben, stattdessen wird lediglich eine *Empfehlung* (siehe gestrichelte Linien) abgegeben, wie die Identity Assurance mit der Authentication Assurance kombiniert werden kann; bspw. indem eine ähnliche Stärke der Identität und Authentifizierung miteinander kombiniert werden [ZSL19].

5.3 Empfehlungen und Maßnahmen für Service Provider unter Verwendung eines risikobasierten Ansatzes

In diesem Abschnitt werden Empfehlungen zur praktischen Umsetzung der Authentication Assurance für Service Provider skizziert. Ein Großteil dieser Empfehlungen bzw. Hilfestellungen und Anleitungen wurde bereits vorab, anhand repräsentativer Beispiele aus dem R&E Umfeld, in [ZSG+21a] veröffentlicht und umfasst neben den Empfehlungen zur Authentication Assurance auch diejenigen zur Identity Assurance. Der Fokus dieses Kapitels liegt, analog zu den bisherigen Kapiteln dieser Arbeit, auf der Authentication Assurance, wobei

aber nicht alle Maßnahmen stets trennscharf sind. Somit sind Teile der hier präsentierten Empfehlungen ebenfalls auf die Identity Assurance (vgl. Abschnitt 5.2.4) anwendbar.

Neben der Service Provider Perspektive wurden in [ZSG+21a] auch Empfehlungen und Hilfestellungen für Identity Provider erarbeitet. Diese unterstützen Identity Provider dabei, wie sie die Konformität zu den Anforderungen der Identity und Authentication Assurance überprüfen können. Dazu wird auf ein repräsentatives R&E Szenario zurückgegriffen, der „Campus Use Case“, wobei zusätzlich Implementierungsbeispiele referenziert werden. Der *Campus Use Case* stellt an dieser Stelle einen Anwendungsfall dar, bei dem ein Identity Provider durch eine Universität betrieben wird. Insbesondere im Fall der Identity Assurance, bei der das Identitätsfeststellungsverfahren oftmals als Bürde empfunden wird, wird verdeutlicht, dass Universitäten schon seit eh und je die Identität ihrer, z.B. Studierenden, überprüfen, woraus folgt, dass dieses Verfahren nicht neu zu etablieren ist, sondern lediglich auf das passende Assurance-Profil abgebildet werden muss. Dazu wird auf ein rollenbasiertes Vorgehen verwiesen, da sofern die Rolle einer Person bekannt ist, wie bspw. Student oder Angestellter, das damit assoziierte Verfahren zur Identitätsfeststellung bekannt ist und somit die entsprechende Identity Assurance Information herausgegeben werden kann. Natürlich sind auch Sonderfälle, wie bspw. Studierende eines Auslandssemesters, die ebenfalls die Rolle Student einnehmen, aber deren Identitätsfeststellung u.U. auf eine andere Art und Weise abläuft, zu beachten. Die Identity Provider Seite wird in dieser Arbeit jedoch nicht weiter vertieft (vgl. Abschnitt 2.5) und ist im Rahmen von Folgearbeiten zu adressieren.

Fokus dieses Abschnitts ist die Service Provider Seite gemäß [ZSG+21a], bei der unter Verwendung eines risikobasierten Ansatzes Service Provider bei der Auswahl eines angemessenen Authentication-Assurance-Profils (vgl. SFA- und MFA-Profil) unterstützt werden.

Im Allgemeinen ist die Auswahl eines angemessenen Assurance Levels bzw. Profils eng mit dem Risikomanagement verknüpft, wie es auch durch „*Identity assurance is concerned with the proper management of risks associated with identity management.*“ [BBMS07] verdeutlicht wird. Somit wägen Service Provider idealerweise die durch den Service zugreifbaren Assets gegen die ausgesetzten Risiken und gegen den Wert des/der Assets ab. In diesem Zusammenhang spielen Prozessmanagement-Rahmenwerke eine wichtige Rolle, wie bspw. die ISO/IEC 27001, die das Asset- und Risikomanagement in das übergreifende Informationssicherheitsmanagement einbettet. Gemäß ISO/IEC 27001 [ISO13a] ist der Risikomanagement-Prozess in zwei elementare Teilaktivitäten untergliedert, nämlich die *Risikobeurteilung*, die wiederum die Identifikation von Risiken, deren Analyse und Bewertung umfasst (siehe Punkt 2 in nachfolgender Auflistung) sowie die *Risikobehandlung*, die sich mit Behandlungsstrategien (i.W.: Akzeptieren eines Risikos, Vermeiden eines Risikos, Reduzieren eines Risikos, Übertragen eines Risikos) und der Akzeptanz von Restrisiken beschäftigt (siehe Punkt 3 in nachfolgender Auflistung). Die Auswahl eines angemessenen Authentication-Assurance-Profils (d.h. keine Authentication Assurance, SFA oder MFA) kann dabei als Maßnahme zur Risikoreduktion betrachtet werden. Risiken stehen dabei im Bezug zu organisatorischen Assets, wobei die Assets in einem organisationsweiten Asset-Inventar zu kategorisieren und dokumentieren sind. Im Fall von Authentifizierungen und dem damit verbundenen Risiko des unberechtigten Zugriffs, das weiter unten elaboriert wird, können grundsätzlich beliebige, durch einen föderierten Service zugreifbare Asset-Kategorien betroffen sein und sind

nicht auf eine spezifische Art von Assets beschränkt (vgl. Auflistung der Asset-Kategorien auf Seite 175).

Unter der Annahme, dass ein Service Provider einer Identitätsföderation die Prozesse zum Asset- und Risikomanagement bereits etabliert hat, würde die Auswahl eines angemessenen Assurance-Profils für einen durch föderierte Identitäten zugreifbaren Service auf einem dreistufigen Vorgehen basieren, wobei die Schritte 1 und 2 gemäß den Asset- und Risikomanagement-Prozessen bereits durchgeführt wurden [ZSG+21a]:

1. Identifizierung aller organisatorischen Assets, Erzeugung eines Asset-Inventars
2. Risikobeurteilung für jedes der Assets
3. Risikobehandlung durch Auswahl eines angemessenen Authentication-Assurance-Profils (d.h. keine Authentication Assurance, SFA oder MFA) als Teilmenge verschiedener Maßnahmen sowie die Akzeptanz von Restrisiken

Jedoch ist die Etablierung und Aufrechterhaltung formaler Prozesse kosten- und zeitintensiv und stellt vor allem im wissenschaftlichen Bereich eine Herausforderung dar. Das Leibniz-Rechenzentrum in München erhält bspw. im Jahr 2019 als erstes wissenschaftliches Höchstleistungs-Rechenzentrum in Europa die Zertifikate der Normen ISO/IEC 20000 (Service Management) und ISO/IEC 27001 (Informationssicherheitsmanagement) [Lei19] und stellt somit zu diesem Zeitpunkt eine Vorreiterrolle gegenüber anderen deutschen wissenschaftlichen Einrichtungen dar.

Es werden folglich Hilfestellungen und Anleitungen für Service Provider zur Auswahl eines angemessenen Authentication-Assurance-Profils benötigt, die keine formalen Prozesse implementiert haben. Da der Fokus dieser Arbeit auf der Authentifizierung und der Authentication Assurance liegt, wird im Folgenden das Risiko des *unberechtigten Zugriffs* betrachtet (d.h. *Wie sicher bzw. verlässlich ist es, dass sich die „richtige“ Person einloggt?*), dem Service Provider, die Zugriff auf ihre(n) Dienst(e) unter Verwendung föderierter Identitäten erlauben, ausgesetzt sind. Ein unberechtigter Zugriff auf einen Dienst kann dabei auf verschiedenartige Bedrohungen und Schwachstellen zurückzuführen sein, ob ausgelöst durch einen Angriff, wie bspw. Identitätsdiebstahl, oder aufgrund eines Authentifizierungsfehlers.

Wie in Abschnitt 4.3 bereits beschrieben wurde, können nicht alle Bedrohungen und Schwachstellen durch die Auswahl eines angemessenen Authentication-Assurance-Profils reduziert werden, weswegen daneben noch weitere Maßnahmen, die nicht Teil dieser Arbeit sind, benötigt werden.[2]

Um einen potentiellen Schaden und dessen Auswirkung klassifizieren und diesen präventiv durch Auswahl eines entsprechenden Authentication-Assurance-Profils (neben begleitenden Maßnahmen) mindern zu können, müssen zunächst die involvierten Assets identifiziert werden. Abbildung 5.18 greift dabei erneut die in der Architektur (siehe Abbildung 4.3) erarbeiteten Informationsobjekte auf (d.h. `AuthNAssurance` `AuthenticationRisk`, `Asset` und

[2] Weitere Maßnahmen zur Reduktion eines unberechtigten Zugriffs sind beispielsweise regelmäßige Sicherheitsupdates der Systeme, die Klassifikation von Informationen gemäß verschiedener Vertraulichkeitsstufen sowie die Etablierung eines Berechtigungskonzeptes.

`Harm`) und verdeutlicht die Schritte des in [ZSG+21a] erarbeiteten Vorgehens. Im Folgenden werden diese von oben beginnend nach unten fortführend erläutert.

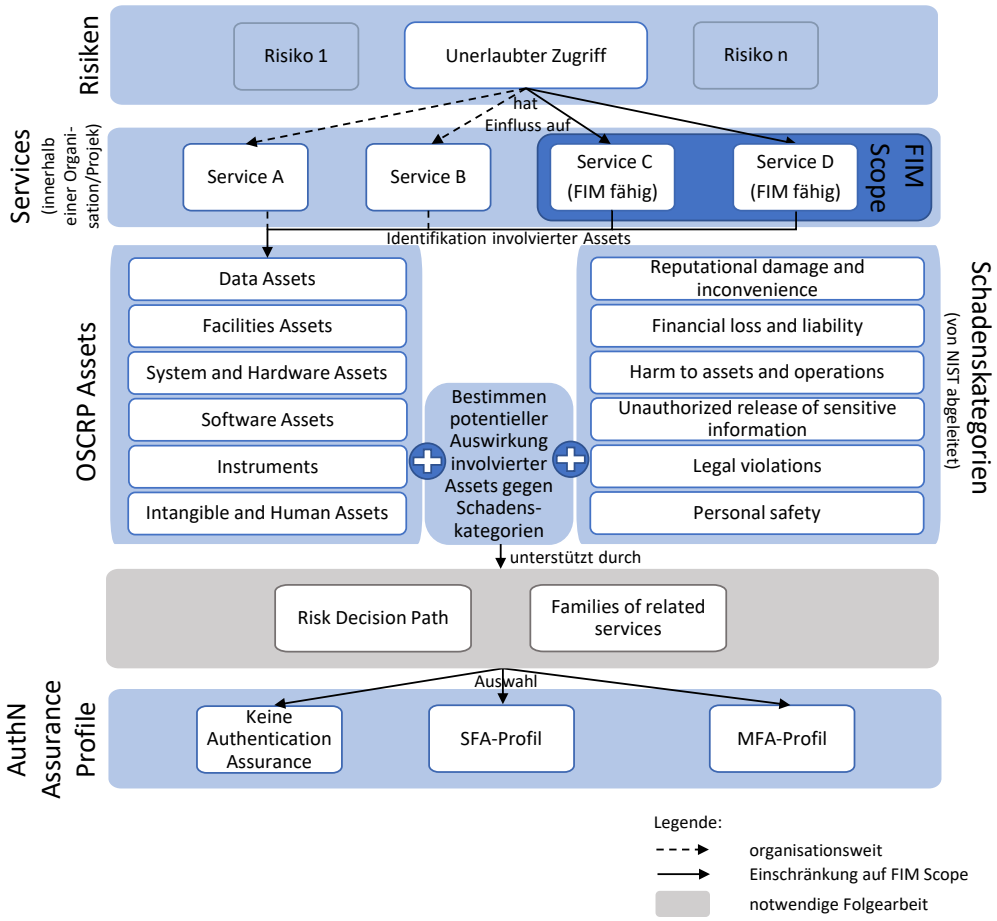


Abbildung 5.18: Ablaufschritte eines risikobasierten Vorgehens

Das mit Authentifizierungen verbundene Risiko des unberechtigten Zugriffs (`Authentication-Risk`), neben weiteren auf Services bezogene Risiken, bei dem eine Person, z.B. ein Angreifer, einen Benutzeraccount einnimmt, der ihm nicht rechtmäßig zusteht, wirkt auf das bzw. die Assets (`Asset`), die durch einen föderierten Service nutzbar bzw. zugreifbar sind. Anstatt der Identifikation und Bewertung aller organisatorischen Assets, wie es durch Prozessmanagement-Rahmenwerke (innerhalb eines definierten Anwendungsbereiches) vorgeschrieben ist, kann der Fokus mit Blick auf FIM weiter eingeschränkt werden (vgl. dunkelblaue Box in Abbildung 5.18) und nur diejenigen Services analysiert werden, auf die durch das Konzept einer Föderation zugegriffen werden kann. Weiter zu berücksichtigen ist, dass lediglich der Teil des Services bzw. der Transaktion zur Auswahl eines angemessenen Assurance-Profils zu bewerten ist, der mittels FIM zugreifbar ist und nicht zwangsweise der gesamte, unterstützte Geschäftsprozess [GGF17b]. Zur Klassifikation von Assets stellt das *Open Science Cyber Risk Profile (OSCRP)* [PVWB+20] einen pragmatischen Startpunkt dar, da dieses zwischen sechs gängigen wissenschaftlichen Asset-Kategorien (Attribut `category`) unterscheidet.

Diese sind (in Englisch aufgelistet) [PVWB+20]:

- Data Assets
- Facilities Assets
- System and Hardware Assets
- Software Assets
- Instruments
- Intangible and Human Assets

Die sechs Asset-Kategorien werden dann jeweils weiter in Unterkategorien verfeinert. Für *Data Assets* sind dies gemäß OSCRP bspw. die Folgenden (ebenfalls in Englisch aufgelistet):

- Public Data
- Non-Public Data
- Internal Data
- Documentation
- Accounting Information
- For Approved Access Only

Die gemäß OSCRP spezifizierten Asset-Kategorien können somit als initiale Orientierung verwendet werden, wobei Asset-(Unter-)Kategorien je nach Bedarf hinzugefügt, modifiziert oder entfernt werden können.

Nach der Identifikation und Dokumentation der betroffenen Assets lassen sich diese gegen die von NIST definierten Schadenskategorien [GGF17b] testen. Die Schadenskategorien (vgl. Klasse `Harm`, Attribut `category`) wurden dazu in [ZSG+21a] z.T. generalisiert, da das Rahmenwerk von NIST ursprünglich aus dem Bereich der US-Regierung stammt. Die von NIST abgeleiteten Schadenskategorien sind (in Englisch) die Nachfolgenden. Dabei handelt es sich nicht um ein Ordnungssystem, stattdessen wurden die Schadenskategorien lediglich aus Gründen der besseren Referenzierbarkeit nummeriert.

1. Reputational damage and inconvenience
2. Financial loss and liability
3. Harm to assets and operations
4. Unauthorized release of sensitive information
5. Legal violations
6. Personal safety

In [ZSG+21a] sind diese Kategorien jeweils mit Beispielen aus R&E versehen; ferner wird anhand von zwei realen Beispielen dargestellt, wie die Asset- und Schadenskategorien des

erarbeiteten Konzepts angewendet werden können, um ein angemessenes Assurance-Profil herzuleiten. Im Folgenden wird eines der Beispiele aufgegriffen.

Das erste Beispiel in [ZSG+21a] stellt die Forschungsinfrastruktur ELIXIR aus dem Bereich der Lebenswissenschaften dar, auf die bereits in Abschnitt 2.4 Bezug genommen wurde. ELIXIR stellt u.a. Zugriff auf biologische Daten und Daten bezogen auf Menschen (z.B. Genomsequenzen) bereit und hat somit starke Anforderungen, wer und zu welchem Zweck auf die Daten zugreift und diese verarbeitet. Gemäß OSCRP handelt es sich in diesem konkreten Fall um *Data Assets*, die aufgrund des Bezuges zum Menschen gesetzlichen Bestimmungen unterliegen, sodass gemäß der ableiteten Schadensklassifikation von NIST eine hohe Auswirkung in der Schadenskategorie *legal violations* zu erwarten ist. Darüber hinaus sind die Daten auch strikt vor unbefugter Verarbeitung oder Veränderung zu schützen (vgl. im Besonderen *Harm to assets and operations* und *Unauthorized release of sensitive information*). Um die Risiken des unberechtigten Zugriffs zu mitigieren, fordert ELIXIR eine starke Authentifizierung und ermöglicht neben einem MFA-Step-Up Service [Lin19] ebenfalls REFEDS-MFA basierend auf dem Identity Provider ORCID, um diesem entgegenzuwirken.

Ein weiteres Beispiel in diesem Zusammenhang, welches in [ZSG+21a] nicht erläutert wurde, stellt das *National Institute of Health* dar, das ebenfalls aufgrund des Bezuges zum Gesundheitssektor ab September 2021 die Verwendung einer Multi-Faktor-Authentifizierung für bestimmte Dienste fordert [InC21].

In Abschnitt 6.2.2, als Teil der Evaluation, prototypischen Implementierung und Anwendung, wird das in Abbildung 5.18 skizzierte Vorgehen exemplarisch einmal durchlaufen. Dazu wird ein Webdienst, der einen Ablageort für projektspezifische Ergebnisse implementiert, betrachtet, der aufgrund der Teilnahme an einer Identitätsföderation dem authentifizierungsbezogenen Risiko des unberechtigten Zugriffs ausgesetzt ist.

In Ergänzung zu dem OSCRP Asset-Klassifikationsschema und den abgeleiteten NIST-Schadenskategorien kann mit Blick auf Folgearbeiten im nächsten Schritt ein *Risk Decision Path* spezifiziert werden. Dabei können durch das Stellen gezielter Fragen Service Provider bei der Auswahl eines angemessenen Authentication-Assurance-Profils weiter unterstützt werden. Dazu werden die verschiedenen Authentication-Assurance-Profile aus Abschnitt 5.2 als (vertikale) Swimlanes dargestellt, woraus sich insgesamt drei Swimlanes ergeben:

- keine Authentication Assurance bzw. keine Authentifizierung
- SFA
- MFA

Der Referenzpunkt bzw. Startpunkt des Risk Decision Path liegt in der mittleren Swimlane, d.h. bei dem SFA-Profil, welches bei Webauthentifizierungen den gewöhnlichsten Fall darstellt, wobei sich die Lage des Startpunkts je nach Anwendungsfall auch in eine der beiden Richtungen verschieben lässt. Unter der Annahme, dass der Startpunkt in der mittleren Swimlane liegt, wird ein Service Provider dann durch das Beantworten gezielter Fragen durch den Risk Decision Path navigiert, wobei dieser potentiell mehrere Swimlanes durchläuft und am Ende dann in derjenigen Swimlane ankommt, die für den konkreten Anwendungsfall des Service Providers am geeignetsten scheint. Das Set der Fragen gilt es zu spezifizieren, stets

unter Berücksichtigung der Asset- und Schadenskategorien sowie mit Blick darauf, wie sehr ein Service Provider seine User tatsächlich kontrollieren muss. Der Risk Decision Path könnte bspw. mit folgender Frage starten: *Müssen wiederkehrende Benutzer erkannt werden?* Lautet die Antwort „nein“ würde ein Service Provider zur nächsten Frage navigiert werden, die in der Swimlane „keine Authentication Assurance“ liegt, wohingegen bei Antwort „ja“ der Befragte mit der nächsten Frage aus der mittleren Swimlane konfrontiert wird. Die Fragen sollten dabei möglichst einfach und mit einer begrenzten Auswahl an Antworten entworfen werden.

Um Service Provider weiter bei der Auswahl eines angemessenen Authentication-Assurance-Profils zu unterstützen, können Risikobewertungen für gängige Servicetypen, bspw. unter Berücksichtigung eines vorhandenen Service-Katalogs, durchgeführt und der Allgemeinheit bereitgestellt werden. Dazu sind Templates erforderlich, die das OSCRP Asset-Klassifikationsschema, die abgeleiteten NIST-Schadenskategorien sowie die oben aufgelisteten Authentication-Assurance-Profile (vgl. Swimlanes) in Bezug zueinander setzen. Als Resultat können Gruppen von Familien mit ähnlichen Assurance-Anforderungen (vgl. *families of related services* in [For17]) erzeugt werden [ZSG+21a].

5.4 Konzept zur Realisierung eines Fallback MFA-Workflows

Da die Erweiterung des existierenden 1FA-Workflows um die Schritte zur Realisierung eines Fallback-MFA Workflows bereits ausführlich in Abschnitt 4.4, im Besonderen anhand des Kommunikationsmodells, skizziert wurde, wird an dieser Stelle auf eine erneute Darstellung des resultierenden MFA-Workflows verzichtet. Die lesende Person wird stattdessen auf Abschnitt 4.4.4 verwiesen, der anhand eines UML-Sequenzdiagramms die erweiterten Schritte aufzeigt. Die dazu notwendige Erweiterung der SP-Komponente wird an späterer Stelle in Abschnitt 6.3.2 prototypisch implementiert.

Zur Realisierung des MFA-Workflows muss das in Abschnitt 5.2.1 skizzierte SFA-Profil erweitert werden, was in dem entsprechenden Modell des Architekturteils WF (vgl. Abschnitt 4.5) noch nicht detailliert wurde. Dies umfasst die **Erweiterung der URI des SFA-Profils im Authentifizierungskontext**, da gemäß des Fallback MFA-Workflows die jeweiligen Faktoren nun von mehreren Faktorprüfern (i.S.v. IDP und TPP) stammen,[3] sodass u.a. zu evaluieren ist, ob die Authentifizierungsfaktoren der eingesetzten Faktorprüfer tatsächlich unterschiedlichen Typs sind. Da sowohl IDPs als auch TPPs mit einem Authentifizierungskontext auf eine Anfrage eines SPs antworten (vgl. Abbildung 4.2), geht anhand der high-level URI *https://refeds.org/profile/sfa* des SFA-Profils aus Abschnitt 5.2.1 nicht hervor, welche Art von Faktor bei einer Authentifizierung herangezogen wurde.

An dieser Stelle ist zu diskutieren, ob die repräsentierende Klasse, wie z.B. *memorized secret* ausreichend ist oder ob die konkrete (Realisierungs-) Methode, wie „Passwort“ oder „PIN“, der URI hinzugefügt werden sollte. Um potentielle Fehler in der Verarbeitung zu reduzieren, sollte die Verwendung von standardisierten URIs zunächst auf ein Minimum be-

[3] d.h. MFA resultiert aus einer Summe mehrerer 1FAs

schränkt werden, weswegen hier die Verwendung der übergreifenden Klasse vorgeschlagen wird. Somit wird die SFA-Spezifikation aus Abschnitt 5.2.1 durch die folgenden vier URIs verfeinert:

- https://refeds.org/profile/sfaMemorizedSecret
- https://refeds.org/profile/sfaTotp
- https://refeds.org/profile/sfaHotp
- https://refeds.org/profile/sfaCryptographicSD

Die Erweiterung der URI des SFA-Profils im Authentifizierungskontext ist dabei ebenfalls für proxy-basierte Szenarien nützlich (vgl. Abschnitt 2.4), bei denen Authentifizierungsinformationen ebenfalls aus mehreren Quellen stammen.

Ferner ist eine potentielle Erweiterung der URI für MFA in Folgearbeiten zu analysieren, insbesondere unter dem Aspekt, dass in einer Antwortnachricht nur ein Wert im Authentifizierungskontext angegeben werden kann. Wie aus Abschnitt 3.5 und den Templates des Universellen Modells in Abschnitt 5.1.4.3 ersichtlich wurde, existiert eine Vielzahl unterschiedlicher Realisierungsmöglichkeiten für MFA (vgl. z.B. IDP-seitiges MFA versus Verwendung einer Trusted Third Party), die Einfluss auf das Vertrauen haben können, da unterschiedliche verifizierende Entitäten zum Einsatz kommen und daher ggf. weiter berücksichtigt und an einen SP kommuniziert werden sollten.

5.5 Abschließende Bewertung

Die Einführung und Konkretisierung von UASM in Abschnitt 5.1 hat gezeigt, wie komplex Authentifizierungsszenarien inzwischen geworden sind und dass es daher umso wichtiger ist, ein Gesamtbild herzustellen, bevor neue Komponenten in einer Infrastruktur hinzugefügt oder Änderungen durchgeführt werden. Ferner wurde verdeutlicht, dass die Modellierung der Authentifizierung bzw. deren Komponenten als Service durchaus seine Daseinsberechtigung haben und dass das MNM Service Modell inkl. dessen verschiedene Sichten eine geeignete Grundlage bilden. Aufbauend auf MSM wurde eine einheitliche Terminologie für Authentifizierungsszenarien erzeugt und darüber hinaus verschiedene UASM Sichten für eine service-orientierte Darstellung abgeleitet. Ergänzend wurden MFA Templates als Hilfestellung erarbeitet.

In Abschnitt 5.2 wurde das Authentication-Assurance-Konzept, im Speziellen das SFA-Profil, vorgestellt, welches sowohl Kriterien für Authentifizierungsfaktoren als auch Kriterien für Prozeduren zum Ersetzen eines Authentifizierungsfaktors umfasst. Für das MFA-Profil, das ursprünglich aus der amerikanischen Föderation InCommon stammt, wurde eine Erweiterung der Kriterien vorgeschlagen, damit die verwendeten Faktoren, analog zum SFA-Profil, ebenfalls mit Qualitätskriterien versehen sind. Außerdem wurde zum Verständnis des Gesamtbildes das REFEDS Identity Assurance Framework [REF18a] kurz umrissen, da dieses anhand der Cappuccino- und Espresso-Profile gemeinsame Schnittstellen mit dem SFA- und MFA-Profil aufweist.

In Abschnitt 5.3 wurde aufbauend auf den Authentication-Assurance-Profilen gezeigt, wie das Asset-Klassifikationsschema des Open Science Cyber Risk Profile in Kombination mit den Schadenskategorien abgeleitet von NIST sinnvoll angewendet werden können, um Service Provider bei der Auswahl eines angemessenen Authentication-Assurance-Profils zu unterstützen.

Zuletzt wurde in Abschnitt 5.4 das Konzept zur Realisierung eines Fallback MFA-Workflows vorgestellt, wobei bereits im Rahmen des Kapitels 4 (Architektur) anhand eines UML-Sequenzdiagramms (vgl. Abbildung 4.7) die jeweiligen Ablaufschritte verdeutlicht wurden. Ferner wurde die URI des SFA-Profils, die im Authentifizierungskontext angegeben wird, erweitert, um eine exakte Evaluation und Aggregation (vgl. Funktion `aggregateAAL()`) der verwendeten Authentifizierungsfaktoren zu ermöglichen.

Im folgenden Kapitel 6 werden die entsprechenden Konzepte der Architektur gegen die Anforderungen abgeglichen und bewertet sowie prototypisch implementiert und angewendet.

Kapitel 6

Evaluation, prototypische Implementierung und Anwendung

Inhalt dieses Kapitels

Ziel dieses Kapitels ist die Evaluation, prototypische Implementierung und Anwendung der Konzepte des vorherigen Kapitels.

Dazu wird in Abschnitt 6.1 das Universelle Modell für Authentifizierungsszenarien erneut aufgegriffen und anhand der Anforderungen aus Abschnitt 2.6.5 den in Abschnitt 3.7.3 bereits evaluierten Informations- und Service-Managementmodellen gegenübergestellt.

Im darauffolgenden Abschnitt 6.2 wird dargestellt, wie anhand eines Reviewprozesses innerhalb der R&E Community die Kriterien des publizierten SFA-Profils evaluiert wurden. Es findet eine Diskussion und Bewertung unter Einbezug der Anforderungen statt; ferner wird auch der risikobasierte Ansatz zur Auswahl eines angemessenen Authentication-Assurance-Profils methodisch angewendet.

Zuletzt findet in Abschnitt 6.3 eine prototypische Implementierung des Fallback MFA-Workflows statt, wobei ebenfalls die technische Anwendbarkeit des SFA-Profils sowie deren

vorgeschlagene Erweiterungen getestet werden. Zusätzlich werden verschiedene Anwendungsmodelle betrachtet, die methodisch darstellen, wie der erarbeitete MFA-Workflow auf reale Szenarien übertragbar ist.

Das Kapitel schließt mit einer Zusammenfassung ab.

6.1 Evaluation von UASM

In Abschnitt 5.1 wurde UASM auf Basis des in Abschnitt 4.5 spezifizierten Architekturteils UM systematisch erarbeitet. Es wurden die zentralen Rollen RAS, TAS, TAP und TAC eingeführt und auf Basis von MSM Interaktionen gemäß Nutzungs- und Managementfunktionalität klassifiziert. Es wurde das generische Konzept von AuthNI bzw. TAuthNI eingeführt und nach Analyse zahlreicher Use Cases die zwei Serviceklassen TAAS und TAPS abgeleitet. Basierend auf dem MSM Basic Service Model wurde die UASM Basic View abgeleitet, die nach schrittweiser Verfeinerung in der $\text{UASM}_{\text{subject-service}}$ Basic View resultiert. Anhand der UASM Service View wurden die durch MSM klassifizierten seitenunabhängigen Aspekte in Authentifizierungsszenarien genauer betrachtet, während durch die UASM Realization View die Provider-interne Realisierung und das Prinzip von Service-Hierarchien (Verkettung bzw. Rekursion) erläutert wurde. Unter Berücksichtigung der MFA-Forschungsansätze aus Abschnitt 3.5 sowie des in dieser Arbeit spezifizierten MFA-Workflows wurden MFA Templates erarbeitet, die bei der Beschreibung und Modellierung eines Authentifizierungsszenarios als Hilfestellung herangezogen werden können.

Das Ziel dieses Abschnitts ist die Evaluation dieser Aspekte gegen die Anforderungen aus Abschnitt 2.6.5. Zugleich soll UASM einer methodischen Anwendung unterzogen werden, um dessen Anwendbarkeit in realen Authentifizierungsszenarien zu beweisen. Da in Abschnitt 5.1 die UASM Komponenten und Konzepte jedoch stets unter Einbezug repräsentativer Beispiele erarbeitet wurden, wird an dieser Stelle auf eine erneute (methodische) Anwendung verzichtet. Die lesende Person wird stattdessen im Besonderen auf Abschnitt 5.1.4.2 verwiesen, in dem ausführlich anhand eines Sales Services die UASM Basic View erläutert wird. Wie sich hier zeigt, greift der Sales Service auf einen Student Validation Service zurück, anhand dessen Studenten einen Rabatt auf Produkte des Sales Services bekommen. Der Student Validation Service nutzt wiederum den SAML IDP eines Nutzers zur Authentifizierung, wodurch neben der generellen Anwendbarkeit auch die rekursive Anwendung eines TAPS demonstriert wird.

Im folgenden Abschnitt findet daher direkt eine Diskussion und Bewertung von UASM unter Einbezug der Anforderungen statt.

6.1.1 Diskussion und Bewertung

Der Abgleich der Anforderungen mit SID und MSM hat bereits in Abschnitt 3.7.3 gezeigt, dass der Erfüllungsgrad der beiden Frameworks, in Hinblick auf die spezifizierten Anforderungen gleichwertig ist (siehe auch Tabelle 6.1 auf Seite 184). Daher werden nachfolgend im

Besonderen diejenigen Anforderungen diskutiert, die durch SID und MSM nicht oder nur teilweise erfüllt werden. Dabei wird im Besonderen überprüft, da UASM auf MSM aufbaut, inwiefern die Anforderungen durch UASM erfüllt werden. Durch SID und MSM werden die folgenden Anforderungen *teilweise erfüllt*:

- [FA_Terminologie]
- [FA_Managementaspekte]
- [FA_Nutzungsaspekte]

Nicht erfüllt wurde die Anforderung:

- [FA_Schablonen]

Die Erfüllung der Anforderung [FA_Terminologie] durch UASM kann an dieser Stelle klar als *erfüllt* beantwortet werden, da die Etablierung einer einheitlichen Terminologie gemäß des integrierten Anforderungskataloges eine essentielle Anforderung darstellt und somit beim Design von UASM aufbauend auf MSM explizit berücksichtigt wurde. Auf Basis des generischen Begriffs AuthNI bzw. TAuthNI wurde eine protokoll- und technologie-agnostische Terminologie für UASM Entitäten und UASM Services entwickelt. Ein positiver Effekt, bei der doch recht komplizierten Namensgebung, zeigt sich bei den verwendeten Abkürzungen, wobei UASM Entitäten konsistent mit einer Abkürzung bestehend aus drei Buchstaben und UASM Services mit vier Buchstaben abgekürzt werden.

Da sowohl SID und MSM die Anforderungen [FA_Managementaspekte] und [FA_Nutzungsaspekte] aufgrund des fehlenden Bezuges zu Authentifizierungsszenarien nur teilweise erfüllen, wurden in UASM die entsprechenden Funktionalitäten aufgegriffen und adressiert. V.a. in der UASM Service View, die die seitenunabhängigen Aspekte von Authentifizierungsszenarien näher beleuchtet, sind einige dieser Aspekte exemplarisch in Abbildung 5.12 dargestellt. Als zukünftige Folgearbeit sollten diese erneut aufgegriffen und gemäß MSM anhand von z.B. UML-Sequenzdiagrammen weiter detailliert werden.

Zwar stellen SID und MSM verschiedene Templates (vgl. Anforderung [FA_Schablonen]) bereit, wie z.B. im Falle von MSM die MSM Basic View, die Service View und Realization View, jedoch wurden diese noch nicht auf komplexe und heterogene Authentifizierungssysteme angewendet. Wie sich in Abschnitt 5.1.4 zeigt, wurde basierend auf der MSM Basic View nicht nur eine UASM Basic View abgeleitet, sondern insgesamt vier Basic Views, die schrittweise verfeinert wurden und schlussendlich in einer Zusammenführung der Ausprägungen münden (vgl. $\text{UASM}_{\text{subject-service}}$ Basic View in Abbildung 5.3). Im Gegensatz zur $\text{UASM}_{\text{subject-service}}$ Basic View werden in der $\text{UASM}_{\text{generic}}$ Basic View, der initialen Ausprägung, Subjekte noch nicht als selbstständig handelnde Entitäten betrachtet. Dadurch lässt sich eine Vielzahl von Anwendungsfällen abdecken, wie z.B. Szenarien bei denen reale Tiere authentifiziert bzw. gezählt werden. Darüber hinaus wurden die verschiedenen MFA-Forschungsansätze aus Abschnitt 3.5 sowie der in dieser Arbeit spezifizierte MFA-Workflow mithilfe der UASM Basic View modelliert (vgl. Abbildungen 5.8 bis 5.10), sodass die generierten Templates ebenfalls als Hilfe bei der Modellierung zukünftiger Authentifizierungsumgebungen herangezogen können. Der Abschnitt 5.1.5.1 zeigt high-level, wie die MFA Templates der UASM Service View aussehen. Die Anforderung gilt somit ebenfalls als erfüllt.

Abschließend zusammengefasst, kann UASM somit entweder allein oder in Kombination mit dem zugrundeliegenden MSM angewendet werden. Während sich MSM für die Beschreibung und Modellierung beliebiger Service Provider eignet, spezialisiert sich UASM auf die authentifizierungsbezogenen Abhängigkeiten von Entitäten und Services.

Tabelle 6.1: Gegenüberstellung und Bewertung von UASM

Anforderung	**Gewichtung**	**TM Forum SID**	**MNM Service Model**	**UASM**
[FA_Terminologie]	(4)	(✓)	(✓)	✓
[FA_Service_Orientierung]	(4)	✓	✓	✓
[FA_Rekursion]	(4)	✓	✓	✓
[FA_Managementaspekte]	(2)	(✓)	(✓)	✓
[FA_Nutzungsaspekte]	(2)	(✓)	(✓)	✓
[FA_Schablonen]	(1)	✗	✗	✓
$G(p) = \sum w \cdot p$	G(p) max 34	24	24	34

✓: Anforderung erfüllt (2 Punkte)
(✓): Anforderung teilweise erfüllt (1 Punkt)
✗: Anforderung nicht erfüllt (0 Punkte)

wobei w: Gewichtung, p: Punkte und $G(p)$: Gesamtsumme Punkte

6.2 Evaluation des SFA-Profils sowie Anwendung des risikobasierten Ansatzes zur Auswahl eines angemessenen Authentication-Assurance-Profils

Nachdem die Kriterien des SFA-Profils in Abschnitt 5.2.1 vorgestellt wurden, werden diese im nächsten Schritt hinsichtlich deren Umsetzbarkeit in Identitätsföderationen überprüft. Da, wie bereits erwähnt, die Spezifikation aus der REFEDS Assurance Working Group hervorgegangen ist, sieht REFEDS, bevor Spezifikationen in eine finale, publizierte Version übergehen, die Durchführung einer sogenannten „Community Consultation“ vor, deren Vorgehensweise im Folgenden erläutert wird. Dazu wird auf die veröffentlichten Ergebnisse in [ZSL19] Bezug genommen.

Gemäß REFEDS ist der Zweck einer Community Consultation „*to ensure that broad consensus is achieved within the community. Consistent consultation and consensus gathering means that adoption is significantly more likely.*“ [REF20c]. In dieser Community sind sowohl Repräsentanten von nationalen Identitätsföderationen als auch von Forschungsinfrastrukturen vertreten (vgl. Szenarien nationales FIM und Forschungsinfrastrukturen). Darüber hinaus verdeutlicht eine Übersicht der Föderationen [REF20b] die Größe des Adressatenkreises der Community Consultation.

Das Ziel der Consultation war also primär das Erzielen eines Konsensus hinsichtlich der Anwendbarkeit bzw. Annahmefähigkeit innerhalb der Community (vgl. v.a. Nicht-funktionale Anforderungen). Im Rahmen dieses Vorgehens kann zwar potentielles Bedenken hinsichtlich der technischen Umsetzbarkeit gegeben werden, jedoch handelt es sich nicht um einen technischen Piloten (i.S.v. der Überprüfung der Implementierbarkeit). Die Implementierbarkeit (vgl. Anforderung [NFA_LoA_Implementierbarkeit]) wurde sowohl durch einen technischen Piloten der REFEDS Assurance WG [ZSL19, REF18b] sowie unabhängig davon, durch die in Abschnitt 6.3 beschriebene Testumgebung als Teil des Fallback-MFA Workflows verifiziert.

Das sich in einem Draft-Modus befundene SFA-Profil wurde somit der Community zum Review vorgelegt. In einem Zeitraum von üblicherweise vier bis sechs Wochen haben die Community Member dann die Möglichkeit Feedback zu dem Draft geben. Als Teil dieses Kapitels werden die Ergebnisse der Community Consultation des SFA-Profils aufgegriffen. Zwar fand zeitgleich zur SFA-Profil Consultation auch die der Identity Assurance (REFEDS Assurance Framework) statt, da der Fokus dieser Arbeit auf der Authentication Assurance liegt, werden die Ergebnisse der Identity Assurance an dieser Stelle nicht weiter vertieft.

Explizit zu erwähnen ist, dass eine abgeschlossene Community Consultation nicht automatisch zum Übergang in eine finale, publizierte Version führt. Im Fall der Identity Assurance waren bspw. zwei Community Consultation Runden erforderlich, da der erste Reviewprozess gezeigt hat, dass gemäß Einschätzung der Community Member noch größere Überarbeitungen erforderlich sind, bevor die Spezifikation in eine finale Version übergehen kann.

Im Fall des SFA-Profils war eine Review-Runde ausreichend. Hierzu wurde in einem Change Log (vgl. Abbildung 6.1) das Feedback der Community Member erfasst. Im nachfolgenden Abschnitt wird das Feedback des Reviews diskutiert und die Anforderungen aus Abschnitt 2.6.2 aufgegriffen.

6.2.1 Diskussion und Bewertung

Die Tabelle 6.2 listet dazu die Sub-Anforderungen der Hauptanforderung AK erneut auf und stellt eine Gegenüberstellung mit den in Abschnitt 3.6.4 evaluierten LoA-Rahmenwerken bereit. Die letzte Spalte der Tabelle 6.2 repräsentiert dabei sowohl das SFA-Profil als auch das MFA-Profil, um das ganzheitliche Authentication-Assurance-Konzept zu betrachten. Hierbei zeigt sich, dass alle Anforderungen durch das SFA- und MFA-Profil erfüllt werden; in der nachfolgenden Diskussion aufgrund der durchgeführten Community Consultation jedoch v.a. das SFA-Profil einer detaillierten Bewertung unterzogen wird.

Number	Line / Reference	Proposed Change or Query	Proposer	Action / Decision (please leave blank)
1	General	The proposal sticks quite closely to NIST's guidelines (https://pages.nist.gov/800-63-3/sp800-63b.html) - it would be helpful to add a statement on whether these guidelines are in line with NIST 800-63B to allow people to self audit more easily	Hannah Short (CERN)	All NIST references were removed from the main document to avoid the impression that there is a connection to the NIST guidelines. Only the terminology used is aligned with NIST which is stated in the newly created appendix A.
2	Chapter 4, Table	Could those pools be opened, from where this amount of characters is taken from? Like "e.g. 52 letters (a-z)(A-Z)"	Sami Silén (CSC)	Appendix B was added which contains some examples of character sets.
3	Chapter 4, Table	Kind of minor notice, but might be something to open up a little bit. Reading this table after reading this NIST guidelines, I had problems to understand that second line in each "Authenticator type". It didn't mean secrets chosen randomly by the CSP (Which was the assumption I had got from the NIST document). Both of lines are subscriber chosen and length is just different because of wider pool.	Sami Silén (CSC)	Appendix A was added which defines the authenticator types used in the profile. This avoids the need to look into the NIST guidelines. Appendix B provides some examples, which should make it clear how to use the table.
4	Chapter 4, list	Suggest giving the required conditions names, so they can be referenced. E.g. SFA-1 (secret strength), SFA2 (secret lifetime), SFA3 (replacement). Not sure if it's worth referring to the sub-options.	Jens Jensen (STFC)	The unordered list in section 4 has been replaced by a numbered list for easy referencing.

Abbildung 6.1: Ergebnisse der REFEDS Community Consultation. Eigene Bildschirmkopie von [REF18d]

Tabelle 6.2: Gegenüberstellung und Bewertung des SFA- und MFA-Profils

Anforderung	**Gewichtung**	**NIST 800-63 v3**	**eIDAS**	**Kantara IAF**	**DFN-AAI Vertrauenswürdigkeitsklassen**	**IGTF Authentication Profiles**	**ITU-T X.1254**	**SFA-/MFA-Profil**
[NFA_LoA_Minimalität]	(4)	✗	(✓)	✗	✓	(✓)	(✓)	✓
[NFA_LoA_Modularität]	(4)	✓	✗	✗	✗	✗	✗	✓
[NFA_LoA_Umsetzbarkeit]	(4)	✗	✗	✗	✓	(✓)	(✓)	✓
[FA_LoA_1FA]	(2)	✓	✗	✓	✗	(✓)	(✓)	✓
[FA_LoA_MFA]	(2)	✓	✗	✓	✗	✗	(✓)	✓
[FA_LoA_Protokollkompatibilität]	(2)	✓	✓	✓	✓	✓	✓	✓
[NFA_LoA_Unabhängigkeit]	(2)	(✓)	✗	✓	✓	✓	✓	✓
[NFA_LoA_Implementierbarkeit]	(2)	✗	✗	✗	✓	(✓)	(✓)	✓
[NFA_LoA_Verständlichkeit]	(2)	✗	✗	✗	✓	✓	✗	✓
[NFA_LoA_Eigenständigkeit]	(1)	(✓)	✓	✗	✓	(✓)	(✓)	✓
$G(p) = \sum w \cdot p$	G(p) max 50	23	10	16	34	25	23	50

✓: Anforderung erfüllt (2 Punkte)
(✓): Anforderung teilweise erfüllt (1 Punkt)
✗: Anforderung nicht erfüllt (0 Punkte)

wobei w: Gewichtung, p: Punkte und $G(p)$: Gesamtsumme Punkte

Hierbei zeigt sich, dass die Anforderungen [FA_LoA_1FA] und [FA_LoA_MFA] durch die entsprechende Spezifikation, d.h. das SFA- bzw. MFA-Profil, erfüllt werden. Ziel war es, ein leichtgewichtiges Authentication-Assurance-Konzept zu entwickeln, das sowohl Kriterien an Authentifizierungen mit einem Faktor als auch mit mehreren Faktoren berücksichtigt. In Abschnitt 5.2.1 wurde dazu das vorab publizierte SFA-Profil aufgegriffen und gezeigt, wie dieses mit dem existierenden MFA-Profil zusammenhängt. Aufgrund der getrennten Spezifikationen wird somit auch die Anforderung [NFA_LoA_Modularität] erfüllt. Ferner erfüllen beide Spezifikationen die Anforderung [NFA_LoA_Unabhängigkeit], da keine nationalen Gegebenheiten bzw. Regulierungen integriert wurden.

Auch hinsichtlich der Anforderungen [NFA_LoA_Minimalität] und [NFA_LoA_Umsetzbarkeit] lässt sich aus den Ergebnissen der REFEDS Community Consultation (vgl. Abbildung 6.1) schließen, dass das SFA-Profil offenbar den richtigen (Detail-) Grad an Kriterien getroffen hat, da keine Anmerkungen über unverhältnismäßige SFA-Kriterien eingegangen sind. Dies ergibt sich u.a. aus der Tatsache, dass bei der Spezifikation des SFA-Profils die umfassenden Kriterien des NIST-Standards berücksichtigt wurden, diese jedoch auf ein minimal akzeptables Level herunter gebrochen wurden, um ein leichtgewichtiges Konzept zu erhalten. Obwohl das SFA-Profil zwar in Anlehnung an den NIST-Standard entstanden ist, bedeutet eine Erfüllung der Kriterien des SFA-Profils nicht automatisch die Erfüllung der NIST-Kriterien, weswegen gemäß des Kommentars mit der Nummer 1 des Reviews (vgl. Abbildung 6.1), der Bezug zum NIST-Standard entfernt bzw. in den Anhang verschoben wurde. Bei Betrachtung der Anforderung [NFA_LoA_Minimalität] in Bezug auf das MFA-Profil werden, wie bereits in Abschnitt 5.2.3 diskutiert, die Kriterien des MFA-Profils durch die Autorin als zu minimal erachtet, weswegen eine hierarchische Kopplung der beiden Profile vorgeschlagen wurde, um ebenfalls qualitative Authentifizierungsfaktoren bei Authentifizierungen mit mehreren Faktoren zu gewährleisten. Diskussionen im zweiten Halbjahr 2021, v.a. angestoßen durch das National Institute of Health, haben ebenfalls bestätigt, dass die Kriterien des MFA-Profils zu unspezifisch sind, weswegen eine REFEDS MFA Subgroup gegründet wurde, die Vorschläge zur Ergänzung des MFA-Profils erarbeitet. Hier werden v.a. zunächst implementierungstechnische Aspekte, wie z.B. die Länge von MFA SSO Sessions, adressiert.

Die Kommentare mit der Nummer 2, 3 und 4 des Reviews lassen sich hingegen der Anforderung [NFA_LoA_Verständlichkeit] zuordnen. Zu dem erhaltenen Feedback zählte hier u.a., ob die einem Geheimnis (z.B. Passwort) zugrundeliegende Zeichenbasis erweitert werden könne. Zur Verbesserung der Verständlichkeit wurde somit als Antwort auf alle drei Kommentare die Spezifikation entsprechend ergänzt. Die Anforderung [NFA_LoA_Eigenständigkeit] die zur Verständlichkeit beiträgt, wird aufgrund des Verzichtes auf Referenzdokumente ebenfalls erfüllt.

Die [FA_LoA_Protokollkompatibilität] und [NFA_LoA_Implementierbarkeit] des SFA- und MFA-Profils kann ebenfalls als erfüllt beantwortet werden. Die lesende Person wird hier im Besonderen auf die prototypische Implementierung des MFA-Workflows in Abschnitt 6.3 verwiesen, da dort die definierten URIs und die vorgeschlagenen Erweiterungen aus Abschnitt 5.4 erfolgreich mit der in R&E verwendeten Standard-Software im Rahmen einer SAML-Testumgebung konfiguriert werden.

Obwohl kein expliziter Test mit OIDC stattfand, zeigt Abschnitt 4.2.4, dass OIDC analog zu SAML das Konzept eines Authentifizierungskontexts (in OIDC als acr bezeichnet) unterstützt.

Abschließend zusammengefasst kann das Authentication-Assurance-Konzept sowohl von Föderationen föderationsintern als auch als gemeinsamer Nenner zur föderationsübergreifenden Aggregation von Assurance-Information herangezogen werden. Für diejenigen Identitätsföderationen (vgl. Szenario nationales FIM in Abschnitt 2.2), die z.T. bereits eigene Assurance Level implementieren, gilt es an dieser Stelle weiter zu untersuchen, inwieweit hier bei einem Mapping der Authentication Assurance Level unterstützt werden kann.

Da insgesamt nur vier Feedbackpunkte kleineren Ausmaßes eingegangen sind, wurde nach dessen Einarbeitung geschlussfolgert (vgl. rechte Spalte in Abbildung 6.1), dass Konsensus erzielt wurde und ein Übergang der Draft-Spezifikation in eine finale Version möglich ist. Die letzte Kontrollinstanz stellte das REFEDS Steering Committee dar, das schlussendlich das SFA-Profil final abgezeichnet und publiziert hat.

Zuletzt wurde stellvertretend durch die Autorin dieser Arbeit, zu diesem Zeitpunkt Chair der REFEDS Assurance Working Group, eine Aufnahme aller REFEDS Identity- und Authentication-Assurance-Profile bei der Internet Assigned Numbers Authority (IANA) in der Protocol Registry unter „Level of Assurance (LoA) Profiles“ [Int20] in Konformität mit der RFC 6711 [Joh12] beantragt. Nach stattgefundenem Experten Review wurden diese im Jahr 2019 erfolgreich registriert.

6.2.2 Methodische Anwendung des risikobasierten Ansatzes

Im nächsten Schritt findet, aufbauend auf der Diskussion und Bewertung des SFA- sowie MFA-Profils, eine methodische Anwendung des risikobasierten Ansatzes statt. Es wird gezeigt, wie die Auswahl eines angemessenen Authentication-Assurance-Profils unter Zuhilfenahme der abgeleiteten Schadenskategorien von NIST sowie dem OSCRP Asset-Klassifikationsschema erfolgt. Dazu wird ein triviales Beispiel, nämlich ein Webdienst, der einen Ablageort für projektspezifische Daten bzw. Ergebnisse implementiert (häufig als Wiki bezeichnet) und mittels FIM zugreifbar ist, herangezogen, anhand dessen das Vorgehen einmal methodisch durchlaufen wird. Der Betreiber des Webdienstes stellt noch weitere Dienste bereit; da diese jedoch nicht durch FIM zugreifbar sind, sind diese nicht Teil des hier skizzierten Vorgehens. Des Weiteren ist gemäß [GGF17b] zu berücksichtigen, dass nur derjenige Teil des Dienstes zu analysieren ist, der durch das Konzept von FIM zugreifbar ist und nicht zwangsweise alle damit verbundenen Transaktionen bzw. Geschäftsprozesse. Da in diesem Fall alle Bereiche des Ablage-Webdienstes durch FIM zugreifbar sind und keine isolierten Teilbereiche existieren, ist der Webdienst bzw. die involvierten Assets daher vollständig zu betrachten.

In diesem Anwendungsbeispiel ist der Zweck des Wikis das Hochladen, Speichern sowie die Dokumentation und Anzeige von forschungsprojektbezogenen Daten bzw. Ergebnissen, die vor unberechtigtem Zugriff zu schützen sind. Gemäß OSCRP handelt es sich somit um *Da-*

ta Assets,[1] wobei nicht alle Unterkategorien gemäß der OSCRP Data Assets zwangsweise dasselbe Authentication-Assurance-Profil benötigen. Im Folgenden werden einige dieser Kategorien, die in Wikis verarbeitet bzw. gespeichert werden, aufgegriffen und anhand der abgeleiteten NIST-Schadenskategorien diskutiert.

Die der OSCRP Data Assets untergeordnete Kategorie *Public Data*, bezeichnet dabei alle Daten, wie z.B. *Open Science Data*, die nicht sensibel sind, sodass aufgrund ihrer Klassifikation kein Schaden beim Zugriff durch Dritte zu erwarten ist. Dazu zählen bspw. Forschungsergebnisse wie die des GÉANT-Projekts, die aufgrund der Förderung durch die Europäische Kommission ohnehin zu veröffentlichen sind. Assets dieser Unterkategorie benötigen folglich keine Authentication Assurance (d.h. keine Benutzerauthentifizierung) und lassen sich im öffentlichen bzw. dem nicht durch eine Authentifizierung geschützten Bereich des Wikis ablegen.

Wie oben bereits erwähnt, dienen Wikis zur Dokumentation, für die das OSCRP Asset-Klassifikationsschema die der Data Assets untergeordnete Kategorie *Documentation* vorsieht. Gemäß OSCRP gehören zur Projektdokumentation informative Daten, wie Blogs oder Anleitungen, die auch andere Asset-Kategorien unterstützen können. In Bezug auf Anleitungen können das z.B. Installations- und Konfigurationsanleitungen für Assets des Typs *Software* (*OSCRP Software Assets*) sein. Während Anleitungen für Endnutzer, z.B. für Forschende zum Aufsetzen eines SAML IDPs, aufgrund des nicht vorhandenen Schadenspotentials eher keine Authentication Assurance benötigen, sollten Anleitungen, die die (interne) Infrastruktur betreffen, mindestens eine geringe Authentication Assurance (z.B. SFA-Profil) erfordern, da hier ein unberechtigter Zugriff auf die Dokumentation gemäß der abgeleiteten Schadenskategorien von NIST v.a. Schaden in der Kategorie *Harm to assets and operations* verursachen kann.

Möglicherweise werden, im Gegensatz zu den oben erläuterten *Public Data*, auch *Non-Public Data* im skizzierten Dienst abgelegt. OSCRP listet hier bspw. Rohdaten von Instrumenten oder Daten die nicht veröffentlicht werden können bzw. noch nicht veröffentlicht wurden, auf. Zu diesem Zweck geht OSCRP noch einen weiteren Schritt in die Tiefe und nennt neben der Kategorie *Embargoed Data*[2] u.a. auch die Kategorie *Regulated Data*. Regulierte Daten sind z.B. Gesundheitsinformationen oder PII, deren Preisgabe strafrechtliche Folgen (vgl. v.a. Schadenskategorien *Legal violations* und *Unauthorized release of sensitive information*) nach sich zieht. Regulierte Daten sind daher besonders schützenswert und benötigen aufgrund des erwartbar hohen Schadens in den genannten Schadenskategorien eine starke Authentication Assurance. Wie in Abschnitt 5.3 bereits betrachtet, beschäftigt sich ELIXIR als auch NIH mit derartigen Daten und erfordern in diesem Zusammenhang die Verwendung einer Multi-Faktor-Authentifizierung für bestimmte Dienste.

Anhand der methodischen Anwendung wurde deutlich, dass selbst bei relativ trivialen Diensten wie Wikis, die im Organisationskontext häufig implementiert werden, kein allgemeingültiges Authentication-Assurance-Profil festgelegt werden kann, da die mit dem Dienst ver-

[1] Je nach Nutzung können auch andere Kategorien involviert sein, die an dieser Stelle nicht näher betrachtet werden.

[2] Gemäß OSRCP handelt es sich hierbei, zu einem bestimmten Zeitpunkt, um *gesperrte Daten*, die ggf. zu einem späteren Zeitpunkt veröffentlicht werden können.

bundenen Assets, aufgrund deren potentiellen Schaden stets einer individuellen Bewertung bedürfen. Der risikobasierte Ansatz, der in Abbildung 5.18 visualisiert wird, zeigt, wie Assets anhand des OSCRP Asset-Klassifikationsschemas effektiv identifiziert und anhand der Schadenskategorien abgeleitet von NIST auf ein passendes Authentication-Assurance-Profil abgebildet werden können. Der in Abbildung 5.18 skizzierte *Risk Decision Path* sowie die *Families of related services*, die in Folgearbeiten weiter zu konkretisieren sind, können zukünftig zwar als hilfreiche Unterstützung und Orientierungspunkt herangezogen werden, ersetzen aber nie das Durchführen einer eigenen Bewertung unter Berücksichtigung der involvierten Asset- und Schadenskategorien.

Da der Hauptanforderung RM keine Sub-Anforderungen zugrunde liegen (vgl. Abschnitt 2.6.3) beschäftigt sich der nachfolgende Abschnitt direkt mit der prototypischen Implementierung des MFA-Workflows.

6.3 Prototypische Implementierung des MFA-Workflows

Dieser Abschnitt hat das Ziel, anhand eines *Proof of Concepts* die technische Umsetzbarkeit des in Abschnitt 5.4 spezifizierten Fallback MFA-Workflows zu überprüfen. Dabei wird auch die technische Anwendbarkeit des Authentication-Assurance-Konzepts, d.h. die Kommunikation mittels URIs und den in Abschnitt 5.4 vorgeschlagenen Erweiterungen getestet. Damit dies überprüft werden kann, wird eine Testumgebung mit mehreren SAML IDPs und SAML SPs aufgebaut, sodass anhand derer ein Föderationskonstrukt simuliert werden kann.[3] Insgesamt wird eine Testumgebung benötigt, die der realen Situation einer vollvermaschten Identitätsföderationen möglichst nahe kommt, sodass eine Evaluation auf Basis einer wahrheitsgetreuen Nachbildung des Ecosystems stattfinden kann. Um dies zu unterstützen, werden auch die in R&E meistgenutzten Open Source Software-Implementierungen herangezogen. Zugleich muss die Testumgebung flexibel, leicht veränderbar und anpassbar sein, sodass SAML IDPs und SAML SPs einfach hinzugefügt bzw. entfernt werden können. Um dies zu ermöglichen, werden organisatorische Prozesse im Rahmen der Testumgebung nicht nachgebildet und werden folglich abstrahiert. Um die Testumgebung nicht unnötig komplex zu gestalten, werden z.T. auch technische Komponenten, die keinen oder nur wenig Einfluss auf die zu testenden Komponenten besitzen, abstrahiert. Dazu zählt bspw. die Implementierung einer Managementoberfläche zur Metadatenverwaltung, anhand derer Föderationsbetreiber die Metadaten ihrer Teilnehmer verwalten. Das Hinzufügen von Metadateninformationen von Entitäten zur Föderation findet in der Testumgebung folglich nicht über eine Managementoberfläche, sondern stattdessen bedarfsbasiert, entweder manuell oder anhand automatisierter Skripte statt. Ferner werden selbstsignierte Zertifikate verwendet.

Die Testumgebung basiert auf Vorarbeiten und Ergebnissen einer Bachelorarbeit [Zac19], die u.a. eine Anleitung zum Aufsetzen einer SAML-basierten Testumgebung bereitstellt. Zugleich werden die dort verwendeten Maschinen und Deployments z.T. in der hier beschriebenen Testumgebung wiederverwendet. Um den in Abschnitt 5.4 spezifizierten MFA-Workflow nachzubilden und zu evaluieren, wird die Testumgebung entsprechend erweitert.

[3] Die Übertragbarkeit auf OIDC wird in Abschnitt 6.3.3 diskutiert.

Dazu zählt z.B. der Einsatz einer containerbasierten Lösung, sodass mehrere SAML IDPs bzw. SPs auf einer Virtuellen Maschine (VM) bereitgestellt werden können. Ferner wird neben der Shibboleth-Software, wie in [Zac19] beschrieben, auch die Open Source Software SimpleSAMLphp verwendet (vgl. Abschnitt 3.2.3.2), die ebenfalls eine IDP- und SP-Implementierung bereitstellt. Während die Shibboleth-Distribution (vgl. Abschnitt 3.2.3.1) hier zwischen Identity Providern und Service Providern unterscheidet, besitzt SimpleSAMLphp einen einzigen, gemeinsamen Software-Stack für sowohl Identity Provider und Service Provider. Hier muss während der Konfiguration in der Konfigurationsdatei (config.php) lediglich angegeben werden, ob es sich um einen IDP ('enable.saml20-idp' => true) oder einen SP handelt.

Zusätzlich wird ein Lokalisierungsdienst bzw. Discovery Service benötigt, anhand dessen Benutzer zum SAML IDP ihrer Heimatorganisation weitergeleitet werden. Dieser stellt gemäß der Konzeption (vgl. Abschnitt 4.4 und Abbildung 4.7) ebenfalls eine elementare Komponente dar. Dazu wird die WAYF[4]-Implementierung des tschechischen NRENs CESNET [CES19, CES21] herangezogen.

Der WAYF-Dienst wird synonym auch als Discovery Service (DS) bezeichnet, obwohl die Bezeichnung des Discovery Services ursprünglich aus der SAML-Spezifikation zur Implementierung eines DS-Protokolls stammt. WAYF und DS werden im Rahmen dieser Arbeit jedoch synonym verwendet, obwohl das DS-Protokoll im Vergleich zu WAYF feine Unterschiede aufweist. [SWI21b]

6.3.1 Aggregierte Sicht auf die Testumgebung

Nachdem die erforderlichen, technischen Komponenten erläutert wurden, wird in diesem Abschnitt ein Teil der Testumgebung skizziert. Wie oben bereits beschrieben, liegt die dedizierte Software auf den VMs in jeweils abgeschotteten Containern vor. Abbildung 6.2 zeigt daher einen Auszug gleichzeitig aktiver Container zur Repräsentation einer kleinen vollvermaschten Föderation.[5] Diese sind für den PoC zunächst ausreichend. Im Folgenden werden die Zusammenhänge in Abbildung 6.2 kurz erläutert: In der Mitte des Setups in Abbildung 6.2 befindet sich innerhalb eines Containers der zuvor beschriebene CESNET WAYF (vgl. „Lokalisierungsdienst“ in der Abbildung). Damit dieser die Benutzer entsprechend routen kann, benötigt er die (Föderations-) Metadaten aller Entitäten, d.h. sowohl die Metadaten der IDPs, des TPPs als auch der SPs, welche in der abgebildeten Metadatendatei vorliegen. CESNET WAYF transformiert die Metadaten der IDPs und des TPPs dann in einen sogenannten *JSON Feed*, aus dem die Auswahlliste für Benutzer entsteht.[6] Das Listing 6.1 zeigt exemplarisch die Darstellung des resultierenden JSON Feeds der Testumgebung.[7]

[4] Where Are You From

[5] Die Tatsache, dass die Entitäten vollvermascht sind, lässt sich daran erkennen, dass alle IDPs und SPs in einer zentralen Metadatendatei registriert sind und somit jede Entität die anderen Entitäten „kennt“. Im Vergleich, bei proxy-basierten Architekturen benötigen IDPs und SPs nur die Metadaten des Proxies, wohingegen der Proxy die Metadaten aller IDPs und SPs innehält.

[6] SP-Metadaten müssen nicht transformiert werden, da diese nicht in der Auswahlliste angezeigt werden.

[7] IDPs, die MFA unterstützen, können aus Listing 6.1 nicht direkt ausgelesen werden, da gemäß Abschnitt 4.4.3 ein IDP-seitiges Flag zur Realisierung des MFA-Workflows nicht zwangsweise benötigt wird.

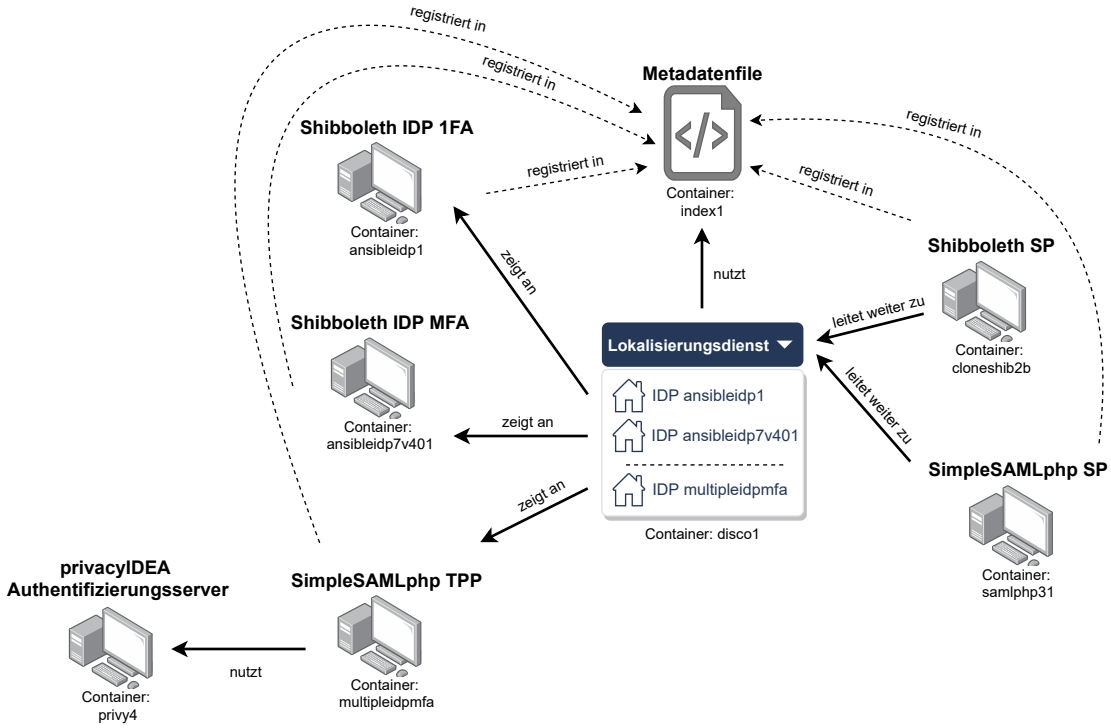


Abbildung 6.2: Auszug aus dem Setup einer Testumgebung

```
{
   "entities" : {
      "https://ansibleidp7v401.shib2.test/idp/shibboleth":{
         "label" : {...},
         "logo" : ...
      },
      "https://multipleidpmfa.shib2.test/simplesamlphp/saml2/idp/metadata.php
    ":{
         "EC" : [
            "https://refeds.org/profile/sfa-tpponly"
         ],
         "logo" : ...,
         "label" : {...}
      },
      "https://ansibleidp1.shib3.test/idp/shibboleth":{
         "label" : {...},
         "logo" : ...
      }
   },
   "label" : "index1shib2",
   "id" : "https://index1.shib2.test/metadata/federation-metadata.xml"
}
```

Listing 6.1: Resultierender CESNET WAYF [CES19, CES21] JSON Feed der Testumgebung

Die Namen der in Abbildung 6.2 gezeigten Container ergeben sich meist aus der verwendeten Software. Bspw. deutet „samlphp“ auf die Verwendung der SimpleSAMLphp-Software hin, wohingegen „ansibleidp“ aus einer Shibboleth-Implementierung in Kombination mit Ansible-Playbook abgeleitet ist. Die darauffolgende Zahlen- bzw. Buchstabenkombination ergibt sich entweder aus der verwendeten Version und/oder dem Klonen von Containern.

Auf der rechten Seite der Abbildung 6.2 ist ein Auszug der SAML SPs der Testumgebung abgebildet. In Abschnitt 6.3.2 wird nachfolgend aufgezeigt, wie unter Verwendung des SimpleSAMLphp SPs der MFA-Workflow realisiert wird.

Auf der linken Seite der Abbildung 6.2 ist ein Auszug der SAML IDPs bzw. TPPs der Testumgebung abgebildet. Diese besitzen die folgende Funktionalität:

- Shibboleth IDP 1FA (Container: ansibleidp1) unterstützt lediglich Ein-Faktor-Authentifizierungen, d.h. eine Kombination aus Benutzername und Passwort.
- Shibboleth IDP MFA (Container: ansibleidp7v401) stellt IDP-seitige MFA-Funktionalität zur Verfügung. D.h. auf eine MFA-Anfrage eines SPs kann der IDP direkt mit MFA im Authentifizierungskontext antworten.
- SimpleSAMLphp TPP (Container: multipleidpmfa) repräsentiert einen externen Zweitfaktor-Prüfer, der nur Authentifizierungen von Zweitfaktoren vornimmt. Der TPP greift dazu auf einen, in einem dedizierten Container liegenden, privacyIDEA-Server zu. Durch die von privacyIDEA bereitgestellte Managementoberfläche kann der Zweitfaktor an einen Benutzer gebunden werden (in der Testumgebung: zeitbasiertes OTP, d.h. TOTP).

Im nächsten Abschnitt wird unter Verwendung der skizzierten Software-Komponenten aufgezeigt, wie der MFA-Workflow mithilfe eines Moduls für SimpleSAMLphp in der Testumgebung realisiert wird.

6.3.2 Realisierung des MFA-Workflows mit SimpleSAMLphp

Der in Abschnitt 5.4 skizzierte MFA-Workflow unter Verwendung eines externen Faktorprüfers (TPP) zeigt, dass in diesem Workflow die SP-Softwarekomponente die aktiv triggernde Komponente darstellt, da diese nach einer nicht stattgefundenen Multi-Faktor-Authentifizierung eine weitere Authentifizierungsanfrage an einen durch den Benutzer ausgewählten TPP sendet. Zur Unterstützung des spezifizierten MFA-Workflows muss folglich die SP-Softwarekomponente erweitert werden. Da in der Testumgebung die Open Source Softwareprodukte eingesetzt werden, die hauptsächlich auch in den Szenarien nationales FIM und Inter-FIM des Kapitels 2 Anwendung finden, lassen sich diese beliebig erweitern. Inwiefern proprietäre SP-Softwareprodukte den Workflow unterstützen, gilt es in Folgearbeiten zu untersuchen.

Im Rahmen dieses Abschnitts wird prototypisch ein SimpleSAMLphp SP erweitert. Da SSP aufgrund der neu spezifizierten Architektur einen derartigen Workflow nicht out-of-the-box unterstützt, wird im Folgenden getestet, ob der in Abschnitt 5.4 erarbeitete MFA-Workflow technisch mit SSP umsetzbar ist. SSP basiert auf einem modularen Ansatz und bietet den

Vorteil, dass verschiedene Authentifizierungsmechanismen anhand von Third-Party Modulen implementiert werden können. Neben den von SSP auf der Webseite bereitgestellten Modulen[8] [Uni21] können in SSP somit auch eigene Module zur Authentifizierung definiert werden. Neue Module werden dann in dem Ordner `/simplesamlphp/modules` abgelegt. Die Subdirectories und Files müssen einer bestimmten Konvention entsprechen, damit diese später gefunden und geladen werden können. Während Module früher mit einer anderen Syntax entwickelt wurden, die zum direkten Laden des Moduls geführt haben, werden Module inzwischen mit PSR-4 [Pau21] entwickelt, die einen Composer (PHP Dependency Manager) zum Laden benötigen.

Zur Realisierung des MFA-Workflows wird somit für den SimpleSAMLphp SP ein neues Authentifizierungsmodul benötigt. Dazu wird ein Grundgerüst von [Góm20] herangezogen, das entsprechend erweitert wird. Die Konfiguration des Grundgerüsts basiert dabei auf zwei sogenannten „Authentifizierungsquellen“, die bei Bedarf hintereinander aufgerufen werden, sodass im Falle, sofern ein IDP kein MFA liefert, eine weitere Authentifizierungsanfrage an einen TPP angestoßen werden kann.

Das Listing 6.2, das einen Teil der SP-seitigen Konfiguration in `authsources.php` darstellt, zeigt die zwei Authentifizierungsquellen (hier: `sources`), die jeweils mit den Namen `ssp-a` und `ssp-b` versehen sind. Grundsätzlich könnten hier auch beliebig viele Authentifizierungsquellen hintereinander kontaktiert werden, um bspw. MFA unter Verwendung von drei Faktoren bzw. Faktorprüfern zu realisieren, jedoch sind zur Veranschaulichung des MFA-Workflows zunächst zwei Quellen ausreichend. Die zweite Quelle kontaktiert einen TPP jedoch nur dann, wenn die erste Quelle nicht mit MFA im Authentifizierungskontext geantwortet hat (s.u. Listing 6.5).

```
1 $config['multissp'] = [AuthMultiSP::class,
2   'sources' => [
3     ['name' => 'ssp-a', 'uid' => 'uid'],
4     ['name' => 'ssp-b', 'uid' => 'samlLoginName'],
5   ]
6 ];
```

Listing 6.2: Konfiguration des SimpleSAMLphp SPs gemäß [Góm20]

Die Listings 6.3 und 6.4 zeigen jeweils die Konfiguration des `ssp-a` und `ssp-b`. Sowohl `ssp-a` und `ssp-b` besitzen jeweils eine eigene `entityID` und folglich auch eigene Metadaten. Sie können daher als zwei SPs innerhalb der selben Installation angesehen werden. Ein Nachteil dieses Vorgehens ist, dass jede entityID, sofern der damit assoziierte SP in einer (Inter-) Föderation teilnehmen soll, in der zentralen Metadatendatei zu registrieren ist, was zu einem Wachstum der Metadatendatei führt. In [Héd21] wurde hierzu ein Experiment durchgeführt, um zu testen, welche Metadatendatei-Größen die in R&E gängigen SAML-Implementierungen handhaben können. Es wurden Test-Metadatendateien mit 10-, 15-, 30-, 50- und 100-tausend Entitäten generiert.[9] Das Ergebnis der Shibboleth- und

[8] Anhand von Modulen können neben Authentifizierungsmechanismen auch Filter, Themes oder neue Protokolle unterstützt werden.

[9] Zum Vergleich, Ende 2021 sind in eduGAIN circa 8100 Entitäten registriert [GÉ21b].

SimpleSAMLphp-Software gemäß [Héd21] zeigte, dass bei hunderttausend Entitäten, aufgrund des exponentiell anwachsenden Speicherverbrauchs, keine Verarbeitung mehr durchgeführt werden konnte. Somit kann die Registrierung weiterer TPPs, bezüglich der durch die Software verarbeitbare Menge, als vernachlässigbar angesehen werden.

```
1  $config['ssp-a'] = array('saml:SP',
2  'entityID' => null,
3  'idp' => null,
4  'privatekey' => ...,
5  'certificate' => ...,
6  'discoURL' => 'http://disco1.shib2.test/wayf/wayf.php',
7  'AuthnContextClassRef' => array(
8   'https://refeds.org/profile/mfa',
9   'urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport',
10  ),
11 );
```

Listing 6.3: Konfiguration ssp-a

```
1  $config['ssp-b'] = array('saml:SP',
2   'entityID' => null,
3   'idp' => null,
4   'privatekey' => ...,
5   'certificate' => ...,
6   'discoURL' => 'http://disco1.shib2.test/wayf/wayf.php?filter=eyJ2ZXIiOiIy
7    IiwiYWxsb3dGZWVkcyI6eyJpbmRleDFzaGliMiI6eyJhbGxvd0VDIjpbImh0dHBzOi8vcmVmZ
8    WRzLm9yZy9wcm9maWxlL3NmYS10cHBvbmx5Il19fX0=',
9   'AuthnContextClassRef' => array(
10   'https://refeds.org/profile/sfaTotp',
11   ),
12 );
```

Listing 6.4: Konfiguration ssp-b

Der `ssp-a` triggert somit, gemäß Abbildung 4.7, die erste Authentifizierungsanfrage an den IDP eines Benutzers. Davor wird ein Benutzer noch über den Discovery Service zur Auswahl seines IDPs geleitet. Das Listing 6.3 zeigt hierzu die entsprechende `discoURL`, über die der Discovery Service kontaktiert wird.

Sowohl die SAML- als auch die OIDC-Spezifikation erlauben die Angabe mehrerer Authentifizierungskontexte in der Authentifizierungsanfrage. Aus diesem Grund wird in den Zeilen 7 bis 9 in Listing 6.4 exemplarisch sowohl `https://refeds.org/profile/mfa` als auch `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` angefragt. Liefert der kontaktierte IDP bereits MFA, wie es bspw. bei dem Shibboleth IDP MFA (Container: ansibleidp7v401) aus dem Auszug der Testumgebung in Abbildung 6.2 der Fall wäre, wird der Fallback MFA-Workflow unter Verwendung eines TPPs nicht initiiert und die Authentifizierungsanfrage des `ssp-a` genügt. Kann der kontaktierte IDP kein MFA liefern (vgl. Shibboleth IDP 1FA der Testumgebung), akzeptiert die Konfiguration des `ssp-a` auch eine Ein-Faktor-Authentifizierung, wobei hier exemplarisch `PasswordProtectedTransport` angegeben wurde.[10] Der Betreiber eines IDPs muss somit zur Realisierung des MFA-Workflows

[10]Wie sich später in [REF21] zeigt, kann die Liste an Authentifizierungskontexten in der SAML Request

keine Anpassungen an seiner SAML-Implementierung vornehmen. Auf lange Sicht ist jedoch die Implementierung der Maßnahmen zur Authentication Assurance (vgl. Abschnitte 5.2.1 und 5.4) und das Antworten mit dem Authentifizierungskontext `https://refeds.org/profile/sfaMemorizedSecret` anstelle von `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` anzustreben. Aufgrund des IDP-seitigen Fehlens des MFA-Authentifizierungskontextes triggert der `ssp-b` eine weitere Authentifizierungsanfrage (vgl. Abbildung 4.7). Zur dynamischen Auswahl eines TPPs wird ein Benutzer dann erneut über den Discovery Service geleitet. Da in der zentralen Metadatendatei alle Entitäten registriert sind und in der Benutzerauswahl des Discovery Services nur TPPs (und keine IDPs) angezeigt werden sollen, wird anhand des in Abschnitt 4.4.3 beschriebenen Flags gefiltert. Das Flag, hier mittels der Entity Category (EC) `https://refeds.org/profile/sfa-tpponly` realisiert, ist in Listing 6.1 bei dem TPP (Container: multipleidpmfa) ersichtlich. CESNET WAYF, der in der Testumgebung verwendet wird, unterstützt die Filter-Funktion (vgl. `filterEntities()` aus Abschnitt 4.4.3) bereits out-of-the-box und stellt dazu einen Filtergenerator bereit. Hierbei handelt es sich um einen base64-kodierten String, der der `discoURL` angehängt wird. Die Zeilen 6 bis 8 in Listing 6.4 zeigen die korrespondierende `discoURL` des `ssp-b`. Als Authentifizierungskontext wurde hier exemplarisch `https://refeds.org/profile/sfaTotp` angefragt.

Nachdem nun sequenziell die Authentifizierungsanfragen durch `ssp-a` und `ssp-b` angestoßen wurden und der Benutzer den gesamten Workflow durchlaufen hat, werden die eingegangenen Authentifizierungsantworten durch die SP-Installation in `AuthorizeController.php` überprüft. Hier ist zum einen definiert (vgl. Listing 6.5), ob die zweite Authentifizierungsquelle `ssp-b` benötigt wird oder nicht.

```
1  // if MFA sent by ssp-a then done
2  if(($authnContext[$sourceName] == "https://refeds.org/profile/mfa") &&
       $sourceName == "ssp-a"){
3
4      \SimpleSAML\Auth\Source::completeAuth($state);
5
6      throw new \SimpleSAML\Error\AuthSource('Auth Source not completed');
7  }
```

Listing 6.5: Auszug aus der Datei `AuthorizeController.php`

Ferner wird in `AuthorizeController.php` überprüft, sofern Authentifizierungsanfragen durch sowohl `ssp-a` und `ssp-b` angestoßen wurden, ob die Kombination der erhaltenen Authentifizierungskontexte einer validen Multi-Faktor-Authentifizierung entsprechen (vgl. Abschnitt 3.4.3). Darüber hinaus werden die zwischen IDP und TPP ausgetauschten UserIDs (vgl.

nicht zuverlässig zur Priorisierung, i.S.v. „Ein SP bevorzugt aber erfordert kein MFA“, verwendet werden. Dadurch könnte es evtl. passieren, dass, auch wenn ein IDP MFA unterstützt, der Nutzer zur Ein-Faktor-Authentifizierung weitergeleitet wird, um bspw. den Workflow für einen Nutzer vermeintlich „abzukürzen“. Dies hätte zur Folge, dass die zweite Authentifizierungsquelle `ssp-b` angestoßen wird, obwohl der IDP, der durch `ssp-a` kontaktiert wurde, selbst in der Lage wäre MFA durchzuführen. Alternativ könnte bei der SSP SP-Implementierung bei `ssp-a` nur der MFA Authentifizierungskontext angegeben werden, wobei anhand eines sog. *Authentication Processing Filters* [Uni21] jedoch mehr Authentifizierungskontexte akzeptiert werden, als tatsächlich angefragt wurden. Dieses Vorgehen wurde allerdings in der Testumgebung nicht mehr getestet.

Abschnitt 4.4.4) gegeneinander abgeglichen, um zu überprüfen, ob es sich um denselben Benutzer handelt. Das Listing 6.2 zeigt, dass in der Testumgebung hierzu exemplarisch die *uid* und der *samlLoginName* herangezogen wurden.

Im nachfolgenden Abschnitt findet unter Einbezug der Anforderungen aus Abschnitt 2.6.4 eine Diskussion und Bewertung des prototypisch implementierten MFA-Workflows statt.

6.3.3 Diskussion und Bewertung

Im vorherigen Abschnitt wurde die technische Realisierbarkeit des MFA-Workflows unter Verwendung der SSP-Software anhand eines neuen Authentifizierungsmoduls prototypisch demonstriert. Der PoC basiert dabei auf dem in Abschnitt 3.2.2.1 beschriebenen Protokoll SAML, da dies zum Entstehungszeitpunkt der Dissertation den State-of-the-Art in R&E Föderationen darstellt. Da jedoch zunehmend auf OIDC basierende Service Provider in R&E Föderationen eingegliedert werden, gewinnt auch OIDC in R&E zunehmend an Wichtigkeit. Dies zeigt sich bspw. durch die Entwicklung von Proxies wie SATOSA [Ide21], die ein Mapping zwischen verschiedenen Authentifizierungsprotokollen (insbesondere SAML, OIDC und OAuth) vornehmen. Auch der in Abschnitt 3.2.2.3 referenzierte IETF Draft zu OIDC-Föderationen verdeutlicht das Eintreffen des OIDC-Protokolls in R&E. Da in der Testumgebung die Anwendbarkeit des Moduls in OIDC nicht getestet wurde, wird an dieser Stelle ein Teil der in SAML zur Realisierung des MFA-Workflows verwendeten Aspekte aufgegriffen und auf theoretischer Basis diskutiert, inwieweit diese in OIDC vorhanden bzw. umsetzbar sind. Hierbei zeigt sich, dass bspw. der durch die SAML-Spezifikation definierte Authentifizierungskontext (AuthnContextClassRef) zur Kommunikation der SFA- und MFA-Profile analog auch in OIDC vorhanden ist (vgl. Abschnitt 4.2.4). In OIDC wird dieser als acr claim bezeichnet, wobei „acr“ für Authentication Context Class Reference steht. Dieser kann als optionaler Parameter innerhalb des ID Tokens angegeben werden und sollte einer absoluten URI oder einem gemäß des RFC 6711 [Joh12] registrierten Namens entsprechen [SBJ+14b]. Die grundsätzliche Fähigkeit zur Kommunikation der in Abschnitt 6.2 evaluierten Authentifizierungsprofile ist also gemäß der OIDC-Spezifikation auf SAML-ähnliche Art und Weise gegeben. Ob jedoch implementierungsspezifische Einschränkungen, wie bspw. beim Setzen eines individuellen Authentifizierungskontexts in ADFS[11] bestehen (vgl. [ZSL19, REF18b]), kann an dieser Stelle nicht allgemeingültig beantwortet bzw. beurteilt werden.

Da OIDC in verschiedenen Punkten, wie bspw. hinsichtlich der Signierung, einfacher gehalten ist als SAML, lässt sich die OIDC-Funktionalität oftmals schon anhand von Libraries umsetzen und benötigt nicht zwangsweise eigenständig lauffähige Software. So gibt es bspw. für Apache Server ein Modul zur Unterstützung der RP-Funktionalität (libapache2-mod-auth-openidc [Oro21]). Ob derartige, vorhandene Libraries bzw. Module zur Unterstützung des MFA-Workflows erweitert werden können, gilt es in Folgearbeiten zu untersuchen. Insgesamt zeigt sich jedoch, auch hinsichtlich der SAML-Softwarekomponenten, dass die Fähigkeit zur Unterstützung des MFA-Workflows von der verwendeten Software bzw. Library abhängig ist.

[11] Das schwedische NREN SUNET [SUN22] arbeitet, zum Zeitpunkt des Entstehens dieses Abschnitts, an einer Lösung.

In Bezug auf die Discovery, die im MFA-Workflow zur Präsentation und dynamischen Auswahl eines TPPs verwendet wird, stellt bspw. das o.g. Apache RP-Modul, ähnlich zur SAML Discovery, ebenfalls eine interne Discovery-Seite zur Auswahl eines OIDC OPs durch den Benutzer bereit. Die OIDC-Discovery-Spezifikation definiert jedoch an dieser Stelle verschiedene Wege, um die Location eines OPs herauszufinden [SBJJ14]. Dazu zählt bspw. u.a. die Eingabe durch den Benutzer anhand einer E-Mail-Adresse oder einer URL. Daraus lässt sich folgern, dass in OIDC, im Gegensatz zu SAML, je nach Realisierung der Discovery von der Implementierung eines Filters, der die TPP-Auswahlliste einschränkt, abstrahiert werden kann.

Nachdem wesentliche Aspekte des MFA-Workflows in Bezug auf OIDC diskutiert wurden, werden als nächstes die Anforderungen aus Abschnitt 2.6.4 erneut aufgegriffen, wobei anhand der prototypischen SAML-Implementierung überprüft wird, inwiefern diese erfüllt werden. Dazu werden zuerst die Anforderungen, die als *essentiell* priorisiert wurden, betrachtet, da die Erfüllung dieser Anforderungen als elementar gilt. Diese sind:

- [NFA_Integrierbarkeit]
- [FA_Koexistenz]
- [NFA_Einrichtungsaufwand]

Die erste aufgelistete Anforderung, [NFA_Integrierbarkeit], bezieht sich hierbei auf die Notwendigkeit, dass der spezifizierte MFA-Workflow mit verschiedenen Föderationsarchitekturen kompatibel sein muss und keine grundlegenden Änderungen an der vorhandenen (Inter-) Föderationsarchitektur nach sich ziehen soll. In Abschnitt 3.2.4 wurden dazu die drei zentralen Architekturmuster zusammengefasst,[12] wobei bereits in Abschnitt 2.2 gezeigt wurde, dass in H&S Architekturen, d.h. proxy-basierten Architekturen, MFA relativ einfach am zentralen Proxy für die daran angeschlossenen Entitäten implementiert werden kann (vgl. Abbildung 2.4). D.h. obwohl der MFA-Workflow mit Blick auf vollvermaschte Föderationsarchitekturen spezifiziert wurde,[13] darf dieser nichtsdestotrotz nicht konfliktär zu den anderen Architekturmustern stehen, da bspw. in dem Szenario Inter-FIM aus Kapitel 2 verschiedene Föderationen (mit unterschiedlichen Architekturmustern) anhand eines vollvermaschten Prinzips verknüpft wurden. Bei der Analyse des MFA-Ansatzes mit Proxy zwischen IDP und SP zeigte sich zwar, dass dieser rein technisch auch in vollvermaschten Szenarien realisierbar wäre, dies jedoch dem vollvermaschten Prinzip widersprechen würde, weswegen die Integrierbarkeit des Ansatzes, als nicht erfüllt bewertet wurde. Im Gegensatz dazu erfüllt der hier spezifizierte MFA-Workflow die Anforderung, da er keine Änderungen am Grundsatz der Föderationsarchitektur erfordert. Auch wenn dies nicht explizit in der Testumgebung getestet wurde, könnte bspw. der SP 1 der nationalen Föderation A aus Abbildung 4.4 die Erweiterung zur Realisierung des MFA-Workflows implementieren. Somit könnte z.B. der IDP 1 der Föderation A, unter der Annahme, dass dieser kein MFA bereitstellt, nach wie vor die proxy-basierte MFA-Lösung zum Zugriff auf SP 1 nutzen. Der Workflow wäre dann:

[12] Diese sind: Vollvermaschte Architektur, H&S Architektur mit verteiltem Login und H&S Architektur mit zentralisiertem Login

[13] Da für vollvermaschte Architekturen ein geeigneter Fallback MFA-Workflow, nach ausführlicher Recherche, noch nicht existiert.

SP 1 → IDP-SP-Proxy → IDP 1 → IDP-SP-Proxy → MFA → IDP-SP-Proxy → SP 1. Da der IDP-SP-Proxy die Antworten zusammenführt und als eine aggregierte Antwort an den SP 1 weiterleitet, würde das in Abschnitt 6.3.2 beschriebene Authentifizierungsmodul nach `ssp-a` stoppen und `ssp-b` würde nicht aufgerufen werden. Zugleich könnten auch nicht MFA-fähige IDPs außerhalb der Föderation A, die nicht an den zentralen IDP-SP-Proxy der Föderation A angeschlossen sind, unter Verwendung eines beliebigen TPPs auf SP 1 zugreifen. Der hier spezifizierte MFA-Workflow funktioniert daher auch mit anderen Architekturmustern, v.a. wenn diese miteinander kombiniert werden. Die Beispiele verdeutlichen auch, dass der spezifizierte MFA-Workflow skalierbar ist (vgl. Anforderung [NFA_Skalierbarkeit]) und sowohl auf Föderations- als auch Interföderationsebene anwendbar ist.

Eng im Zusammenhang mit der Anforderung [NFA_Integrierbarkeit] steht die Anforderung [FA_Koexistenz], die erfordert, dass vorhandene MFA-Lösungen trotz eines spezifizierten Fallback MFA-Workflows nach wie vor nutzbar sein müssen. Dies ist sowohl für die bereits evaluierten MFA-Ansätze der Fall (vgl. Tabelle 6.3), da bspw. der MFA-Workflow unter Verwendung eines Proxies nur dann angestoßen wird, wenn IDP-seitig kein MFA geliefert werden kann. Wie das etwas komplexere Beispiel im vorherigen Abschnitt unter Einbezug der Abbildung 4.4 bereits verdeutlicht hat, erfüllt auch der im Rahmen dieser Arbeit spezifizierte MFA-Workflow diese Anforderung, da der MFA-Workflow unter Verwendung eines externen Faktorprüfers nur dann angestoßen wird, wenn MFA nicht auf eine andere Art und Weise (z.B. IDP-seitig oder durch einen Proxy) geliefert wurde.

Hinsichtlich der Anforderung [NFA_Einrichtungsaufwand] agiert der externe Faktorprüfer, d.h. der TPP, als Service Provider gegenüber dem IDP. Aus Sicht des SPs verhält sich der TPP wiederum als spezialisierter Identity Provider, was zur Erfüllung der wünschenswerten Anforderung [FA_Konformität] führt. Dies vermag den Anschein eines proxybasierten Ansatzes zu erwecken (vgl. Abschnitt 3.5.2), tatsächlich ist hier jedoch eine klare Abgrenzung zu ziehen, da ein IDP (mit Ausnahme des initialen Austausches des User Identifiers, was allerdings, je nach Realisierung, auch durch den Nutzer selbst geschehen kann) im MFA-Workflow eines Benutzers, nie mit einem TPP SAML-Nachrichten austauscht. Ein TPP agiert somit im spezifizierten, technischen MFA-Workflow nicht als zentrale Vermittlungsstelle zwischen IDP und SP (bspw. im Sinne: SP → TPP → IDP → TPP → SP), sondern kann vielmehr als ein weiteres, nicht-zentralisiertes Element einer Authentifizierungskette (d.h. SP → IDP → SP → TPP → SP) interpretiert werden. Der technische, IDP-seitige Einrichtungsaufwand, d.h. die Anpassung der Softwarekomponenten, ist somit, wie man in Abschnitt 6.3.2 gesehen hat, zu vernachlässigen, da auch der bisher vom IDP verwendete Authentifizierungskontext vom MFA-Workflow unterstützt wird. Der technische, SP-seitige Einrichtungs- und Pflegeaufwand wird hingegen als vertretbar eingeschätzt, da die SP-Software um ein entsprechendes Modul zu erweitern ist. Der organisatorische Einrichtungs- und Pflegeaufwand, der im Gegensatz zu technischen Seite, aufgrund der Etablierung verschiedener, notwendiger Verfahren (z.B. Bindung des Authentifizierungsfaktors, Verfahren bei Verlust bzw. Vergessen des Faktors) sehr einrichtungs- und plegeintensiv ist, wird as-a-Service an einen darauf spezialisierten TPP ausgelagert. Im nachfolgenden Abschnitt 6.3.4 werden hierzu noch zwei Anwendungsmodelle diskutiert. Im ersten Anwendungsmodell wird von begrenzt vorhandenen Ressourcen eines IDPs ausgegangen, sodass ein IDP in die Etablierung der Verfahren involviert werden kann. Das zweite Anwendungsmodell hingegen diskutiert einen vollständi-

gen Third Party TPP. Die Anforderung [NFA_Einrichtungsaufwand] zusammenfassend zeigt sich, dass neben der technischen Umsetzung die Herausforderung vielmehr die Etablierung der damit verbundenen Verfahren und Prozesse ist. Die Tabelle 6.3 zeigt daher den möglichst minimalen, technischen IDP-seitigen Einrichtungsaufwand als erfüllt und den SP-seitigen Einrichtungsaufwand als nur teilweise erfüllt.

Im nächsten Schritt werden die als *wichtig* und *wünschenswert* priorisierten, verbleibenden Anforderungen evaluiert. Die als *wichtig* priorisierten Anforderungen sind:

- [NFA_Realisierbarkeit]
- [NFA_Unabhängigkeit]
- [FA_Dynamik]
- [SIA_Faktorprüfung]
- [FA_Benutzbarkeit]
- [DSA_Datenminimalisierung]
- [SIA_Vertraulichkeit]

Als *wünschenswert* sind die folgenden, verbleibenden Anforderungen klassifiziert:

- [FA_Messbarkeit]
- [FA_Fehlerbehandlung]

Die Realisierbarkeit mittels der in R&E genutzten Standard-Software, d.h. Shibboleth und SimpleSAMLphp, wird als erfüllt erachtet. Für SimpleSAMLphp wurde dies anhand der prototypischen Implementierung im vorherigen Abschnitt demonstriert. Obwohl die Shibboleth-Software in der Testumgebung nicht prototypisch erweitert wurde, ist hier jedoch von der Erfüllung der Anforderung aufgrund des Open Source Charakters und der damit verbundenen Fähigkeit zur Erweiterung auszugehen. Inwiefern der MFA-Workflow unter Einsatz von proprietärer SP-Software oder OIDC RP-Libraries (vgl. oben) unterstützt wird, konnte nicht getestet werden und gilt in Folgearbeiten zu untersuchen.

Die Anforderung [NFA_Unabhängigkeit] gilt, analog zu den anderen, in der Tabelle 6.3 aufgelisteten MFA-Ansätzen ebenfalls als erfüllt, da ein Nutzer keinen dedizierten TPP pro SP registrieren muss, sondern einen beliebigen TPP, bei dem bereits ein Zweitfaktor registriert wurde, auswählen kann.

Im Hinblick auf die Anforderung [FA_Dynamik] grenzt sich der spezifizierte MFA-Workflow positiv von dem AA-basierten Ansatz ab. Bei dem AA-basierten Ansatz, bei dem es sich um einen PoC handelt und der, soweit bekannt, nicht operativ im Einsatz ist, sind zum Einen der SAS IDP und SAS SP fest miteinander verdrahtet und zum anderen stellt der MFA-fordernde SP eine Attribute Query nur an die in der Konfiguration angegebene(n) EntityID(s), wodurch keine Auswahl durch den Benutzer möglich ist. Zwar könnte der SAS IDP wiederum verschiedene Authentifizierungsquellen integrieren, jedoch ist ein Benutzer dann an die Verwendung dieses speziellen SAS IDPs und ggf. an die damit verbundenen organisatorischen Verfahren gebunden. Während dies in nationalen Föderationen ein sinnvoller Ansatz sein

kann, stellt dies in einer Interföderation, d.h. wenn ein derartiger Dienst bspw. als globaler eduGAIN Sub-Service betrieben werden würde, v.a. hinsichtlich des Datenschutzes einen Nachteil dar und würde u.U. keine übergreifende Annahme finden. Dadurch dass gemäß der Architektur der MFA-Workflow die Integration beliebig vieler und vollständig verteilter TPPs erlaubt und fördert, besteht hier größtmögliche Flexibilität. Aus diesem Grund findet im spezifizierten MFA-Workflow auch eine explizite Überprüfung der Authentifizierungskontexte statt (vgl. Anforderung [SIA_FAKTORPRÜFUNG]), wohingegen die anderen Ansätze, aufgrund der kontrollierten MFA-Umgebung und der damit verbundenen, begrenzten Auswahlfähigkeit von Zweitfaktoren z.T. darauf verzichten können.

Was die Anforderung [FA_BENUTZBARKEIT] betrifft, werden im spezifizierten MFA-Workflow ausschließlich Ansätze verwendet, die einem Nutzer durch den bereits existierenden Ein-Faktor-Authentifizierungsworkflow bekannt sind. Dazu zählt bspw. die Verwendung eines Discovery-Services zur Auswahl eines TPPs. Beim zweiten Durchlaufen der Discovery wurde die Auswahlliste exemplarisch anhand einer Entity Category, wie in Listing 6.1 ersichtlich wurde, gefiltert, sodass hier nur TPPs und nicht sowohl IDPs und TPPs angezeigt werden. Dies führt zu einer verbesserten Benutzbarkeit. Da einige, als auch die in Abschnitt 6.3.1 skizzierte und in der Testumgebung verwendete DS-Implementierung, die IDP-Auswahl eines Benutzers anhand eines Cookies im Browser speichert, wird beim ersten Durchlaufen der Discovery zwar ein Cookie gesetzt (auf dessen Information innerhalb desselben Browsers zu einem späteren Zeitpunkt zugegriffen werden kann), jedoch wird beim zweiten Durchlaufen zur Auswahl eines TPPs auf die im Cookie gespeicherte IDP-Auswahl nicht zurückgegriffen, da alle IDPs aufgrund des Filters aus der Auswahlliste herausgefiltert wurden. Ein Benutzer bekommt somit stets die korrekten Entitäten angezeigt. Im Zusammenhang mit der Benutzererfahrung auf Basis von Cookies ist auch das Session Management zu betrachten, da nach einer erfolgreichen Benutzerauthentifizierung Cookies mit SessionIDs erzeugt werden, um SSO zu ermöglichen. Im spezifizierten MFA-Workflow werden, in Bezug auf die Benutzerauthentifizierung, insgesamt drei Cookies mit SessionID erzeugt: pro Webserver, d.h. also ein IDP-Cookie, TPP-Cookie sowie SP-Cookie. Beim Auslesen der SP-seitigen PHP-Variable `$_Session` zeigt sich, dass die Sessionvariable die SessionIDs von sowohl IDP (`ssp-a`) und TPP (`ssp-b`) enthält und somit als eine Art Zwischenspeicher agiert. Somit kann, solange die beiden Sessions noch gültig sind, der MFA-Workflow ohne erneute Reauthentifizierung (d.h. ohne Eingabe des Geheimnisses) durchlaufen werden. Anhand der Gültigkeitsdauer von Sessions lassen sich somit verschiedene Anwendungsfälle abdecken, bspw. ob SSO mit MFA erlaubt sein sollte oder nicht. Durch Setzen einer kurzen TPP-Session könnte dies bspw. unterbunden werden. Es ist folglich die richtige Balance zwischen Usability und Security zu finden, was an dieser Stelle jedoch nicht generalisiert entscheidbar bzw. bewertbar ist, sondern vom individuellen Anwendungsfall abhängig ist. Die Anforderung [SIA_VERTRAULICHKEIT] gilt an dieser Stelle ebenfalls als erfüllt, da der TPP als spezialisierter IDP agiert und somit vergleichbare Mechanismen implementiert.

Im Gegensatz zum MFA-Ansatz mit Proxy zwischen IDP und SP gilt die Anforderung [DSA_DATENMINIMALISIERUNG] als erfüllt, da ein TPP in Bezug auf die Benutzerauthentifizierung, nur einen eindeutigen User Identifier benötigt, wohingegen ein MFA-Proxy die Informationen aus den verschiedenen Quellen zusammenführt und als aggregierte Response an einen SP sendet. Die mit der Benutzerauthentifizierung verbundenen, organisatori-

schen Verfahren wurden beim jeweiligen Abgleich nicht mit einbezogen. Hier ist allerdings zu berücksichtigen, dass allein bei der Bindung des Faktors an den Nutzer und der damit verbundenen Identitätsfeststellung eine Vielzahl sensibler Daten verarbeitet und (u.a. zu Audit-Zwecken) gespeichert werden. Um auch hier die Datenverarbeitung und -speicherung durch Dritte zu minimieren, wird im nachfolgenden Abschnitt 6.3.4 ein Vorgehen beschrieben, wie die mit der Benutzerauthentifizierung verbundenen Verfahren in potentiell bereits vorhandene Verfahren eines IDP integriert werden können.

Die Anforderung [FA_Messbarkeit] wird nur teilweise erfüllt. Zwar können IDPs von TPPs aufgrund des EC-Flags voneinander unterschieden werden, jedoch können IDPs, die nur 1FA unterstützen, nicht von MFA-fähigen IDPs differenziert werden. Würden IDPs ebenfalls mit einem entsprechenden Flag (z.B. in den Metadaten) versehen werden, könnte zwar die grundsätzliche Fähigkeit, ob ein IDP MFA unterstützt oder nicht, abgelesen werden, ob MFA aber tatsächlich bei einer Benutzerauthentifizierung durchgeführt wurde, wird erst zur Laufzeit ersichtlich. Zur Messung stattgefundener MFA-Authentifizierungsevents sind folglich weitere Mechanismen zur Messbarkeit und Statistik erforderlich. Die Anforderung [FA_Fehlerbehandlung] gilt als erfüllt, da ein Benutzer nach einer stattgefundenen Ein-Faktor-Authentifizierung aufgrund fehlendem MFA nicht mit einer Fehlermeldung abgewiesen wird, sondern, bspw. indem die Discovery-Seite mit zusätzlicher, textueller Information angereichert wird, auf das Fehlen eines Zweitfaktors und die Option zur Nutzung eines externen Faktorprüfers hingewiesen werden kann.

Nachdem der spezifizierte MFA-Workflow gegen die Anforderungen abgeglichen wurde, gibt Tabelle 6.3 einen Überblick über die Erfüllung der Anforderungen und stellt diese den bereits evaluierten MFA-Ansätzen gegenüber.

Zusammenfassend zeigt sich, das keiner der MFA-Workflows alle Anforderungen vollständig erfüllt. Während der technische Einrichtungsaufwand bei einem MFA-Ansatz mit Proxy zwischen IDP und SP vermutlich größtenteils beim Infrastruktur- bzw. Föderationsbetreiber liegt, wird im Falle des AA-basierten MFA-Ansatzes sowie beim, in dieser Dissertation spezifizierten MFA-Workflow, mehr auf die SP-Seite verlagert. Abschließend zeigt sich, dass es keine Lösung gibt, die alle Anwendungsfälle perfekt abdeckt, sondern dass eine heterogene Authentifizierungslandschaft von verschiedenen Lösungen lebt und profitiert. Der Vorteil des hier spezifizierten MFA-Workflows liegt jedoch klar darin, dass im Gegensatz zu den anderen evaluierten MFA-Ansätzen, dieser keine statische Kombination von Faktorprüfern vorschreibt, sondern eine beliebige Auswahl durch Benutzer ermöglicht.

Tabelle 6.3: Gegenüberstellung und Bewertung des spezifizierten MFA-Workflows

Anforderung	**Gewichtung**	**MFA-Ansatz: Proxy zwischen IDP und SP**	**MFA-Ansatz: AA-basiertes MFA**	**Spezifizierter MFA-Workflow**
[NFA_Integrierbarkeit]	(4)	✗	✓	✓
[FA_Koexistenz]	(4)	✓	✓	✓
[NFA_Einrichtungsaufwand]	(4)	IDP: ✓ SP: ✓	IDP: ✓ SP: (✓)	IDP: ✓ SP: (✓)
[NFA_Realisierbarkeit]	(2)	✓	✓	✓
[NFA_Unabhängigkeit]	(2)	✓	✓	✓
[FA_Dynamik]	(2)	i.a.	✗	✓
[SIA_Faktorprüfung]	(2)	i.a.	✗	✓
[NFA_Skalierbarkeit]	(2)	✓	✓	✓
[FA_Benutzbarkeit]	(2)	✓	(✓)	✓
[DSA_Datenminimalisierung]	(2)	✗	✓	✓
[SIA_Vertraulichkeit]	(2)	✓	✓	✓
[FA_Messbarkeit]	(1)	✓	(✓)	(✓)
[FA_Fehlerbehandlung]	(1)	i.a.	✓	✓
[FA_Konformität]	(1)	✓	✓	✓
$G(p) = \sum w \cdot p$	G(p) max 62	45	49	59

✓: Anforderung erfüllt (2 Punkte)
(✓): Anforderung teilweise erfüllt (1 Punkt)
i.a.: Implementierungsabhängig, daher nicht generalisiert bewertbar (1 Punkt)
✗: Anforderung nicht erfüllt (0 Punkte)

wobei w: Gewichtung, p: Punkte und $G(p)$: Gesamtsumme Punkte

6.3.4 Methodische Anwendung

Auf Basis der prototypischen Implementierung in Abschnitt 6.3.2 werden im folgenden Abschnitt zwei Anwendungsfälle skizziert, die methodisch demonstrieren, wie der in Abschnitt 6.3.2 implementierte MFA-Workflow auf ein reales Szenario übertragen werden kann.

Als Grundlage der ersten methodischen Anwendung dient die vorhandene Infrastruktur und Gegebenheiten der deutschen Föderation DFN-AAI (vgl. auch Abschnitt 2.2). Da die deutsche Föderation zum Zeitpunkt des Entstehens dieser Arbeit ohnehin eine Transition von den DFN Verlässlichkeitsklassen zu den publizierten Assurance-Spezifikationen plant, eignet sich das Anwendungsbeispiel gut zur Veranschaulichung. Neben der Darlegung des MFA-Workflows wird v.a. skizziert, wie eine potentielle, ganzheitliche Anwendung aussehen kann; einschließlich einiger Konzepte zur Identity Assurance, die in den vorherigen Kapiteln stets ausgeklammert wurden. Hier wird ein Anwendungsmodell diskutiert, bei dem ein TPP, neben beliebig vielen anderen TPPs, durch den Betreiber der Föderation realisiert wird, sodass Teilnehmer, sofern Bedarf, diesen Dienst in Anspruch nehmen können. Zugleich wird hier ein geringes Maß an Ressourcen seitens der Identity Provider angenommen, sodass einige der Verfahren (z.B. Identitätsfeststellung, Binden des Faktors an den Benutzer) durch den Identity Provider selbst realisiert werden.

Die zweite methodische Anwendung greift auf das interföderierte Szenario eduGAIN aus Abschnitt 2.3 zurück, bei dem mehrere Föderationen wiederum eine Interföderation bilden. Hier werden, im Gegensatz zum ersten Anwendungsbeispiel, TPPs betrachtet, die durch beliebige externe Dienstleister realisiert werden. Aufgrund der globalen Skalierung des Szenarios werden in diesem Zusammenhang TPPs in Kombination mit remote-Verfahren zur Identitätsfeststellung diskutiert.

- **Anwendungsbeispiel DFN-AAI:** In diesem Anwendungsbeispiel agiert der Infrastrukturbetreiber, z.B. der Betreiber der nationalen Föderation DFN-AAI, zeitgleich als (externer) Faktorprüfer. Er betreibt die technische Komponente TPP (Stereotyp «software» gemäß Abbildung 4.9), d.h. einen spezialisierten SAML IDP, der nur Authentifizierungen von Zweitfaktoren durchführt. Gegenüber aller Service Provider, die das entsprechende, in Abschnitt 6.3.2 beschriebene Modul implementieren,[14] verhält sich der TPP somit als (spezialisierter) Identity Provider, d.h. TPP, während er gegenüber den Identity Providern als Service Provider agiert. Abhängig von den implementierten Verfahren zur Identitätsfeststellung und Bindung der Faktoren stellt der Föderationsbetreiber den Dienst eines Faktorprüfers entweder nur den IDPs der eigenen Föderation oder potentiell auch den IDPs anderer Föderationen zur Verfügung. Im letzteren, föderationsübergreifenden Fall müssten die Verfahren entsprechend geplant und ausgerichtet sein und remote-Verfahren zum Einsatz kommen, damit dies föderationsübergreifend praktikabel ist. Im Folgenden wird jedoch der konkrete Fall betrachtet, bei dem die Identity Provider der DFN-AAI aktiv in die Bindung der Faktoren der ihr zugehörigen Nutzer involviert werden. Dabei stellt eine Realisierungsmöglichkeit ein analoges Vorgehen oder bzw. die Wiederverwendung der Infrastruktur gemäß des Dienstes der DFN Public Key Infrastructure (PKI) dar, der (Benutzer-) Zertifikate für

[14] d.h. auch föderationsübergreifend

die im deutschen Forschungsnetz teilnehmenden Institutionen und Nutzer ausstellt. Da bei Benutzerzertifikaten ebenfalls eine hohe Verlässlichkeit erforderlich ist und ein Zertifikat zweifelsfrei an die rechtmäßige Person zu binden ist, existiert hier ein Face-to-Face (F2F) Vorgehen. D.h. um ein Benutzerzertifikat des DFN zu erhalten, muss eine Person vor-Ort bei einer Registration Authority (RA) vorsprechen, die in diesem Zuge die Identität des Benutzers überprüft. Da die Institutionen des deutschen Forschungsnetzes über viele verschiedene Standorte in Deutschland verteilt sind und eine Reise zum Standort des DFN in unverhältnismäßigem Aufwand bzw. Kosten stehen würde, wurden zu diesem Zwecke mehrere RAs eingerichtet, die an die entsprechenden Standorte der Institutionen ausgelagert wurden. So ist bspw. das Leibniz-Rechenzentrum in München zeitgleich eine RA für Zertifikate des DFN. Ein LRZ-Mitarbeiter der folglich ein neues Zertifikat beantragen möchte, führt zunächst die auf der entsprechenden Webseite[15] beschriebenen Schritte zur Beantragung eines Benutzerzertifikats aus und erscheint dann bei der durch den DFN beauftragen RA im Hause des LRZ. Anhand eines offiziellen Dokuments, z.B. Personalausweis oder Reisepass, wird dann die Identität der Person überprüft und ein Nachweis über die stattgefundene Identifizierung erzeugt. Erst dann kann das Zertifikat von der Person genutzt werden. Die bereits etablierten, verteilten RAs würden sich ebenfalls für die Bindung weiterer Authentifizierungsfaktoren für den durch einen Föderationsbetreiber betriebenen Two-Plus Dienst eignen. Ein Nutzer würde somit bei der RA erscheinen, um einen zweiten bzw. weiteren Authentifizierungsfaktor zu registrieren. Entweder geschieht dies analog zum Vorgehen bei Zertifikaten, sodass bspw. ein Nutzer vorab bestimmte Schritte selbst erledigen muss (z.B. Registrierung eines Authentifizierungsfaktors anhand einer Self-Service Webseite) und ein Vertreter der RA nur noch die Identität überprüft und den Faktor aktiviert oder indem alle Schritte vor-Ort durch die RA selbst getätigt werden (d.h. Aushändigen eines Tokens, Identitätsfeststellung, Bindung des Tokens an den Identifier der Person, Aktivierung). Ein derartiges Vorgehen ermöglicht darüber hinaus, dass das Vertrauen in die Bindung zwischen Person und Authentifizierungsfaktor, obwohl der Dienst durch den Betreiber der Föderation bereitgestellt wird, trotzdem lokal etabliert wird. Zusätzlich kann die RA als Anlaufstelle für authentifizierungsfaktorbezogene Prozeduren, wie bspw. das Ersetzen eines verlorenen Authentifizierungsfaktors gemäß SFA-Profil, dienen. Ein vergleichbares Vorgehen existiert auch bei der niederländischen Föderation SURF [HW17].

- **Anwendungsbeispiel eduGAIN:** In diesem Anwendungsbeispiel agiert, im Gegensatz zum zuvor skizzierten Modell, ein beliebiger, externer Dienstleister als Zweitfaktorprüfer. Hier kann es sich bspw. um eine Non-Profit Organisation handeln, die sich im Bereich der Multi-Faktor-Authentifizierung spezialisiert hat. Je nachdem in welchem Land sich die Organisation befindet, stellt diese eine Anfrage bei der entsprechenden nationalen Föderation zur Aufnahme als Teilnehmer und der damit verbundenen Integration in die Föderationsmetadaten. Die Nutzung dieses Faktorprüfers bzw. TPPs ist dabei *nicht* auf die Teilnehmer der entsprechenden nationalen Föderation beschränkt, sondern wurde lediglich aufgrund des hierarchisch aufgebauten Vertrauensmodells (vgl. Abschnitt 3.3.1) in einer der an eduGAIN teilnehmenden Föderationen

[15] https://www.lrz.de/services/pki/wieman/#ablauf

registriert. Dieser TPP stellt idealerweise ein oder mehrere Identitätsfeststellungsverfahren bereit, wovon mindestens eines der Verfahren ein remote-Verfahren darstellen sollte, da in einem globalen Szenario wie eduGAIN nicht von einer vor-Ort Identitätsfeststellung und Faktorbindung ausgegangen werden kann. In [LMZT20] wurden im Rahmen des GÉANT-Projektes verschiedene Identitätsfeststellungsverfahren analysiert, wobei u.a. auch dokumentenbasierte Lösungen betrachtet wurden. Hier wird bspw. der maschinenlesbare Chip des Personalausweises oder Reisepasses mit dem NFC[16]-Reader des Smartphones ausgelesen und bspw. mit einem durch den Benutzer hochgeladenen Selfie-Bildes verglichen. Weitere remote-Verfahren kombinieren dokumentenbasierte Lösungen mit einer Videotelefonie, sodass sich ein Benutzer gegenüber der TPP, bspw. durch Halten des Personalausweises in die Kamera neben seinen Kopf identifiziert. Neben remote-Verfahren ist prinizpiell auch die Bereitstellung eines länderspezifischen bzw. -abdeckenden Verfahrens denkbar, wie bspw. in Deutschland das PostIdent-Verfahren [Deu21b], bei dem eine zu identifizierende Person in einer Filiale der Deutschen Post erscheint. Durch die Registrierung beliebig vieler TPPs in beliebigen Föderationen mit unterschiedlichen Realisierungen hinsichtlich der Identitätsfeststellung und der verwendeten Authentifizierungsfaktoren entsteht so die notwendige Diversität, sodass Nutzer die für sie am besten geeignetste Variante auswählen können. Dies ist auch im Sinne des Datenschutzes, da ein Benutzer dessen IDP keine Multi-Faktor-Authentifizierung implementiert, die freie Wahl hat, wo bzw. wie seine Daten verarbeitet werden.

6.4 Zusammenfassung

Ziel des Kapitels war es, die in Kapitel 5 erarbeiteten bzw. referenzierten Konzepte zu evaluieren, prototypisch zu implementieren und anzuwenden.

Dazu wurde in Abschnitt 6.1 das Universelle Modell für Authentifizierungsszenarien erneut aufgegriffen. Da dessen methodische Anwendung bereits ausführlich in Abschnitt 5.1 anhand von repräsentativen Beispielen demonstriert und Templates auf Basis von realen MFA-Forschungsansätzen abgeleitet wurden, wurde in Abschnitt 6.1 UASM direkt gegen die aufgestellten Anforderungen abgeglichen. Hierbei zeigte sich, dass UASM alle entsprechenden Anforderungen des Anforderungskataloges (d.h. Hauptanforderung UM) erfüllt, da UASM auf MSM aufbaut und somit die durch MSM nicht oder nur teilweise erfüllten Anforderungen vollständig adressiert.

In Abschnitt 6.2 wurde gezeigt, dass das SFA-Profil einem umfassenden, mehrwöchigen Review-Prozess (REFEDS Community Consultation) unterzogen wurde, um die Anwendbarkeit und Annahmefähigkeit in R&E Identitätsföderationen bzw. Infrastrukturen zu evaluieren. Aus dem Reviewprozess, der einen großen Adressatenkreis einbezogen hat, gingen insgesamt nur vier Kommentare hervor (vgl. Abbildung 6.1), was schlussendlich zu einem Konsensus geführt hat und das Profil publiziert wurde. Ferner wurden im Jahr 2019 die REFEDS Identity- und Authentication-Assurance-Profile nach einem stattgefunden Experten-

[16] Near Field Communication

Review erfolgreich in der IANA Protocol Registry registriert. Darüber hinaus wurde der risikobasierte Ansatz zur Auswahl eines angemessenen Authentication Assurace Profils einmal exemplarisch anhand eines Webdienstes, der einen Ablageort für forschungsprojektspezifische Daten und Ergebnisse implementiert, durchlaufen und gezeigt, wie die jeweiligen Komponenten in Kombination verwendet werden können.

In Abschnitt 6.3 wurde der spezifizierte MFA-Workflow und dessen Zusammenspiel mit den Authentication-Assurance-Profilen sowie den vorgeschlagenen Erweiterungen in einer Testumgebung prototypisch implementiert. Es wurde der MFA-Workflow gegen die Anforderungen abgeglichen und anhand verschiedener Anwendungsmodelle methodisch diskutiert, wie die erarbeiteten Komponenten und Konzepte auf reale Szenarien übertragen werden können. Dabei wurden auch Verfahren zur Identitätsfeststellung adressiert und exemplarisch beschrieben, wie weitere Authentifizierungsfaktoren verlässlich, bspw. unter Wiederverwendung einer vorhandenen PKI-Infrastruktur, an eine Person gebunden werden können.

In dem folgenden, letzten Kapitel 7 wird die hier vorliegende Arbeit als Ganzes noch einmal aufgegriffen und die Ergebnisse sowie offene Forschungsfragestellungen übersichtlich zusammengefasst.

Kapitel 7

Zusammenfassung und Ausblick

Inhalt dieses Kapitels

Bereits vor aber auch beschleunigt durch den Ausbruch der globalen COVID-19 Pandemie [Wor22] verlagert sich unser alltägliches Leben, wenn auch z.T. unerwarteterweise, zunehmend ins Virtuelle, weswegen digitale Identitäten wichtiger denn je werden. Ob im privaten Bereich zur Verwendung von Streaming- und Socialising-Diensten oder im beruflichen Alltag zur Verwendung von Videokonferenz-Angeboten, wird deutlich, dass wir uns regelmäßig bei diversen Diensten registrieren. Dabei wird es vor allem für Personen, die auf die Verwendung eines Passwort-Managers o.ä. verzichten, immer herausfordernder sich die Vielzahl der verwendeten Benutzernamen, E-Mail-Adressen und Passwörter zu merken. Im kommerziellen Sektor haben, vorangehend durch die großen und weltweit bekannten *Big Five* (Identity) Provider, subsumiert unter der Abkürzung *GAFAM* [Wik21] (Google, Amazon, Facebook, Apple und Microsoft) darauf reagiert, indem sie anderen Service Providern Schnittstellen zur Verfügung stellen und diesen einen „Login mit ...“ anbieten. Auf diese Art und Weise wird die Benutzerverwaltung und Authentifizierung von den eigentlichen Diensten (und deren Autorisierung bzw. Zugriffskontrolle) entkoppelt, sodass Dienstbetreiber selbst von einer eigenen Implementierung abstrahieren können und ein Benutzer auf einen bereits vorhandenen Benutzeraccount zurückgreifen kann.

In der Forschung als auch im Allgemeinen ist eine entkoppelte Benutzerverwaltung und Authentifizierung unter dem Begriff föderiertes Identitätsmanagement bekannt. FIM greift auf das Konzept einer Föderation zurück, indem sich bspw. voneinander autonome Parteien (d.h. Identity Provider und Service Provider) bewusst dazu entscheiden eine Föderation zu gründen, sodass die teilnehmenden Identity Provider, Service Provider und Benutzer von den gegenseitig angebotenen Diensten profitieren können. Inter-FIM setzt darauf auf, indem mehrere Föderationen wiederum selbst eine Föderation gründen; eine Föderation von Föderationen, sprich eine Interföderation. Das Konzept der Interföderation findet in globalem Stil in *Research and Education* (R&E) Anwendung (vgl. Kapitel 2). Hier haben nationale Identitätsföderationen eine länderübergreifende Interföderation gebildet, sodass global auf R&E bezogene Dienste zugegriffen werden kann. Ende des Jahres 2021 sind hier rund 4600 Identity Provider und 3500 Service Provider aus 73 Föderationen vertreten [GÉ21b].

In dieser Dissertation wurden existierende Konzepte zur Authentication Assurance und Multi-Faktor-Authentifizierung in (Inter-) FIM untersucht und darauf aufbauend durch eigene Beiträge ergänzt. Die *Authentication Assurance*, die häufig in Form von Leveln, d.h. Level of Authentication Assurance, oder Profilen zum Ausdruck gebracht wird, beschreibt dabei den Grad bzw. die Stärke des Vertrauens einer durchgeführten Authentifizierung. Wird mehr als ein Authentifizierungsfaktor, im Sinne einer *Multi-Faktor-Authentifizierung*, an eine Person gebunden und erfüllt dieser, die gemäß einer Authentication-Assurance-Spezifikation festgeschriebenen Anforderungen, steigert dies das Vertrauen bzw. die Verlässlichkeit, dass eine Person, die sich authentifiziert hat, auch tatsächlich diejenige ist, die sie vorgibt zu sein. Da bereits vorhandene LoA-Rahmenwerke in den betrachteten Szenarien aufgrund der Vielzahl der enthaltenen Kriterien nicht umsetzbar sind, wurde im Rahmen der REFEDS Assurance Working Group, mit der Autorin dieser Arbeit als eine der Hauptautoren, eine leichtgewichtige Authentication-Assurance-Spezifikation für Authentifizierungen mit einem Faktor entwickelt (SFA-Profil), die in Kapitel 5 vorgestellt wurde. Neben der publizierten Version des SFA-Profils [ZSL19, REF18c, Zie18], die in Kapitel 5 aufgegriffen wurde, enthält diese Dissertation ebenfalls sinnvolle Erweiterungen, die u.a. das SFA-Profil mit dem MFA-Profil [REF17, Zie17] in einen logischen Zusammenhang setzen. Als praxisbezogene Hilfestellung wurde ein risikobasierter Ansatz erarbeitet, anhand dessen Service Provider bei der Auswahl eines angemessenen Authentication-Assurance-Profils unterstützt werden, dessen Schritte in Abschnitt 6.2.2 methodisch angewendet werden. Darüber hinaus wurde ein Fallback MFA-Workflow für Benutzer konzeptioniert, deren Identity Provider über keine eigene MFA-Implementierung verfügen. Der MFA-Workflow eignet sich im Besonderen für vollvermaschte Authentifizierungsszenarien, d.h. Szenarien, bei denen keine zentrale (technische) Instanz involviert ist, an die eine MFA-Lösung gekoppelt werden könnte. Der MFA-Workflow ist jedoch auch mit zentralisierten Architekturmodellen oder v.a., wenn verschiedene Architekturmodelle miteinander kombiniert werden, kompatibel. Die Architektur in Kapitel 4 führt dazu einen sogenannten Two-Plus Provider, d.h. einen externen Zweit-Faktorprüfer ein, der von einem MFA-fordernden Service Provider kontaktiert wird. Der Vorteil dieser Lösung ist, dass der MFA-Workflow, im Gegensatz zu den anderen evaluierten MFA-Ansätzen, keine statische Kombination von Faktorprüfern erzwingt, sondern eine beliebige Auswahl durch Benutzer ermöglicht. Zuletzt wurde anhand eines Universellen Modells für Authentifizierungsszenarien ein Lösungsansatz entwickelt, um Authentifizierungsszenarien ganzheitlich und auf service-orientierte Art und Weise zu beschreiben. Es wurden Templates erzeugt, die bei der Einführung neuer Technologien oder als Grundlage für Simulationen oder zur formalen Verifikation herangezogen werden können.

7.1 Zusammenfassung der Ergebnisse

Die Hauptbeiträge dieser Arbeit sowie die bereits vorab publizierten Beiträge, auf die in dieser Arbeit Bezug genommen wird, sind sowohl visuell in Abbildung 7.1 als auch nachfolgend, jeweils kapitelweise gegliedert, zusammengefasst.

Kapitel 2

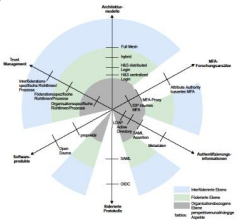
Problemstellung und Anforderungsanalyse

- Erfassung repräsentativer FIM-Szenarien
- Systematische Ableitung von Anforderungen auf Basis von vier Hauptanforderungsklassen
- Integrierter Anforderungskatalog

Kapitel 3

Grundlagen und Status quo

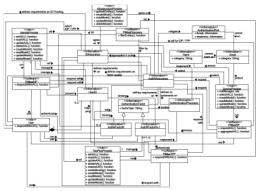
- Umfassende Zusammenstellung wesentlicher Grundlagen sowie Status quo



Kapitel 4

Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM

- Konzeption einer Gesamtarchitektur auf Basis der vier Teilmodelle für Managementarchitekturen [HAN99]



Kapitel 5

Spezifikation erforderlicher Konzepte

- Universelles Service Modell für Authentifizierungsszenarien
- SFA-Profil inklusive Erweiterungen
- Empfehlungen und Maßnahmen für Service Provider unter Verwendung eines risikobasierten Ansatzes
- Fallback MFA-Workflow

Kapitel 6

Evaluation, prototypische Implementierung und Anwendung

- Evaluation der Konzepte gegen die Anforderungen
- Prototypische Implementierung durch Aufbau einer Testumgebung
- Methodische Anwendung ausgewählter Konzepte

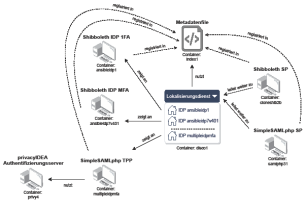


Abbildung 7.1: Überblick über die Ergebnisse der Arbeit

- Kapitel 1 befasst sich im Wesentlichen mit der Problemstellung und den daraus abgeleiteten Fragestellungen. Ein weiterer Output dieses Kapitels sind die Teile der Arbeit, die bereits vorab in Form von wissenschaftlichen Veröffentlichungen publiziert wurden.
- In Kapitel 2 wurde eine systematische Anforderungsanalyse auf Basis repräsentativer FIM-Szenarien durchgeführt. Die daraus resultierenden Hauptbeiträge sind:
  - Erfassung repräsentativer FIM-Szenarien
  - Die initiale Ableitung von vier Hauptanforderungsklassen:
    * Hauptanforderung AK: Definition eines leichtgewichtigen Authentication Assurance Konzepts zum Austausch der Qualität durchgeführter Authentifizierungen
    * Hauptanforderung RM: Umsetzungsunterstützung für Service Provider zur Auswahl eines angemessenen Authentication-Assurance-Profils
    * Hauptanforderung WF: Analyse existierender MFA-Realisierungsoptionen und Konzeption eines Fallback MFA-Workflows für vollvermaschte Authentifizierungsszenarien
    * Hauptanforderung UM: Service-orientierte und ganzheitliche Beschreib- und Modellierbarkeit von Entitäten und Diensten eines Authentifizierungsszenarios unabhängig von zugrundeliegendem Protokoll, Standard, Technologie oder Framework
  - Die Verfeinerung der Hauptanforderungsklassen gemäß eines Top-Down Ansatzes hin zu 30 detaillierten Einzelanforderungen
  - Die Gewichtung aller Anforderungen und deren Erfassung in einem integrierten Anforderungskatalog
- Kapitel 3 deckt die Grundlagen und den Status quo ab und fasst somit die wesentlichen Konzepte übersichtlich zusammen. Dazu zählt:
  - Identity & Access Management, Föderiertes Identitätsmanagement, Interföderiertes Identitätsmanagement
  - Authentifizierung, Multi-Faktor-Authentifizierung, MFA-Forschungsansätze in FIM und Level of Assurance
  - Informations- und Service-Managementmodelle
- In Kapitel 4 wurde eine Architektur zur Authentication Assurance und Multi-Faktor-Authentifizierung in FIM erarbeitet. Die Hauptbeiträge sind:
  - Die strukturierte Ableitung des Idealzustandes unter Verwendung der vier Teilmodelle (Organisations-, Informations-, Funktions- und Kommunikationsmodells) für Managementarchitekturen [HAN99]
  - Anwendung der Teilmodelle auf die vier zentralen Hauptanforderungen, was in vier Teilen der Architektur resultiert (Architekturteile AK, RM, WF und UM)

  - Spezifikation einer Gesamtarchitektur

- In Kapitel 5 wurden die durch die Architektur resultierenden, erforderlichen Konzepte detailliert erarbeitet. Die Hauptbeiträge sind die Folgenden:
  - Ein Universelles Service Modell für Authentifizierungsszenarien
  - Ein Konzept zur Authentication Assurance, im Speziellen das SFA-Profil, sowie einige Erweiterungen
  - Empfehlungen und Maßnahmen für Service Provider unter Verwendung eines risikobasierten Ansatzes
  - Ein Konzept zur Realisierung eines Fallback MFA-Workflows
- Kapitel 6 beschreibt die Evaluation, prototypische Implementierung und Anwendung der Konzepte. Dies umfasst:
  - Die Evaluation von UASM
  - Die Evaluation des SFA-Profils sowie die methodische Anwendung des risikobasierten Ansatzes zur Auswahl eines angemessenen Authentication-Assurance-Profils
  - Den Aufbau einer Testumgebung zur prototypischen Implementierung des MFA-Workflows sowie die Skizzierung verschiedener Anwendungsmodelle inklusive Anwendungsbeispiel in der DFN-AAI und eduGAIN

7.2 Ausblick auf offene Forschungsfragestellungen

Trotz des hier gelieferten, wesentlichen Beitrags zur Authentication Assurance und Multi-Faktor-Authentifizierung im föderierten Identitätsmanagement stellt dieses Forschungsthema nur ein Puzzlestück im Gesamtbild dar, aus dem sich in dessen Anlehnung, weitere interessante Forschungsfragestellungen ableiten lassen. Im Folgenden werden einige weitere Projekte vorgestellt:

- **Identity Assurance und Verfahren zur Feststellung der Identität**: Da das Thema Identity Assurance und Identitätsfeststellungsverfahren einen eigenen, umfassenden Forschungsbereich darstellt, sollte mit dieser Thematik als logische Konsequenz an die hier vorliegende Arbeit angeknüpft werden. Wie bereits aus den vorherigen Kapiteln ersichtlich wurde, stehen die Identity Assurance und Authentication Assurance in einem engen thematischen Zusammenhang, weswegen deren Zusammenspiel, aber auch deren Abhängigkeiten und Wechselwirkungen, weiter untersucht werden sollten. Da u.a. die Identitätsfeststellung in hochverteilten Szenarien eine Herausforderung darstellt (nicht nur zum Zwecke von MFA), wurden als Teil des GÉANT-Projekts mögliche Anwendungsfälle und Lösungsansätze bereits initial untersucht [LMZT20]. Hierbei wurden bspw. dokumentenbasierte Lösungen näher betrachtet, die das Scannen eines kompatiblen Ausweisdokumentes mit dem Smartphone erlauben. In diesem Zuge

wurden anhand eines Interviews einige NRENs, Forschungsinfrastrukturen und Institutionen hinsichtlich deren Anwendungsfälle und Anforderungen befragt. Dabei zeigt sich, dass sich die meisten Befragten mit der Thematik bereits beschäftigt haben und Anwendungsfälle bekannt sind, jedoch konkrete Anforderungen und Lösungsansätze nur kaum bis nicht vorhanden sind.

Der in Kapitel 5 spezifizierte MFA-Workflow setzt ebenfalls die Notwendigkeit eines eindeutigen, nicht wiederverwendbaren Identifiers voraus, der die Identität eines Benutzers widerspiegelt und an den weitere Authentifizierungsfaktoren geknüpft werden können. eduID befasst sich bspw. mit der Etablierung einer lebenslangen, digitalen Identität für R&E und ist bereits bei einigen Ländern in Planung oder z.T. bereits umgesetzt [DFN19, SUN21, SUR21a, SWI21a]. Ein weiterer Ansatz ist MyAcademicID [MyA19], eine Forschungsinitiative der Europäischen Union, die die Entwicklung einer europäischen eID (elektronische ID) für „Higher Education“ vorantreibt. Inwiefern hier ein Zusammenspiel möglich ist, bleibt zu untersuchen.

- **Biometrische Authentifizierungsfaktoren inklusive neuer Technologien**: In der SFA-Spezifikation aus Kapitel 5 wurden biometrische Authentifizierungsfaktoren zunächst ausgeklammert, da diese gemäß NIST nicht für Ein-Faktor-Authentifizierungen geeignet sind. Werden die Anforderungen der SFA-Spezifikation jedoch, wie in Abschnitt 5.2.3 beschrieben, ebenfalls auf die Faktoren einer Multi-Faktor-Authentifizierung übertragen, sind auch Anforderungen an biometrische Faktoren ab dem zweiten Faktor zu definieren. Neben der Biometrie selbst, bleibt zu untersuchen, inwieweit neue Technologien referenziert werden können, wie bspw. diejenigen die in die Kategorie „something you do“ (verhaltensbasierte Faktoren) fallen oder auch ortsbezogene Faktoren (*engl. location based factor(s)*).

- **Quantum Computing**: Mit dem visionären Forschungsbereich zur Quantentechnologie (Quantum Computing) [YM08, Hom18], in den das Leibniz-Rechenzentrum ebenfalls aktiv involviert ist [Bay21], sind Faktoren, die kryptographische Operationen einbeziehen, z.B. RSA/DSA-basierte Software oder Geräte, neu zu überdenken, da anhand von Quantentechnik (Qubits) leistungsintensive Rechenprobleme, wie bspw. Verschlüsselungssysteme, deutlich schneller gelöst werden können.

- **Self Sovereign Identity, Blockchain und Distributed Ledger Technologien**: Ein weiterer Forschungsbereich liegt in der durch die Kryptowährung Bitcoin [Nak08] an Bekanntheit gewonnenen Blockchain-Technologie, die oftmals synomym zur DL[1]-Technologie verwendet wird. Hierbei wird von einer Trusted Third Party abstrahiert, indem das Vertrauen in durchgeführte Transaktionen dezentral verwaltet wird. Es ist zu untersuchen inwieweit eine derartige Technologie auf (Inter-) Föderationsszenarien, wie z.B. eduGAIN, übertragbar ist, wo ebenfalls vertrauenswürdige, hierarchisch aufgebaute Trusted Third Parties (i.S.v. Interföderation, Föderation) implementiert sind. Eine weitere Möglichkeit stellt die Verwendung eines DLs nur für einen bestimmten Teilbereich von FIM dar, sodass bspw. Assurance-Information in Form eines öffentlichen DLs ausgetauscht wird.

[1] Distributed Ledger

Weiter zu untersuchen bleibt auch, inwieweit Forschungsansätze zur Self Sovereign Identity, die den Nutzern die Herrschaft über eigene Daten ermöglicht, klassische FIM-Szenarien verbessern oder ablösen können.

Abkürzungsverzeichnis

1FA	Ein-Faktor-Authentifizierung
2FA	Zwei-Faktor-Authentifizierung
AA	Attribute Authority
AAI	Authentication and Authorization Infrastructure
AARC	Authentication and Authorisation for Research and Collaboration
AARC-BPA	AARC Blueprint Architecture
ACR	Authentication Context Class Reference
AK	Authentication-Assurance-Konzept
AMLD V	Anti-Money Laundering Directive V
AMR	Authentication Methods References
API	Application Programming Interface
AS	Authorization Server
AuthN	Authentication
AuthNI	Authentication Information
AWS	Amazon Webservices
CRUD	Create, Read, Update, Delete
CSM	Customer Service Management
CSS	Cascading Style Sheets
DFN	Deutsches Forschungsnetz
DFN-AAI	DFN Authentifikations- und Autorisierungs-Infrastruktur
DFN-Verein	Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DL	Distributed Ledger
DMTF	Distributed Management Task Force
DS	Discovery Service
DSA	Datenschutzanforderung
DSA	Digital Signature Algorithm
EC	Entity Category
eID	Elektronische Identität
eIDAS	Electronic Identification, Authentication and Trust Services
ECDSA	Elliptic Curve Digital Signature Algorithm
EU	Europäische Union
eTOM	enhanced Telecom Operations Map

F2F	Face-to-Face
FA	Funktionale Anforderung
FIM	Föderiertes Identitätsmanagement
FIM4R	Federated Identity Management for Research Communities
GAFAM	Google (Alphabet), Amazon, Facebook, Apple und Microsoft
HOTP	HMAC-based One Time Password
HR	Human Resources
H&S	Hub & Spoke
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAF	Identity Assurance Framework
IAM	Identity & Access Management
IANA	Internet Assigned Numbers Authority
ID	Identifier
IDP	Identity Provider
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
Inter-FIM	Interföderiertes Identitätsmanagement
ISO	International Organization for Standardization
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
JWT	JSON Web Token
KIAF	Kantara Identity Assurance Framework
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
LRZ	Leibniz-Rechenzentrum
MACE	Middleware Architecture Committee for Education
MCA	Multi-Channel-Authentifizierung
MFA	Multi-Faktor-Authentifizierung
MFAaaS	Multi Factor Authentication as a Service
MSM	MNM Service Model
NFC	Near Field Communication
NFA	Nicht-funktionale Anforderung
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NREN	National Research and Education Network
OASIS	Organization for the Advancement of Structured Information Standards
OIDC	OpenID Connect

OP	OpenID Provider
OSCRP	Open Science Cyber Risk Profile
OTP	One Time Password
PHP	Hypertext Preprocessor
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public-Key-Infrastruktur
PoC	Proof of Concept
PSD2	Payment Service Directive 2
QoS	Quality of Service
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAS	Real-World Authentication Subject
RDBMS	Relationales Datenbankmanagementsystem
R&E	Research & Education
RFC	Request for Comments
R-Infra	Research Infrastructure
RM	Risikobasierte Maßnahmen
RP	Relying Party
RSA	Rivest Shamir Adleman
SAC	Service Assessment Criteria
SAML	Security Assertion Markup Language
SAP	Service Access Point
SAS IDP	Step-up Authentication Service Identity Provider
SAS SP	Step-up Authentication Service Service Provider
SIA	Sicherheitsanforderung
SID	Shared Information and Data Model
SIRTFI	Security Incident Response Trust Framework for Federated Identity
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SP	Service Provider
SSO	Single Sign On
SSp	SimpleSAMLphp
SURF	Samenwerkende Universitaire Reken Faciliteiten
TAAS	Trustworthy Authentication Information Administration Service
TAC	Trustworthy Authentication Information Consumer
TAM	Telecom Applications Map
TAP	Trustworthy Authentication Information Provider
TAPS	Trustworthy Authentication Information Provisioning Service
TAS	Trustworthy Authentication Subject
TAuthNI	Trustworthy Authentication Information
TBAC	Trust Based Access Control
TMF	Telemanagement Forum
TOTP	Time-based One Time Password

TPP	Two Plus Provider
UASM	Universal Authentication Service Model
UM	Universelles Modell
UML	Unified Modeling Language
URI	Uniform Resource Identifier
VM	Virtuelle Maschine
VO	Virtuelle Organisation
VoT	Vectors of Trust
WAYF	Where Are You From
WF	(MFA)-Workflow
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

Abbildungsverzeichnis

Listingsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[AAR18] AARC2 Project: *Second factor authentication component for the Life Science AAI*. Technischer Bericht, AARC2 Project, 2018. https://docs.google.com/document/d/18OfWMXLx88zw6eqgPIyG3zIuyIoWGXc0LMMS57dgyOE. (Zitiert auf Seite 37.)

[AAR19] AARC Consortium Partners, AppInt members, Nicolas Liampotis (Editor): *Deliverable DJRA1.4: Evolution of the AARC Blueprint Architecture*. DJRA1.4, AARC2 Project, 2019. https://aarc-project.eu/wp-content/uploads/2019/05/AARC2-DJRA1.4_v2-FINAL.pdf. (Zitiert auf den Seiten 26 und 221.)

[ABB+18] Christopher J. Atherton, Tom Barton, Jim Basney, Daan Broeder, Alessandro Costa, Mirjam van Daalen, Stephanie Dyke, Willem Elbers, Carl Fredrik Enell, Enrico M. V. Fasanelli, João Fernandes, Licia Florio, Peter Gietz, David L. Groep, Matthias B. Junker, Christos Kanellopoulos, David Kelsey, Philip Kershaw, Cristina Knapic, Thorsten Kollegger, Scott Koranda, Mikael Linden, Filip Marinic, Ludek Matyska, Tommi H. Nyrönen, Stefan Paetow, Laura A. D. Paglione, Sandra Parlati, Christopher Phillips, Michal Prochazka, Nicholas Rees, Hannah Short, Uros Stevanovic, Michael Tartakovsky, Gerben Venekamp, Tom Vitez, Romain Wartel, Christopher Whalen, John White und Carlo M. Zwölf: *Federated Identity Management for Research Collaborations version 2*. Technischer Bericht, FIM4R, 2018. https://doi.org/10.5281/zenodo.1307551. (Zitiert auf den Seiten 24, 25 und 26.)

[Ama21] Amazon: *Identity federation in AWS*. https://aws.amazon.com/de/identity/federation/, 2021. [Online; abgerufen am 24.02.2021]. (Zitiert auf Seite 29.)

[Ape21] Apereo Foundation: *Central Authentication Service. Enterprise Single Sign On for All*. https://apereo.github.io/cas/6.3.x/index.html, 2021. [Online; abgerufen am 04.08.2021]. (Zitiert auf Seite 81.)

[App22] Apple: *Touch ID und Face ID - Sicherheit*. https://support.apple.com/de-de/guide/security/sec067eb0c9e/web, 2022. [Online; abgerufen am 22.01.2022]. (Zitiert auf Seite 74.)

[AXE20] AXELOS: *ITIL 4: Create, Deliver and Support.* The Stationery Office, 2020. (Zitiert auf Seite 14.)

[Bay21] Bayerische Akademie der Wissenschaften: *Pressemitteilung; Munich Quantum Valley: Bayerns Beitrag zur nationalen und europäischen Quantenstrategie.* `https://www.badw.de/die-akademie/presse/pressemitteilungen/pm-einzelartikel/detail/munich-quantum-valley-bayerns-beitrag-zur-nationalen-und-europaeischen-quantenstrategie.html`, 2021. [Online; abgerufen am 18.01.2021]. (Zitiert auf Seite 214.)

[BB10] Arndt Bode und Rolf Borgeest (Herausgeber): *Informationsmanagement in Hochschulen.* Springer, 2010. (Zitiert auf Seite 51.)

[BBG+15] T. Barton, J. Basney, D. Groep, N. Harris, L. Johansson, D. Kelsey, S. Koranda, R. Wartel, A. West und H. Short (Editor): *A Security Incident Response Trust Framework for Federated Identity (Sirtfi).* Technischer Bericht, REFEDS, 2015. `https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf`. (Zitiert auf Seite 117.)

[BBMS07] Yolanta Beres, Adrian Baldwin, Marco C. Mont und Simon Shiu: *On Identity Assurance in the Presence of Federated Identity Management Systems.* In: *Proceedings of the 2007 ACM Workshop on Digital Identity Management*, Seiten 27–35. ACM, 2007. (Zitiert auf Seite 172.)

[BDN+13] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta und Emad A. Nabbus: *NIST Special Publication (SP) 800-63-2. Electronic Authentication Guideline.* NIST SP 800-63-2, National Institute of Standards and Technology, 2013. `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf`. (Zitiert auf den Seiten 76 und 89.)

[Ben06] Messaoud Benantar: *Access Control Systems. Security, Identity Management and Trust Models.* Springer US, 2006. (Zitiert auf Seite 6.)

[BJK+13] Daan Broeder, Bob Jones, David Kelsey, Philip Kershaw, Stefan Lüders, Andrew Lyall, Tommi Nyrönen, Romain Wartel und Heinz J. Weyer: *Federated Identity Management for Research Collaborations version 1.* Technischer Bericht, FIM4R, 2013. `https://fim4r.org/wp-content/uploads/2017/07/CERN-OPEN-2012-006-2.pdf`. (Zitiert auf Seite 24.)

[Bou09] Latifa Boursas: *Trust-Based Access Control in Federated Environments.* Dissertation, Technische Universität München, 2009. (Zitiert auf Seite 11.)

[Bro17] Robert Broeckelmann: *When To Use Which (OAuth2) Grants and (OIDC) Flows.* `https://medium.com/@robert.broeckelmann/when-to-use-which-oauth2-grants-and-oidc-flows-ec6a5c00d864`, 2017. [Online, abgerufen am 29.10.2021]. (Zitiert auf Seite 61.)

[Bun22] Bundesamt für Sicherheit in der Informationstechnik: *Glossar der Cyber-Sicherheit.* `https://www.bsi.bund.de/DE/Themen/Unternehmen-und-`

Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html, 2022. [Online; abgerufen am 01.02.2022]. (Zitiert auf Seite 72.)

[CES19] CESNET: *eduid.cz WAYF/DS*. https://www.eduid.cz/en/tech/wayf, 2019. [Online; abgerufen am 27.11.2021]. (Zitiert auf den Seiten 192, 193 und 223.)

[CES21] CESNET: *wayf*. https://github.com/CESNET/wayf, 2021. [Online; abgerufen am 27.11.2021]. (Zitiert auf den Seiten 192, 193 und 223.)

[Cha09] David W. Chadwick: *Federated Identity Management*. In: A. Aldini, G. Barthe und R. Gorrieri (Herausgeber): *Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures*, Seiten 96–120. Springer, Berlin, Heidelberg, 2009. (Zitiert auf den Seiten 3, 50 und 52.)

[CHK+05] Scott Cantor, Frederick Hirsch, John Kemp, Rob Philpott und Eve Maler: *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, OASIS, 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf. (Zitiert auf den Seiten 54 und 56.)

[Cis21] Cisco: *Duo*. https://duo.com/, 2021. [Online; abgerufen am 04.08.2021]. (Zitiert auf Seite 81.)

[CKPM05] Scott Cantor, John Kemp, Rob Philpott und Eva Maler: *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, OASIS, 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf. (Zitiert auf den Seiten 18, 29, 54 und 55.)

[CMPM05] Scott Cantor, Jahan Moreh, Rob Philpott und Eve Maler: *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, OASIS, 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf. (Zitiert auf den Seiten 55 und 56.)

[Cry18] Cryptomatic, by Parker, A. M.: *Overview of the NIST Digital Identity Model compared to eIDAS*. https://www.cryptomathic.com/news-events/blog/overview-of-the-nist-digital-identity-model-compared-to-eidas, 2018. [Online; abgerufen am 10.05.2021]. (Zitiert auf Seite 96.)

[CSC18] CSCfi: *Stepup-proxy*. https://github.com/CSCfi/stepup-proxy, 2018. [Online; abgerufen am 23.01.2018]. (Zitiert auf Seite 82.)

[DC02] Jan De Clercq: *Single Sign-On Architectures*. In: *Infrastructure Security. International Conference. InfraSec 2002*, Seiten 40–58. Springer, 2002. (Zitiert auf Seite 72.)

[Deu21a] Deutsche Bundesbank: *PSD2*. https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/psd2/psd2-775434, 2021. [Online; abgerufen am 24.02.2021]. (Zitiert auf Seite 29.)

[Deu21b] Deutsche Post: *POSTIDENT*. `https://www.deutschepost.de/de/p/postident.html`, 2021. [Online; abgerufen am 27.11.2021]. (Zitiert auf Seite 207.)

[DFN10a] DFN: *DFN-AAI: Der Dienst*. `https://www.aai.dfn.de/der-dienst/`, 2010. [Online; abgerufen am 18.05.2018]. (Zitiert auf den Seiten 2 und 51.)

[DFN10b] DFN: *DFN: Deutsches Forschungsnetz*. `https://www.dfn.de/`, 2010. [Online; abgerufen am 18.05.2018]. (Zitiert auf Seite 17.)

[DFN17] DFN: *Klassen der Verlässlichkeit in der DFN-AAI*. `https://doku.tid.dfn.de/de:degrees_of_reliance`, 2017. [Online; abgerufen am 23.08.2019]. (Zitiert auf Seite 94.)

[DFN19] DFN-Verein: *edu-ID*. `https://doku.tid.dfn.de/de:aai:eduid`, 2019. [Online; abgerufen am 18.01.2021]. (Zitiert auf den Seiten 53 und 214.)

[dMAS+20] B. de Medeiros, N. Agarwal, N. Sakimura, J. Bradley und M. Jones: *OpenID Connect Session Management 1.0 - draft 30*. Implementer's Draft, OpenID Foundation, 2020. `https://openid.net/specs/openid-connect-session-1_0.html`. (Zitiert auf Seite 63.)

[ELI21] ELIXIR: *ELIXIR Research Infrastructure*. `https://elixir-europe.org/`, 2021. [Online; abgerufen am 10.02.2021]. (Zitiert auf Seite 24.)

[Eur14] Europäisches Parlament und Rat der Europäischen Union: *Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG*. `https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=DE`, 2014. [Online; abgerufen am 08.12.2020]. (Zitiert auf den Seiten 34 und 91.)

[Eur15a] Europäische Kommission: *Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt*. `https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R1502&from=DE`, 2015. [Online; abgerufen am 08.12.2020]. (Zitiert auf Seite 91.)

[Eur15b] Europäische Kommission: *Payment services (PSD 2) - Directive (EU) 2015/2366*. `https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en`, 2015. [Online, abgerufen am 24.02.2021]. (Zitiert auf Seite 29.)

[Eur18] Europäische Kommission: *Anti-money laundering (AMLD V) - Directive (EU) 2018/843*. `https://ec.europa.eu/info/law/anti-money-`

`laundering-amld-v-directive-eu-2018-843_en`, 2018. [Online; abgerufen am 24.02.2021]. (Zitiert auf Seite 29.)

[For17] Forum Standaardisatie: *A guide for government organisations - Assurance levels for digital service provision.* `https://www.forumstandaardisatie.nl/sites/bfs/files/atoms/files/Assurance%20levels%20for%20digital%20service%20provision.pdf`, 2017. [Online, abgerufen am 12.04.2021]. (Zitiert auf Seite 177.)

[FSG+01] David Ferraiolo, Ravi Sandhu, Serban I. Gavrila, D. Richard Kuhn und Ramaswamy Chandramouli: *Proposed NIST Standard for Role Based Access Control.* ACM Transactions on Information and System Security, 4(3):224–274, 2001. (Zitiert auf Seite 6.)

[GÉ16] GÉANT Association: *eduGAIN Policy Framework Declaration.* `https://technical.edugain.org/doc/eduGAIN-Declaration-v2bis-web.pdf`, 2016. [Online; abgerufen am 22.1.2021]. (Zitiert auf Seite 70.)

[GÉ17a] GÉANT Project: *eduGAIN Description and Value Proposition.* `https://wiki.geant.org/display/PLMTES/eduGAIN`, 2017. [Online; abgerufen am 22.01.2022]. (Zitiert auf den Seiten 16 und 221.)

[GÉ17b] GÉANT Project: *Federation Architectures.* `https://wiki.geant.org/display/eduGAIN/Federation+Architectures`, 2017. [Online; abgerufen am 15.05.2018]. (Zitiert auf den Seiten 18, 35, 66, 67, 68 und 221.)

[GÉ17c] GÉANT Project: *Identity Assurance Service Attribute Authority.* `https://wiki.geant.org/display/gn42jra3/Identity+Assurance+Service+Attribute+Authority`, 2017. [Online; abgerufen am 24.09.2021]. (Zitiert auf Seite 84.)

[GÉ18] GÉANT Association: *eduGAIN.* `https://edugain.org/`, 2018. [Online; abgerufen am 18.05.2018]. (Zitiert auf den Seiten 3, 15 und 69.)

[GÉ20a] GÉANT Association: *eduroam.* `https://eduroam.org/`, 2020. [Online; abgerufen am 20.10.2020]. (Zitiert auf den Seiten 17 und 39.)

[GÉ20b] GÉANT Project: *Guide for Joining eduGAIN as a Federation.* `https://wiki.geant.org/display/eduGAIN/Guide+for+Joining+eduGAIN+as+a+Federation`, 2020. [Online; abgerufen am 22.1.2021]. (Zitiert auf den Seiten 69 und 70.)

[GÉ21a] GÉANT Association: *eduGAIN Metadata source.* `https://mds.edugain.org/edugain-v1.xml`, 2021. [Online; abgerufen am 18.12.2021]. (Zitiert auf den Seiten 58 und 223.)

[GÉ21b] GÉANT Association: *eduGAIN technical site.* `https://technical.edugain.org/`, 2021. [Online; abgerufen am 18.12.2021]. (Zitiert auf den Seiten 15, 21, 78, 195 und 209.)

[GÉ22a] GÉANT Association: *GÉANT Projects*. `https://geant.org/projects/`, 2022. [Online; abgerufen am 06.02.2022]. (Zitiert auf Seite 15.)

[GÉ22b] GÉANT Association: *InAcademia: Online Student Validation*. `https://inacademia.org/`, 2022. [Online; abgerufen am 04.02.2022]. (Zitiert auf Seite 151.)

[GE16] David Groep (Editor): *IGTF Levels of Authentication Assurance - Version 1.1-2016*. Technischer Bericht, IGTF, 2016. `https://www.igtf.net/ap/authn-assurance/igtf-authn-assurance-1.1.pdf`. (Zitiert auf Seite 95.)

[GFL+17] Paul A. Grassi, James L. Fenton, Naomi B. Lefkovitz, Jamie M. Danker, Yee Yin Choong, Kristen K. Greene und Mary F. Theofanos: *NIST Special Publication 800-63A. Digital Identity Guidelines. Enrollment and Identity Proofing Requirements*. NIST SP 800-63A, National Institute of Standards and Technology, 2017. `https://doi.org/10.6028/NIST.SP.800-63a`. (Zitiert auf den Seiten 33, 76 und 89.)

[GFN+17] Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, Naomi B. Lefkovitz, Jamie M. Danker, Yee Yin Choong, Kristen K. Greene und Mary F. Theofanos: *NIST Special Publication 800-63B. Digital Identity Guidelines. Authentication and Lifecycle Management*. NIST SP 800-63B, National Institute of Standards and Technology, 2017. `https://doi.org/10.6028/NIST.SP.800-63b`. (Zitiert auf den Seiten 33, 74, 75, 90, 166 und 167.)

[GGF17a] Paul A. Grassi, Michael E. Garcia und James L. Fenton: *DRAFT NIST Special Publication 800-63-3. Digital Identity Guidelines*. Draft, National Institute of Standards and Technology, 2017. `https://csrc.nist.gov/CSRC/media/Publications/sp/800-63/3/draft/documents/sp800-63-3-draft-revised.pdf`. (Zitiert auf den Seiten 89 und 96.)

[GGF17b] Paul A. Grassi, Michael E. Garcia und James L. Fenton: *NIST Special Publication 800-63-3. Digital Identity Guidelines*. NIST SP 800-63-3, National Institute of Standards and Technology, 2017. `https://doi.org/10.6028/NIST.SP.800-63-3`. (Zitiert auf den Seiten 33, 38, 72, 75, 88, 89, 90, 123, 174, 175 und 189.)

[GHH+01] Markus Garschhammer, Rainer Hauck, Heinz Gerd Hegering, Bernhard Kempter, Igor Radisic, Harald Roelle, Holger Schmidt, Michael Langer und Michael Nerb: *Towards generic service management concepts a service model based approach*. In: *2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No.01EX470)*, Seiten 719–732. IEEE, 2001. (Zitiert auf den Seiten 101, 135, 137, 142, 150, 158, 160, 164 und 222.)

[GHH+02] Markus Garschhammer, Rainer Hauck, Heinz Gerd Hegering, Bernhard Kempter, Igor Radisic, Harald Roelle und Holger Schmidt: *A case-driven methodology*

for applying the MNM service model. In: *NOMS 2002. IEEE/IFIP Network Operations and Management Symposium. ' Management Solutions for the New Communications World'(Cat. No.02CH37327)*, Seiten 697–710. IEEE, 2002. (Zitiert auf den Seiten 101, 135, 137, 142, 150, 158, 160, 164 und 222.)

[GHK+01] Markus Garschhammer, Rainer Hauck, Bernhard Kempter, Igor Radisic, Harald Roelle und Holger Schmidt: *The MNM service model - Refined Views on Generic Service Management.* Journal of Communications and Networks, 3(4):297–306, 2001. (Zitiert auf den Seiten 101, 135, 137, 142, 150, 158, 160, 164 und 222.)

[Góm20] Sergio Gómez: *GitHub Repository.* `https://github.com/sgomez`, 2020. [Online; abgerufen am 30.10.2020]. (Zitiert auf den Seiten 195 und 223.)

[Goo22] Google: *Bestätigungscodes mit Google Authenticator abrufen.* `https://support.google.com/accounts/answer/1066447`, 2022. [Online; abgerufen am 22.01.2022]. (Zitiert auf Seite 74.)

[GRS+17] Paul A. Grassi, Justin P. Richer, Sarah K. Squire, James L. Fenton, Ellen M. Nadeau, Naomi B. Lefkovitz, Jamie M. Danker, Yee Yin Choong, Kristen K. Greene und Mary F. Theofanos: *NIST Special Publication 800-63C. Digital Identity Guidelines. Federation and Assertions.* NIST SP 800-63C, National Institute of Standards and Technology, 2017. `https://doi.org/10.6028/NIST.SP.800-63c`. (Zitiert auf den Seiten 33 und 90.)

[HAN99] Heinz Gerd Hegering, Sebastian Abeck und Bernhard Neumair: *Integriertes Management vernetzter Systeme – Konzepte, Architekturen und deren betrieblicher Einsatz.* dpunkt–Verlag, 1999. (Zitiert auf den Seiten 5, 8, 108, 109, 112, 114, 115, 117, 139, 212 und 225.)

[Har12] Dick Hardt: *The OAuth 2.0 Authorization Framework.* RFC 6749, RFC Editor, 2012. `https://rfc-editor.org/rfc/rfc6749.txt`. (Zitiert auf den Seiten 29, 54 und 60.)

[HCH+05] John Hughes, Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra, Rob Philpott und Eve Maler: *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, OASIS, 2005. `http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf`. (Zitiert auf den Seiten 55 und 56.)

[Héd21] Mihály Héder: *Pyff+ Optimizations and mock metadata.* `https://wiki.geant.org/display/gn43wp5/Sprint+Demo+3.6+-+February+09?preview=/148089097/247431433/WP5%20-%20T2%20Incubator%20Sprint%20Demo%203.6%20-%20pyFF-Metadata_Mockup.pdf`, 2021. [Online; abgerufen am 09.02.2021]. (Zitiert auf den Seiten 195 und 196.)

[HFCK17] Vincent C. Hu, David F. Ferraiolo, Ramaswamy Chandramouli und D. Richard Kuhn: *Attribute-Based Access Control.* Artech House, 2017. (Zitiert auf Seite 6.)

[HJS+21] R. Hedberg, M. Jones, A. Solberg, S. Gulliksson und J. Bradley: *OpenID Connect Federation 1.0 - draft 17*. Implementer's Draft, OpenID Foundation, 2021. https://openid.net/specs/openid-connect-federation-1_0.html. (Zitiert auf Seite 63.)

[HLP+17] Lukas Hämmerle, Slavek Licehammer, Wolfgang Pempe, Michael Schmidt, Niels van Dijk und Jule Ziegler: *Technical Architecture Options for Providing Step-Up Authentication (and Assurance Levels)*. Technischer Bericht, GÉANT Project, 2017. https://docs.google.com/document/d/1WxF6Ls4svLfUjCTePa6u4DAlR8fTPNU5Gw9KZTnSemE. (Zitiert auf den Seiten 78 und 84.)

[Hom07] Wolfgang Hommel: *Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management*. Dissertation, Ludwig-Maximilians-Universität München, 2007. (Zitiert auf den Seiten 3, 10, 11, 51, 53, 55 und 64.)

[Hom18] Matthias Homeister: *Quantum Computing verstehen: Grundlagen – Anwendungen – Perspektiven*. Springer Vieweg, 2018. (Zitiert auf Seite 214.)

[HPL21] Dick Hardt, Aaron Parecki und Torsten Lodderstedt: *The OAuth 2.1 Authorization Framework*. Internet-Draft, Internet Engineering Task Force, 2021. https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1-04, Work in Progress. (Zitiert auf Seite 61.)

[HPM05a] Frederick Hirsch, Rob Philpott und Eve Maler: *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, OASIS, 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf. (Zitiert auf Seite 55.)

[HPM05b] Jeff Hodges, Rob Philpott und Eve Maler: *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, OASIS, 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf. (Zitiert auf Seite 55.)

[HW17] Bob Hulsebosch und Maarten Wegdam: *Remote Vetting For SURFconext Strong Authentication*. Technischer Bericht, SURF, 2017. https://www.surf.nl/files/2019-02/report%20remote%20vetting%20for%20surfconext%20strong%20authentication.pdf. (Zitiert auf Seite 206.)

[Ide21] Identity Python: *SATOSA*. https://github.com/IdentityPython/SATOSA, 2021. [Online; abgerufen am 27.11.2021]. (Zitiert auf Seite 198.)

[IGT21] IGTF: *Interoperable Global Trust Federation (IGTF)*. https://www.igtf.net/, 2021. [Online; abgerufen am 10.05.2021]. (Zitiert auf Seite 95.)

[InC13a] InCommon: *Identity Assurance Assessment Framework*. Technischer Bericht, InCommon, 2013. https://incommon.org/wp-content/uploads/2019/04/IAAF.pdf. (Zitiert auf Seite 95.)

[InC13b] InCommon: *Identity Assurance Profiles Bronze and Silver - Version 1.2*. Technischer Bericht, InCommon, 2013. `https://incommon.org/wp-content/uploads/2019/04/IAP.pdf`. (Zitiert auf Seite 94.)

[InC21] InCommon: *NIH application to require multi-factor authentication*. `https://www.incommon.org/news/nih-application-to-require-multi-factor-authentication/`, 2021. [Online; abgerufen am 12.04.2021]. (Zitiert auf Seite 176.)

[Int09] International Telecommunication Union: *Series X: Data Networks, Open System Communication and Security. Cyberspace security – Identity management. Baseline capabilities for enhanced global identity management and interoperability*. Recommendation ITU-T X.1250, International Telecommunication Union, 2009. `https://www.itu.int/rec/T-REC-X.1250-200909-I/en`. (Zitiert auf Seite 51.)

[Int12] International Telecommunication Union: *Series X: Data Networks, Open System Communication and Security. Cyberspace security – Identity management. Entity authentication assurance framework*. Recommendation X.1254, International Telecommunication Union, 2012. `https://www.itu.int/rec/T-REC-X.1254-201209-S/en`. (Zitiert auf den Seiten 73, 91 und 169.)

[Int16] Internet2: *eduPerson Object Class Specification (201602)*. Technischer Bericht, Internet2, 2016. `https://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html`. (Zitiert auf den Seiten 117 und 118.)

[Int20] Internet Assigned Numbers Authority: *Level of Assurance (LoA) Profiles*. `https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml`, 2020. [Online; abgerufen am 14.04.2021]. (Zitiert auf Seite 189.)

[Int21] Internet2: *Duo Security*. `https://internet2.edu/services/duo-security/`, 2021. [Online; abgerufen am 24.02.2021]. (Zitiert auf den Seiten 20 und 81.)

[ISO13a] ISO/IEC: *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Technischer Bericht, ISO/IEC, 2013. (Zitiert auf den Seiten 31, 121 und 172.)

[ISO13b] ISO/IEC: *ISO/IEC 29115:2013 Information technology - Security techniques - Entity authentication assurance framework*. Technischer Bericht, ISO/IEC, 2013. (Zitiert auf den Seiten 50, 74, 75 und 90.)

[JB20] M. Jones und J. Bradley: *OpenID Connect Back-Channel Logout 1.0 - draft 06*. Implementer's Draft, OpenID Foundation, 2020. `https://openid.net/specs/openid-connect-backchannel-1_0.html`. (Zitiert auf Seite 63.)

[Jod08] Wolfgang Jodl: *SESAM - Services Standards for the Automotive: Federation Services*. `https://www.kuppingercole.com/files/Jodl_-_SESAM.pdf`, 2008. [Online; abgerufen am 24.02.2021]. (Zitiert auf Seite 28.)

[Joh12] Leif Johansson: *An IANA Registry for Level of Assurance (LoA) Profiles*. RFC 6711, RFC Editor, 2012. `https://rfc-editor.org/rfc/rfc6711.txt`. (Zitiert auf den Seiten 189 und 198.)

[Jon19] Mike Jones: *OpenID Connect Federation Progress*. `https://openid.net/2019/06/25/openid-connect-federation-progress/`, 2019. [Online, abgerufen am 29.10.2021]. (Zitiert auf Seite 63.)

[Jon20] M. Jones: *OpenID Connect Front-Channel Logout 1.0 - draft 04*. Implementer's Draft, OpenID Foundation, 2020. `https://openid.net/specs/openid-connect-frontchannel-1_0.html`. (Zitiert auf Seite 63.)

[Jor17] Jonas Jores: *Evaluation von Lösungsansätzen zur Multi-Faktor Authentifizierung im Inter-Föderierten Identitätsmanagement*. Bachelorarbeit, Ludwig-Maximilians-Universität München, 2017. (Zitiert auf Seite 20.)

[Kan10] Kantara Initiative: *Identity Assurance Framework: Assurance Levels*. KIAF-1200, Kantara Initiative, 2010. `https://kantarainitiative.org/identity-assurance-framework`. (Zitiert auf Seite 92.)

[Kan18a] Kantara Initiative: *Commonly-Applicable Service Assessment Criteria*. KIAF-1410, Kantara Initiative, 2018. `https://kantarainitiative.org/identity-assurance-framework`. (Zitiert auf Seite 92.)

[Kan18b] Kantara Initiative: *Identity Assurance Framework: NIST SP 800-63B Service Assessment Criteria*. KIAF-1440, Kantara Initiative, 2018. `https://kantarainitiative.org/identity-assurance-framework`. (Zitiert auf Seite 93.)

[Kan19a] Kantara Initiative: *Controlling Documents. Identity Assurance Framework*. Technischer Bericht, Kantara Initiative, 2019. `https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework`. (Zitiert auf Seite 92.)

[Kan19b] Kantara Initiative: *Identity Assurance Framework: NIST SP 800-63A Service Assessment Criteria*. KIAF-1430, Kantara Initiative, 2019. `https://kantarainitiative.org/identity-assurance-framework`. (Zitiert auf Seite 93.)

[Kan19c] Kantara Initiative: *Kantara Classic*. `https://kantarainitiative.org/trustoperations/kantara-classic/`, 2019. [Online; abgerufen am 27.08.2019]. (Zitiert auf Seite 92.)

[Kan20] Kantara Initiative: *Operational -63r2 Service Assessment Criteria - Version 1.1.0*. KIAF-1420, Kantara Initiative, 2020. `https://kantarainitiative.org/identity-assurance-framework`. (Zitiert auf Seite 92.)

[Kaw17] Takahiko Kawasaki: *Diagrams of All The OpenID Connect Flows*. `https://darutk.medium.com/diagrams-of-all-the-openid-connect-`

flows-6968e3990660, 2017. [Online, abgerufen am 29.10.2021]. (Zitiert auf den Seiten 60 und 61.)

[KCM+05] John Kemp, Scott Cantor, Prateek Mishra, Rob Philpott und Eve Maler: *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, OASIS, 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf. (Zitiert auf den Seiten 23, 55, 117 und 118.)

[KFI10] Tadashi Kaji, Takahiro Fujishiro und Shinichi Irube: *IdP proxy for combined authentication based on multiple IdPs*. In: *2010 IEEE 4th International Symposium on Advanced Networks and Telecommunication Systems*, Seiten 34–36. IEEE, 2010. (Zitiert auf Seite 83.)

[Kim05] Kim Cameron: *The Laws of Identity*. https://ldapwiki.com/attach/The%20Seven%20Laws%20Of%20Identity/TheLawsOfIdentity.pdf, 2005. [Online; abgerufen am 06.04.2020]. (Zitiert auf Seite 50.)

[KVB09] Dmitri Kuksov und J. Miguel Villas-Boas: *When More Alternatives Lead to Less Choice*. Marketing Science, 29(3):507–524, 2009. (Zitiert auf Seite 96.)

[Laa17] Kari Laalo: *Haka MFA*. https://wiki.eduuni.fi/display/CSCHAKA/2017/09/12/Haka+Multifactor+Authentication+presentation+in+NTW2017, 2017. Presentation at NTW2017. [Online; abgerufen am 27.09.2021]. (Zitiert auf Seite 82.)

[LAB+18] M. Linden, P. Axelsson, A. Buxey, T. Barton und D. Langenberg: *REFEDS Assurance Framework*. https://doi.org/10.5281/zenodo.5113658, 2018. [Online; abgerufen am 18.08.2021]. (Zitiert auf den Seiten 114, 141, 165 und 170.)

[LDA17] LDAP wiki: *Multiple-channel Authentication*. https://ldapwiki.com/wiki/Multiple-channel%20Authentication, 2017. [Online; abgerufen am 28.05.2020]. (Zitiert auf Seite 75.)

[LDA18] LDAP wiki: *Federated Identity*. https://ldapwiki.com/wiki/Federated%20Identity, 2018. [Online; abgerufen am 16.02.2021]. (Zitiert auf Seite 51.)

[LDA19] LDAP wiki: *Level of Assurance*. https://ldapwiki.com/wiki/Level%20Of%20Assurance, 2019. [Online; abgerufen am 16.02.2021]. (Zitiert auf Seite 88.)

[Lei19] Leibniz-Rechenzentrum: *IT-Dienstleistungen am LRZ: Effizient und serviceorientiert*. https://www.lrz.de/presse/ereignisse/2019-10-01_lrz_iso_zertifiziert/, 2019. [Online; abgerufen am 12.04.2021]. (Zitiert auf Seite 173.)

[Lei21] Leibniz-Rechenzentrum: *Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften*. https://www.lrz.de/, 2021. [Online; abgerufen am 04.10.2021]. (Zitiert auf Seite 15.)

[LGP+15] Mikael Linden, David Groep, Daniela Pöhn, Tangui Coulouarn, Wolfgang Pempe und Hannah Short: *Milestone MNA3.1: Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases.* MNA3.1, AARC Project, 2015. `https://aarc-project.eu/wp-content/uploads/2015/11/MNA31-Minimum-LoA-level.pdf`. (Zitiert auf den Seiten 25 und 33.)

[Lin09] Mikael Linden: *Organisational and Cross-Organisational Identity Management.* Dissertation, Tampere University of Technology, 2009. (Zitiert auf Seite 11.)

[Lin19] Mikael Linden: *User Instructions for Multi-Factor Authentication. ELIXIR AAI task.* `https://docs.google.com/document/d/16ObOsMhPTMBVfIKJzbBZvJMhtRI2ZKTf_1gSoCMQXAM`, 2019. [Online; abgerufen am 16.05.2020]. (Zitiert auf Seite 176.)

[LMZT20] Alan Lewis, Branko Marović, Jule Ziegler und Miika Tuisku: *Identity Verification for Research and Education.* Stakeholder Report, GÉANT Project, 2020. `https://wiki.geant.org/download/attachments/148083033/Stakeholder%20Report%20on%20Identity%20Verification%20for%20R%26E_v1.pdf?api=v2`. (Zitiert auf den Seiten 207 und 213.)

[Men19] Mentorium: *Forschungsstand verfassen.* `https://www.mentorium.de/forschungsstand-verfassen/`, 2019. [Online; abgerufen am 10.08.2021]. (Zitiert auf Seite 104.)

[Miz19] Maximilian M. Mizani: *Evaluation von Systemen zur Mehr-Faktor-Authentifizierung am Beispiel des Leibniz-Rechenzentrums.* Bachelorarbeit, Ludwig-Maximilians-Universität München, 2019. (Zitiert auf Seite 20.)

[MPM05] Prateek Mishra, Rob Philpott und Eve Maler: *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, OASIS, 2005. `http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf`. (Zitiert auf Seite 55.)

[MyA19] MyAcademicID: *MyAcademicID Webseite.* `https://myacademic-id.eu/`, 2019. [Online; abgerufen am 18.01.2021]. (Zitiert auf Seite 214.)

[Nak08] Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System.* `https://bitcoin.org/bitcoin.pdf`, 2008. [Online; abgerufen am 18.01.2021]. (Zitiert auf Seite 214.)

[Nat17] National Institute of Standards and Technology: *Digital Identity Guidelines.* `https://pages.nist.gov/800-63-3/`, 2017. [Online, abgerufen am 23.08.2019]. (Zitiert auf Seite 89.)

[net20] netgo: *LinOTP.* `https://www.linotp.org/`, 2020. [Online; abgerufen am 04.08.2021]. (Zitiert auf Seite 80.)

[Net21] NetKnights: *privacyID3A.* `https://www.privacyidea.org/`, 2021. [Online; abgerufen am 04.08.2021]. (Zitiert auf den Seiten 66 und 80.)

[OL01] Dave Orchard und Hal Lockhart: *SAML Domain Model*. Technischer Bericht, OASIS, 2001. `https://www.oasis-open.org/committees/security/docs/draft-sstc-use-domain-05.pdf`. (Zitiert auf Seite 54.)

[Ope21a] OpenID: *eKYC & Identity Assurance WG*. `https://openid.net/wg/ekyc-ida/`, 2021. [Online; abgerufen am 24.02.2021]. (Zitiert auf Seite 29.)

[Ope21b] OpenID Foundation: *OpenID Connect*. `https://openid.net/connect/`, 2021. [Online, abgerufen am 29.10.2021]. (Zitiert auf Seite 60.)

[Ora10] Oracle Corporation: *Sun Java System Access Manager 7.1 Federation and SAML Administration Guide*. `https://docs.oracle.com/cd/E19462-01/819-4674/index.html`, 2010. [Online; abgerufen am 22.02.2021]. (Zitiert auf Seite 54.)

[Oro21] Thomas Orozco: *APT Browse: libapache2-mod-auth-openidc*. `https://www.apt-browse.org/browse/debian/jessie/main/amd64/libapache2-mod-auth-openidc/1.6.0-1/file/etc/apache2/mods-available/auth_openidc.conf`, 2021. [Online; abgerufen am 14.08.2021]. (Zitiert auf Seite 198.)

[Pau21] Paul M. Jones (Editor): *PHP Standards Recommendations. PSR-4: Autoloader*. `https://www.php-fig.org/psr/psr-4/`, 2021. [Online; abgerufen am 27.11.2021]. (Zitiert auf Seite 195.)

[Pöh16] Daniela Pöhn: *Architektur und Werkzeuge für dynamisches Identitätsmanagement in Föderationen*. Dissertation, Ludwig-Maximilians-Universität München, 2016. (Zitiert auf den Seiten 2, 11, 57 und 69.)

[PP01] Darren Platt und Evan Prodromou: *Oasis Security Services Use Cases and Requirements*. Consensus Draft 1, OASIS, 2001. `https://www.oasis-open.org/committees/security/docs/draft-sstc-saml-reqs-01.pdf`. (Zitiert auf Seite 54.)

[PVWB+20] Sean Peisert, Andrew A. Von Welch, RuthAnne Bevier, Michael Dopheide, Rich LeDuc, Pascal Meunier, Steve Schwab und Karen Stocks: *Open Science Cyber Risk Profile (OSCRP)*. Technischer Bericht, Trusted CI, 2020. (Zitiert auf den Seiten 123, 174 und 175.)

[REF17] REFEDS: *REFEDS MFA Profile*. `https://refeds.org/profile/mfa`, 2017. [Online; abgerufen am 12.09.2019]. (Zitiert auf den Seiten 115, 117, 119, 141, 165, 169 und 210.)

[REF18a] REFEDS: *REFEDS Assurance Framework*. `https://refeds.org/assurance`, 2018. [Online; abgerufen am 12.09.2019]. (Zitiert auf den Seiten 114, 141, 165, 170 und 178.)

[REF18b] REFEDS: *REFEDS RAF final report*. `https://wiki.refeds.org/display/GROUPS/RAF+pilot+final+report`, 2018. [Online; abgerufen am 07.12.2018]. (Zitiert auf den Seiten 185 und 198.)

[REF18c] REFEDS: *REFEDS Single Factor Authentication Profile*. `https://refeds.org/profile/sfa`, 2018. [Online; abgerufen am 12.09.2019]. (Zitiert auf den Seiten 9, 25, 114, 117, 119, 141, 165, 166, 167, 210 und 225.)

[REF18d] REFEDS: *REFEDS Wiki Consultation: REFEDS SFA Profile*. `https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+SFA+Profile`, 2018. [Online; abgerufen am 12.11.2020]. (Zitiert auf den Seiten 186 und 222.)

[REF20a] REFEDS: *REFEDS Assurance Working Group*. `https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group`, 2020. [Online; abgerufen am 12.11.2020]. (Zitiert auf den Seiten 114 und 130.)

[REF20b] REFEDS: *REFEDS Federations Map*. `https://refeds.org/federations/federations-map`, 2020. [Online; abgerufen am 12.11.2020]. (Zitiert auf Seite 184.)

[REF20c] REFEDS: *REFEDS Wiki Consultation Home*. `https://wiki.refeds.org/display/CON/Consultations+Home`, 2020. [Online; abgerufen am 12.11.2020]. (Zitiert auf Seite 184.)

[REF21] REFEDS: *MFA Profile FAQ*. `https://wiki.refeds.org/display/PRO/MFA+Profile+FAQ`, 2021. [Online; abgerufen am 04.12.2021]. (Zitiert auf Seite 196.)

[Rei08] Helmut Reiser: *Ein Framework für föderiertes Sicherheitsmanagement*. Habilitation, Ludwig-Maximilians-Universität München, 2008. (Zitiert auf den Seiten 3, 10 und 15.)

[RHP+08] Nick Ragouzis, John Hughes, Rob Philpott, Eve Maler, Paul Madsen und Tom Scavo: *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. Committee Draft 02, OASIS, 2008. `http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf`. (Zitiert auf den Seiten 18, 55, 56 und 127.)

[RJ18] Justin Richer und Leif Johansson: *Vectors of Trust*. RFC 8485, RFC Editor, 2018. `https://rfc-editor.org/rfc/rfc8485.txt`. (Zitiert auf den Seiten 34 und 93.)

[RRWS00] Allan Rubens, Carl Rigney, Steve Willens und William A. Simpson: *Remote Authentication Dial In User Service (RADIUS)*. RFC 2865, RFC Editor, 2000. `https://www.rfc-editor.org/info/rfc2865`. (Zitiert auf Seite 39.)

[SBJ14a] N. Sakimura, J. Bradley und M. Jones: *OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 1*. Final Specification, OpenID Foundation, 2014. `https://openid.net/specs/openid-connect-registration-1_0.html`. (Zitiert auf den Seiten 62 und 63.)

[SBJ+14b] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros und C. Mortimore: *OpenID Connect Core 1.0 incorporating errata set 1*. Final Specification, OpenID Foundation, 2014. `https://openid.net/specs/openid-connect-core-1_0.html`. (Zitiert auf den Seiten 18, 29, 54, 60, 61, 117, 118 und 198.)

[SBJJ14] N. Sakimura, J. Bradley, M. Jones und E. Jay: *OpenID Connect Discovery 1.0 incorporating errata set 1.* Final Specification, OpenID Foundation, 2014. `https://openid.net/specs/openid-connect-discovery-1_0.html`. (Zitiert auf den Seiten 62, 133 und 199.)

[SCS15] Yogendra Shah, Vinod Choyi und Lakshmi Subramanian: *Multi-factor Authentication as a Service.* In: *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, Seiten 144–150. IEEE, 2015. (Zitiert auf Seite 81.)

[Shi07] Robert W. Shirey: *Internet Security Glossary, Version 2.* RFC 4949, RFC Editor, 2007. `https://rfc-editor.org/rfc/rfc4949.txt`. (Zitiert auf den Seiten 51, 71 und 72.)

[Shi21] Shibboleth Consortium: *Shibboleth Software.* `https://www.shibboleth.net/`, 2021. [Online; abgerufen am 04.08.2021]. (Zitiert auf den Seiten 65 und 81.)

[SLV+18] Mischa Salle, Nicolas Liampotis, Davide Vaghetti, Christos Kanellopoulos, Mikael Linden, Shiraz Memon, David Hübner, Alessandro Paolini, Nils van Dijk, Uros Stevanovic, Marcus Hardt und Peter Solagna: *Guidelines on stepping up the authentication component in AAIs implementing the AARC BPA.* AARC-G029, AARC2 Project, 2018. `https://aarc-project.eu/wp-content/uploads/2018/05/AARC-G029_Guidelines-on-Step-Up-Authentication.pdf`. (Zitiert auf Seite 27.)

[SUN21] SUNET: *eduID.* `https://eduid.se/en/`, 2021. [Online; abgerufen am 18.01.2021]. (Zitiert auf den Seiten 53 und 214.)

[SUN22] SUNET: *SUNET Webseite.* `https://www.sunet.se/`, 2022. [Online; abgerufen am 06.02.2022]. (Zitiert auf Seite 198.)

[SUR21a] SURF: *eduID.* `https://eduid.nl/`, 2021. [Online; abgerufen am 18.01.2021]. (Zitiert auf den Seiten 53 und 214.)

[SUR21b] SURF: *OpenConext: Stepup.* `https://openconext.org/stepup/`, 2021. [Online; abgerufen am 27.09.2021]. (Zitiert auf Seite 83.)

[SUR21c] SURF: *SURFsecureID.* `https://wiki.surfnet.nl/display/SsID/SURFsecureID`, 2021. [Online; abgerufen am 27.09.2021]. (Zitiert auf Seite 83.)

[Swa90] John M. Swales: *Genre Analysis: English in Academic and Research Settings.* Cambridge University Press, 1990. (Zitiert auf Seite 104.)

[SWI21a] SWITCH: *Swiss edu-ID: the academic identity made in Switzerland.* `https://projects.switch.ch/eduid/`, 2021. [Online; abgerufen am 18.01.2021]. (Zitiert auf den Seiten 53 und 214.)

[SWI21b] SWITCH: *WAYF Service.* `https://www.switch.ch/aai/support/tools/wayf/`, 2021. [Online; abgerufen am 27.11.2021]. (Zitiert auf Seite 192.)

[Tel20a] Telemanagement Forum: *Business Process Framework (eTOM).* Technischer Bericht, Telemanagement Forum, 2020. (Zitiert auf Seite 100.)

[Tel20b] Telemanagement Forum: *Information Framework (SID).* Technischer Bericht, Telemanagement Forum, 2020. (Zitiert auf Seite 100.)

[Uni21] Uninett: *SimpleSAMLphp Software.* `https://simplesamlphp.org/`, 2021. [Online; abgerufen am 04.08.2021]. (Zitiert auf den Seiten 65, 66, 195 und 197.)

[vdM17] Pieter van der Meulen: *Step-up authentication and the art of creative SAML proxying.* `https://tnc17.geant.org/core/presentation/44.html`, 2017. Conference Talk at TNC17. [Online, abgerufen am 15.1.2022]. (Zitiert auf Seite 83.)

[VELL+18] Davide Vaghetti (Editor), Mikael Linden, Nicolas Liampotis, David Hübner und Jens Jensen: *Guidelines for the evaluation and combination of the assurance of external identities.* AARC-G031, AARC2 Project, 2018. `https://doi.org/10.5281/zenodo.1308682`. (Zitiert auf Seite 27.)

[WE03] Thomas Wason (Editor): *Liberty ID-FF Architecture Overview. Version 1.2.* Technischer Bericht, Liberty Alliance Project, 2003. `https://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf`. (Zitiert auf Seite 54.)

[Wik21] Wikipedia: *GAFAM.* `https://de.wikipedia.org/wiki/GAFAM`, 2021. [Online; abgerufen am 22.01.2021]. (Zitiert auf Seite 209.)

[Win05] Phillip J. Windley: *Digital Identity: Unmasking Identity Management Architecture (IMA).* O'Reilly, 2005. (Zitiert auf Seite 1.)

[Wor22] World Health Organization: *Coronavirus disease (COVID-19) pandemic.* `https://www.who.int/emergencies/diseases/novel-coronavirus-2019`, 2022. [Online; abgerufen am 15.01.2022]. (Zitiert auf Seite 209.)

[YM08] Noson S. Yanofsky und Mirco A. Mannucci: *Quantum Computing For Computer Scientists.* Cambridge University Press, 2008. (Zitiert auf Seite 214.)

[Yub21] Yubico: *Der YubiKey.* `https://www.yubico.com/der-yubikey/?lang=de/`, 2021. [Online; abgerufen am 22.01.2022]. (Zitiert auf Seite 74.)

[Zac19] Ludwig Zacherl: *Eine SAML-basierte Testumgebung für föderiertes Identitätsmanagement.* Bachelorarbeit, Ludwig-Maximilians-Universität München, 2019. (Zitiert auf den Seiten 191 und 192.)

[Zie17] Jule Ziegler: *REFEDS MFA Profile.* `https://doi.org/10.5281/zenodo.5113296`, 2017. [Online; abgerufen am 18.08.2021]. (Zitiert auf den Seiten 117, 119, 141, 165, 169 und 210.)

[Zie18] Jule Ziegler: *REFEDS SFA Profile.* `https://doi.org/10.5281/zenodo.5113499`, 2018. [Online; abgerufen am 18.08.2021]. (Zitiert auf den Seiten 9, 25, 114, 117, 119, 141, 165, 166, 167, 210 und 225.)

[ZS18] Jule A. Ziegler und David Schmitz: *Establishing a Universal Model for Authentication Scenarios based on MNM Service Model.* In: *11. DFN-Forum Kommunikationstechnologien*, Seiten 81–91. Gesellschaft für Informatik e.V., 2018. (Zitiert auf den Seiten 9, 39, 40, 101, 136, 143, 146, 147, 148, 149, 151 und 222.)

[ZSG+21a] Jule A. Ziegler, Uros Stevanovic, David Groep, Ian Neilson, David P. Kelsey und Maarten Kremers: *Making Identity Assurance and Authentication Strength Work for Federated Infrastructures.* In: *International Symposium on Grids & Clouds 2021.* PoS, 2021. (Zitiert auf den Seiten 10, 123, 171, 172, 173, 174, 175, 176, 177 und 222.)

[ZSG+21b] Jule A. Ziegler, Uros Stevanovic, David Groep, Ian Neilson, David P. Kelsey und Maarten Kremers: *Preprint. Making Identity Assurance and Authentication Strength Work for Federated Infrastructures.* `https://doi.org/10.5281/zenodo.4916049`, 2021. [Online, abgerufen am 15.1.2022]. (Zitiert auf Seite 10.)

[ZSL19] Jule A. Ziegler, Michael Schmidt und Mikael Linden: *Improving Identity and Authentication Assurance in Research & Education Federations.* In: *Security and Trust Management. 15th International Workshop. STM 2019*, Seiten 1–18. Springer, 2019. (Zitiert auf den Seiten 9, 24, 25, 34, 114, 141, 166, 167, 171, 184, 185, 198, 210 und 225.)

[ZvD18] Jule A. Ziegler und Niels van Dijk: *Evaluation of possible LS AAI pilot solutions and formal recommendation.* `https://docs.google.com/document/d/12j9VTXmQq402AE5oY1qZH1Pm_XazxgWN-1aRwh_alHk`, 2018. [Online; abgerufen am 16.05.2020]. (Zitiert auf Seite 27.)