eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)

Name	Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)
Standard-Nummer	eCH-0107
Kategorie	Standard (neu)
Reifegrad	definiert; experimentell; implementiert; verbreitet
Version	3.0
Status	Genehmigt; ausser Kraft
Genehmigt am	
Ausgabedatum	2013-12-04
Ersetzt Version	2.0
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Beilagen	--
Autoren	Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Marc Kunz, BFH TI, marc.kunz@bfh.ch Thomas Kessler, Temet, thomas.kessler@temet.ch Torsten Gruoner, ISB, torsten.gruoner@isb.admin.ch Marc Heerkens, ISB, marc.heerkens@isb.admin.ch eCH Fachgruppe IAM V2.0: Ronny Bernold, BFH FBW, ronny.bernold@bfh.ch Gerhard Hassenstein, BFH TI, gerhard.hassenstein@bfh.ch Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Martin Topfel, BFH FBW, martin.topfel@bfh.ch eCH Fachgruppe IAM V1.0: Willy Müller, ISB, willy.mueller@isb.admin.ch Hans Häni, AFT TG SEAC-Projektgruppe IAM
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Das vorliegende Dokument definiert die Prinzipien, die Regeln und den Ordnungsrahmen für die IAM-Systemgestaltung, welche beim Bereitstellen von föderierten IAM-Lösungen im föderalen E-Government Schweiz berücksichtigt werden müssen. Das Gestaltungsprinzip definiert eine modellhafte IAM-Landschaft in organisationsübergreifenden Applikationsszenarien für bestehende und neue Anwendungen. Dabei wird davon ausgegangen, dass Prozesse und Geschäftsservices durch die Anforderungen der verschiedenen Stakeholder motiviert und durch die definierten Rollen verteilt erbracht resp. genutzt werden können. Der Standard spezifiziert die Anforderungen, die Stakeholder und Rollen, die Prozesse, die Informationsarchitektur und die Geschäftsservices. Des Weiteren werden Aspekte des Schutzes der Privatsphäre und die Auswirkungen der Ausdehnung des IAMs auf das Internet of Things diskutiert.
Der Standard kann in allen E-Society-Bereichen angewendet werden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Status des Dokuments

Das vorliegende Dokument wurde vom Expertenausschuss ***genehmigt.*** Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

2 Einleitung

2.1 Überblick

Die Nutzung des Internets hat in den letzten Jahren kontinuierlich zugenommen. Immer häufiger wird das Internet nicht nur als Informationsquelle, sondern auch zum Tätigen von Geschäften verwendet.

Internetbasierte Geschäftsprozesse setzen vertrauenswürdige Subjekte und damit verbundenes Wissen um die Handlungspartner voraus. Entsprechende Dienste wurden bisher erfolgreich durch die organisationsinterne Identitäts- und Zugriffsverwaltung (*Identity and Access Management, IAM*) gewährleistet. In organisationsübergreifenden Anwendungsfällen trifft das interne IAM aber auf seine Grenzen: es kann nicht oder nur durch hohen Aufwand über mehrere Domänen hinweg verwendet werden. Der hier vorliegende Standard definiert die Aufgaben und Design-Prinzipien für die Gestaltung von föderierten IAM-Systemen im E-Government, damit die genannte Grenze überwunden werden kann. Sie sind beim Bereitstellen von Lösungen im E-Government Schweiz zu berücksichtigen, damit lokale Anwendungen und Dienste organisationsübergreifend genutzt werden können. Der Standard dient als Grundlage für alle, welche im E-Government-Umfeld Lösungen entwerfen, die potentiell oder bereits aktuell für extern Zugreifende bereitgestellt werden (Internet-eServices).

Im E-Government-Umfeld geht es, wie im gesamten E-Society-Kontext (E-Government, E-Health, E-Economy), vereinfacht darum, dass *Subjekte* (Verwaltungen, Bürger, Organisationen, Firmen, spezifische Applikationen) *Ressourcen* (Services der Gemeinden, der Kantone, des Bundes oder Dritter) verwenden möchten. Eine besondere Herausforderung ist die Tatsache, dass *E-Ressourcen* und *E-Identities* sich in unterschiedlichen *Domänen* befinden können.

2.1.1 Einführung IAM

Die Kernelemente eines *IAM* sind für das Verständnis des Standards essentiell und werden daher in diesem Abschnitt kurz erläutert. Die in diesem Dokument verwendeten Begrifflichkeiten entstammen dem IAM-Glossar (eCH-0219 [1]) und sind kursiv markiert.

In der nachfolgenden Abbildung 1 werden die Kernelemente des IAM dargestellt. Im Zentrum aller IAM-Bemühungen steht, dass der Zugriff eines *Subjekts* auf eine schützenswerte *Ressource* kontrolliert erfolgt.

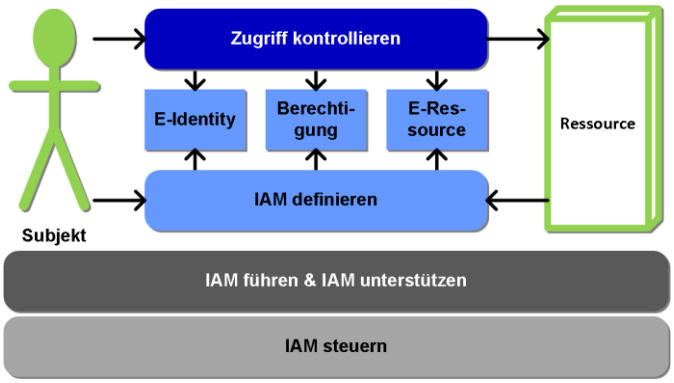


Abbildung 1 IAM im Überblick

Die Elemente *Zugriff kontrollieren* und *IAM definieren* stellen die Kernprozesse dar, welche vom *Subjekt* und der *Relying Party* genutzt werden. Diese Kernprozesse werden zu unterschiedlichen Zeitpunkten verwendet, welche durch die hellblaue und dunkelblaue Farbe (Farbverwendung siehe Tabelle 1) symbolisiert werden.

hellgrau	Hellgrau visualisiert sind diesem Dokument für Elemente, die standardisierenden Charakter haben und Leitplanken bieten bzw. definieren.
dunkelgrau	Dunkelgrau visualisiert in diesem Dokument Elemente, die bereits vor der Definitionszeit und während der gesamten Lebensdauer des IAM-Systems aktiv sind (z. B. unterstützende Prozesse wie Führung oder Support).
hellblau	Die hellblaue Farbe wird in diesem Dokument konsequent für die Definitionszeit verwendet, während der alle Informationen den Informationselementen zugeordnet (also definiert) werden.
dunkelblau	Die dunkelblaue Farbe wird durchgehend für die Laufzeit verwendet. Zur Laufzeit wird der Zugriff basierend auf den definierten Informationselementen kontrolliert (gewährt oder abgelehnt).
hellgrün	Die hellgrüne Farbe wird in diesem Dokument konsequent für Realweltobjekte verwendet.

Tabelle 1 Farbverwendung im Dokument

Subjekt und *Ressource* sind Realweltobjekte, die ihre Ziele mit Hilfe der IAM-Prozesse erreichen. Das Ziel des *Subjekts* ist der Zugriff auf die gewünschte *Ressource*. Das Ziel der *Ressource* ist, sich vor unberechtigten Zugriffen auf Informationen und Services zu schützen.

Damit die Kernprozesse auch in der digitalen Welt funktionieren, werden den Objekten der Realwelt (*Subjekt*, *Ressource*) digitale Abbildungen, sogenannte Informationselemente, zugeordnet. Zum *Subjekt* (grün) wird die *E-Identity* (hellblau) und der *Ressource* (grün) die *E-Ressource* (hellblau) zugeordnet. Die *Ressource* legt zur Umsetzung ihrer Ziele im Informationselement *Berechtigung* (*Zugangsregel/Zugriffsrecht*) fest, welche *E-Identity* unter welchen Bedingungen auf welche *Ressource* zugreifen darf.

Der Prozess IAM steuern umfasst alle Aktivitäten für die Definition der notwendigen Vorgaben und Rahmenbedingungen. Der Prozess IAM führen & unterstützen umfasst die Führung für die Implementierung und den Betrieb einer IAM-Umgebung, sowie Aktivitäten zum Aufnehmen, Verwalten, Verfolgen und schlussendlichen Lösen von Problemen (Support).

2.1.2 Anwendungsgebiet

Die Vision der Vernetzten Verwaltung und die damit verbundenen übergreifenden Prozesse im schweizerischen E-Government bedingen eine über Organisationsgrenzen hinweggreifende *Identitäts- und Berechtigungsverwaltung*. Der vorliegende Standard eCH-0107 bildet die Basis der IAM-Standardisierung. Dabei werden die Definitionen und Begriffe aus dem eCH-0122 [2], der die Architektur des E-Government Schweiz beschreibt, zu Grunde gelegt.

Der eCH-0107 definiert Grundprinzipien, Anforderungen, Prozesse und Geschäftsservices für die IAM-Systemgestaltung, welche beim Bereitstellen von organisationsübergreifenden IAM-Lösungen im föderalen E-Government Schweiz zu berücksichtigen sind, damit lokale Anwendungen organisationsübergreifend genutzt werden können.

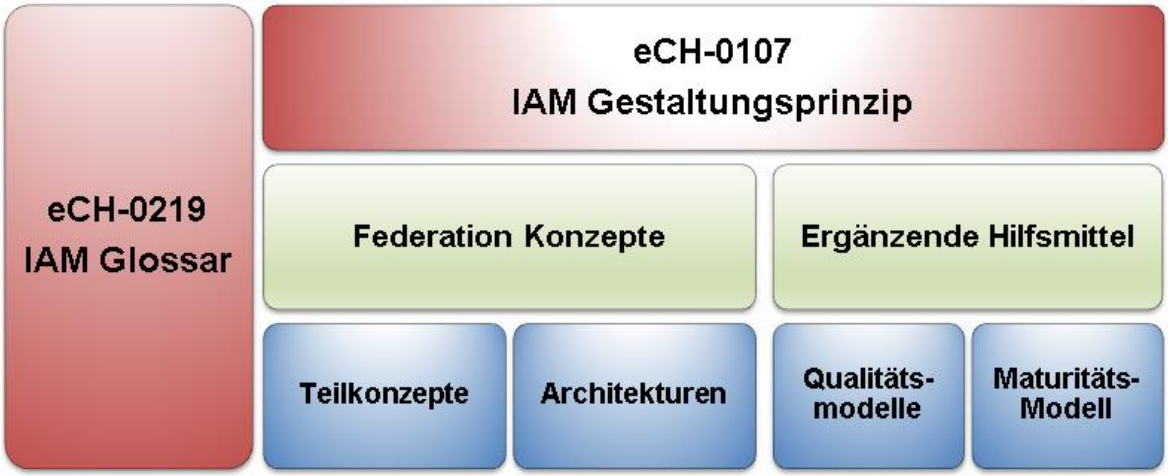


Abbildung 2 Einordnung des eCH-0107 Standards

Unter dem Standard eCH-0107 positionieren sich die Konzepte für föderierte IAM-Lösungen und ergänzende Hilfsmittel. Im IAM Glossar (eCH-0219 [1]) sind Begriffe definiert, die für alle eCH-Standards im Bereich IAM gültig sind. Die Konzepte sind konkrete Beschreibungen, wie ein IAM-Lösungsvorschlag aussieht, und beinhalten Teilkonzepte und Architekturen, die für die Umsetzung berücksichtigt werden müssen. Daneben werden den Konzepten Hilfsmittel zur Seite gestellt, die ergänzende Informationen zur Verfügung stellen und die für mehr als ein Konzept relevant sind. Die dargestellten Qualitäts- und Maturitätsmodelle sind Beispiele für Hilfsmittel und sind nicht abschliessend.

2.1.3 Föderiertes IAM

Im Unterschied zum organisationsinternen IAM geht das *föderierte IAM* von organisationsübergreifenden *E-Identities* und deren organisationsübergreifender Nutzung aus.

Die *E-Identity* für ein *Subjekt* wird in der *Domäne* A erstellt, kann aber auch Informationen aus einer *Domäne* B besitzen und zum Zugriff auf Ressourcen einer Domäne C verwendet werden.

Damit ein *föderiertes IAM* etabliert werden kann, müssen sich die verschiedenen *Domänen* in Bezug auf bestimmte Aspekte gegenseitig vertrauen. Dieses Vertrauen stützt sich auf explizite und implizite Vereinbarungen ab.

Beim *föderierten IAM*, im Gegensatz zum replizierenden IAM (siehe [1]), im E-Government stellen Behörden Ressourcen den Subjekten ihren internen (andere Behörden der Schweiz) oder externen Partnern (Personen, Unternehmen, Organisationen oder Behörden anderer Staaten) zur Verfügung, mit denen definierte Leistungen aus dem Bereich ihrer Zuständigkeit online verfügbar gemacht werden. Diese Ressourcen sollen für Subjekte der eigenen Domäne(n) und für Subjekte mit E-Identities anderer Domänen zugreifbar sein. Eine Behörde kann somit Relying Party aber auch u.U. gleichzeitig IAM-Dienstanbieter sein.

2.1.4 Abgrenzung

Die Gestaltungsprinzipien und Regeln in diesem Standard stellen den Ordnungsrahmen für *föderierte IAM*-Systeme dar. Es werden die Kernelemente (Prozesse und Services) und die wichtigsten Stakeholder und Rollen genannt und erklärt. Ausserdem werden die verschiedenen Typologien von föderierten IAM-Systemen eingeführt. Die Orchestrierung und die konkrete Umsetzung der Lösungsvorschläge werden jedoch in den jeweiligen Konzepten thematisiert und in diesem Standard nicht berücksichtigt.

Generell werden in diesem Dokument nur IAM-Systeme berücksichtigt, die den Zugriff auf **schützenswerte Ressourcen** kontrollieren. Der Zugriff auf *öffentliche* oder *versteckte Ressourcen* ist nicht Teil dieses Standards.

IAM ist eines der Mittel, um wichtige Sicherheitsziele zu erreichen. Entsprechend haben IAM-Lösungen selber die für sie geltenden, häufig hohen Sicherheitsanforderungen zu erfüllen. Diese sind in einschlägigen Sicherheitsstandards beschrieben und werden in diesem Standard nicht nochmals aufgeführt.

2.1.5 Vorteile

Im Umfeld des föderierten *IAM* wurden seit der Version 1 des eCH-0107 Standards wesentliche Fortschritte erzielt, welche bereits in der zweiten Version des Standards dokumentiert und definiert wurden. Die Version 3.0 erweitert und korrigiert die Aussagen aus der zweiten Version.

Dieser Standard erzielt folgende Vorteile:

- Die Kernelemente eines föderierten *IAM* sind bekannt und stellen die Grundlage dar, um Lösungsideen und -vorschläge zu erarbeiten.
- Eine modellhafte *IAM*-Landschaft (Stakeholder, Rollen, Prozesse, Informationsmodell, Geschäftsservices) im organisationsübergreifenden Anwendungsszenario ist definiert.
- Die generellen Anforderungen an föderierte *IAM*-Systeme und die Anforderungen der wichtigsten Stakeholder sind definiert.
- Mögliche Konzepte für Identity Federations sind dargestellt.

- Die Auswirkungen auf das IAM bei Ausdehnung des Wirkungsbereiches auf das Internet of Things werden diskutiert.
- Neu hinzugekommen sind verschärfte Anforderungen zum Schutz der Privatsphäre des Subjektes.

2.2 Schwerpunkte

Der vorliegende Standard eCH-0107 unterteilt sich neben der Einführung in sieben Kapitel, die nachfolgend kurz beschreiben werden.

Kapitel 3 identifiziert die wichtigsten Rollen und Stakeholder sowie ihre Beziehung zueinander in einem *föderierten IAM*.

In Kapitel 4 werden die Grundprinzipien und die allgemeinen Anforderungen an ein föderiertes IAM-System sowie die Anforderungen aller Stakeholder beschrieben.

Kapitel 5 zeigt die Informationsarchitektur und erklärt die einzelnen Elemente. Mit Hilfe der Informationsarchitektur werden die Realweltobjekte über die Semantik den Schnittstellenobjekten zugeordnet.

Im Kapitel 6 werden die Prozesse definiert, welche für alle Stakeholder wichtig sind. Dies bedeutet, dass nicht nur die Prozesse von *IAM-Dienstanbietern* berücksichtigt werden, sondern auch die der IAM-Nutzer.

In Kapitel 7 werden die Services in einem föderierten *IAM* aus Geschäftssicht dargestellt und deren Aufgaben und Schnittstellen definiert.

Kapitel 8 beschreibt die Auswirkungen auf ein IAM-System, wenn dieses auf das Internet of Things ausgeweitet wird und daher auch die Authentifikation und Autorisierung von Dingen mit einbezogen werden.

Kapitel 9 beschreibt Anforderungen zum Schutz der Privatsphäre des Leistungsbezügers (Subjekt), die über die Anforderungen in Kapitel 4.3.1 hinausgehen. Des Weiteren werden Richtlinien zur Verwaltung und Verarbeitung von subjektbezogenen Daten gegeben.

Anhang E stellt die Varianten, ein föderiertes *IAM* aufzubauen, dar.

2.3 Normativer Charakter der Kapitel

Die Kapitel des vorliegenden Standards sind von normativem oder auch deskriptivem Charakter. Die untenstehende Tabelle veranschaulicht diese Einordnung:

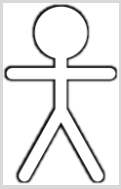
Kapitel	Beschreibung
1 Status des Dokuments	Deskriptiv
2 Einleitung	Deskriptiv
3 Rollen und Stakeholder	Normativ
4 Anforderungen	Normativ
5 Informationsarchitektur	Normativ
6 Prozesse	Die Benennungen und deren Definition sind normativ und die Tätigkeiten und Anmer-

	kungen deskriptiv.
7 Geschäftsservices	Die Benennung und deren Definition sind normativ und die Aufgaben und Anmerkungen deskriptiv.
7.6 Zuordnung Service zu Informationselemente	Normativ
7.7 Zuständigkeiten für Geschäftsservices	Deskriptiv
8 IAM für das IoT	Deskriptiv
9 Privacy	Deskriptiv
Anhang A – Referenzen & Bibliografie	Deskriptiv
Anhang B – Mitarbeiter & Überprüfung	Deskriptiv
Anhang C – Abkürzungen	Normativ
Anhang D – Glossar	Normativ
Anhang E – Identity Federation Modelle	Deskriptiv
Anhang F – Änderungen gegenüber Version 2.00	Deskriptiv

Tabelle 2 Übersicht des normativen Charakters der Kapitel

3 Rollen und Stakeholder

Ein Identity und Access Management System kennt sechs unterschiedliche Rollen, die je nach Kombination und Ausgestaltung von fünf grundlegenden Stakeholdern motiviert werden.



Rolle

Eine Rolle beschreibt Aufgabe und Zweck einer Entität in einer Föderation und führt die Prozesse aus. Eine Rolle in einem IAM-System wird durch einen oder mehrere Stakeholder motiviert.

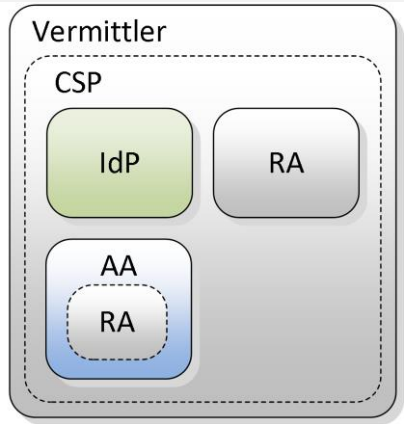
Stakeholder

Die Stakeholder sind Realweltobjekte, d.h. Personen, Gruppen von Personen oder Organisationen, die gemeinsame Interessen im IAM haben. Ein Stakeholder hat einen (oder mehrere) Stake(s) und hat einen Willen.

Stakeholder haben Anforderungen (siehe Kapitel 4) an die verschiedenen Rollen in einem IAM-System.

3.1 Rollen in IAM

Die verschiedenen Rollen, die die eigentlichen (IAM-)Prozesse ausführen, werden in alphabetischer Reihenfolge beschrieben. Für jede Rolle wird zusätzlich der primäre Stakeholder (siehe Kapitel 3.2) angegeben.

IAM-Dienstanbieter	Der *IAM-Dienstanbieter* ist verantwortlich für den Betrieb[1] von einem oder mehreren IAM-Geschäftsservices gemäss Kapitel 7. Es können die Spezialisierungen gemäss Abbildung 3 unterschieden werden, die aber oft gemeinsam implementiert werden.  **Abbildung 3 Dienstanbieter** Die *Registrierungsstelle* (*RA*) erfasst und prüft die E-Identities und Attribute der Subjekte. Der *Identity Provider* (*IdP*) überprüft zur Laufzeit die E-Identities der Subjekte. Die *Attribut-Autorität* (*AA*) verwaltet die Attribute der Subjekte und gibt Attributbestätigungen aus. Der *Credential Service Provider* (CSP) vergibt und verwaltet Authentifizierungsmittel für E-Identities. Ein CSP enthält immer eine RA und umfasst die Dienste zur Überprüfung der E-Identities (IdP). Ein *Vermittler* bietet gemeinsame Dienste, wie Metadatenverwaltung, IdP-Discovery, Identity Linking oder Transformation der Authentifizierungs- und Attributbestätigung, für alle andere IAM-Dienstanbieter und Relying Parties in einer Identity Federation an. Ein Vermittler kann optional einen CSP enthalten. Die Abbildung 3 stellt alle IAM-Dienstanbieter dar, falls sie gemeinsam implementiert werden. Primärer Stakeholder: Dienstanbieter

[1] Der Betrieb kann vom IAM-Dienstanbieter selbst gewährleistet oder auch an einem Betreiber ausgelagert werden (Outsourcing). Im Outsourcing-Fall überträgt der IAM-Dienstanbieter die an ihn gestellten Anforderungen an den Betreiber. Auf das IAM-Gesamtsystem hat das keinen Einfluss und wird daher in diesem Dokument nicht weiter betrachtet.

IAM-Führung	Die *IAM-Führung* ist verantwortlich für das Managen eines IAM-Systems oder von Teilen davon (IAM-Dienstanbieter oder Relying Party). Die *IAM-Führung des Gesamtsystems* managt die teilnehmenden IAM-Dienstanbieter und Relying Parties (z. B. analog zu ITIL [3]) in allen Fachbereichen wie z. B. Release-Management, Qualitätsmanagement, IAM-Lieferanten- und -Konsumentenmanagement, Service-Request-Management. Dies kann sowohl im internen Kontext als auch über Verträge/SLA mit externen IAM-Dienstanbietern und Relying Parties geschehen. Primärer Stakeholder: Führung
IAM-Regulator	Der *IAM-Regulator* (oder die *IAM-Steuerung*) definiert die rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen, innerhalb derer das IAM abgewickelt werden muss. Er berücksichtigt dabei die Interessen aller Stakeholder und beteiligt alle anderen Rollen in geeigneter Weise an der Definition. IAM-Regulatoren existieren in verschiedenen Formen und können sowohl innerhalb einer einzigen Organisation, aber auch organisationsübergreifend agieren. Die *IAM-Steuerung* definiert die IAM-Policy für ein organisationsinternes oder -externes IAM-System bzw. von IAM-Geschäftsservices. Sie sorgt dabei auch für Orchestrierung, die strategische Weiterentwicklung und Governance des Gesamtsystems. Der *Gesetzgeber* definiert die rechtlichen Rahmenbedingungen innerhalb derer sich das Gesamtsystem bewegen und entwickeln muss. Das *Standardisierungsgremium* erstellt Normen und Richtlinien für die prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen. Primärer Stakeholder: Regulator
IAM-Support	Der *IAM-Support* ist verantwortlich für alle Aktivitäten zum Auffinden und Lösen von Problemen. Primärer Stakeholder: Dienstanbieter

Relying Party	Die *Relying Party* vertritt die Interessen der *Ressource* im IAM-System. Sie nutzt IAM-Geschäftsservices und verarbeitet Informationen von *IAM-Dienstanbietern* für den Schutz ihrer *Ressourcen*. Sie braucht zur Beurteilung der *Berechtigung* eines Ressourcenzugriffs nähere Informationen (berechtigungsrelevante Eigenschaften) zu einem *Subjekt,* dessen *E-Identity* und den Kontext des Zugriffs (Lokation, Zeitpunkt, Sicherheitsniveau etc.) Primärer Stakeholder: Leistungserbringer
Subjekt	Eine *natürliche Person*, eine *Organisation* (*juristische Person)*, ein *Service* oder ein *Ding*, das auf eine *Ressource* zugreift oder zugreifen möchte. Ein Subjekt wird durch *E-Identities* repräsentiert. Primärer Stakeholder: Leistungsbezüger

Die Rollen können sich in verschiedenen Organisationseinheiten wiederholen. Es kommt so zu einer fachlichen Zusammenarbeit auf verschiedenen Ebenen und in verschiedenen Kontexten.

Abbildung 4 zeigt die Zusammenarbeit an einem einfachen Beispiel einer Identity Federation bestehend aus einer RP und einem IAM-Dienstanbieter. Es stellt eine Situation dar. Ein Subjekt möchte fachliche Leistungen von Organisation 1 beziehen und wird von Organisation 2 authentifiziert. Die Organisationen haben je eine Führung und je einen Regulator. Innerhalb des IAM-Gesamtsystem (Organisation 3) gibt es eine Führung und einen Regulator, die das Gesamtsystem definieren. Beispiel für ein Standardisierungsgremium ist der eCH.

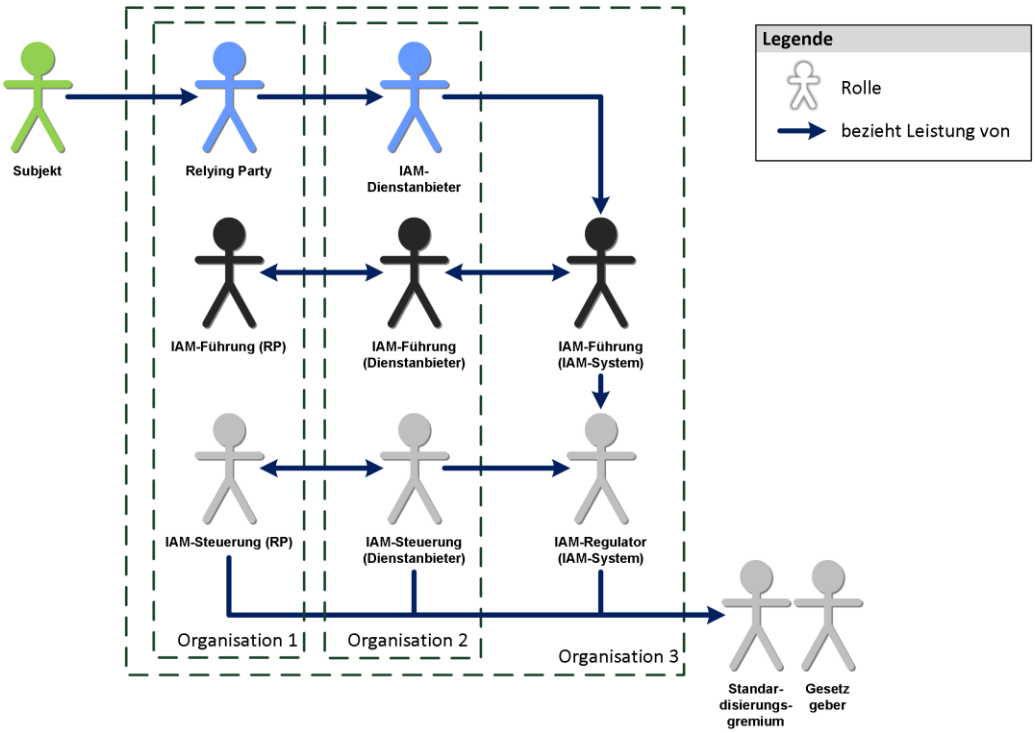


Abbildung 4 Zusammenarbeit von Rollen in einem föderierten IAM-System

3.2 Stakeholder im IAM

Die Rollen in einem IAM-System (siehe Kapitel 3.1) werden durch die Stakeholder motiviert. In den folgenden Abbildungen wird aufgezeigt, welcher Stakeholder die Anforderungen, Kompetenzen und Verantwortungen welche Rollen motiviert.

Leistungsbezüger (LB)	Der Leistungsbezüger möchte jederzeit, kostengünstig und einfach eine fachliche Leistung[2] online in Anspruch nehmen. Er fordert Unterstützung bei Problemen (z. B. bei Identitätsdiebstahl) und erwartet Konformität mit gesetzlichen Regelungen.

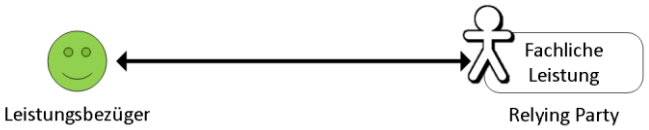


Abbildung 5 Sicht des Leistungsbezügers

Abbildung 5 zeigt die Sicht des Leistungsbezügers auf das Gesamtsystem. Der Leistungsbezüger möchte vorrangig eine fachliche Leistung einer Relying Party in Anspruch nehmen. Das verwendete IAM-System ist für ihn zweitrangig und nur Mittel, um sein Ziel zu erreichen.

Leistungserbringer (LE)	Der Leistungserbringer möchte fachliche Leistungen online anbieten. Dies soll kostengünstig, stabil, einfach und konform mit den gesetzlichen Regelungen sein und von möglichst vielen genutzt werden. Den Zugriff und den Schutz der Ressourcen möchte er gemäss seinen Bedürfnissen (z. B. Risikobereitschaft, Wirtschaftlichkeit) an die IAM-Dienstanbieter übertragen.

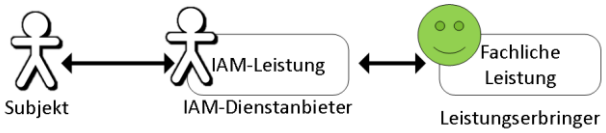


Abbildung 6 Sicht des Leistungserbringers

Abbildung 6 zeigt die Sicht des Leistungserbringers auf das Gesamtsystem. Der Leistungserbringer möchte seine fachliche Leistung dem Subjekt zur Verfügung stellen. Die dazu notwendigen IAM-Leistungen möchte er zumeist nicht selbst erbringen, sondern diese an IAM-Dienstanbieter auslagern.

[2] Die hier erwähnte fachliche Leistung ist z. B. die Bestellung einer Funklizenz oder einer Parkkarte, nicht eine IAM-Leistung von einem IAM-Dienstanbieter.

Dienstanbieter	Der Dienstanbieter möchte, dass seine angebotenen IAM-Leistungen von möglichst vielen verwendet werden. Zudem strebt er eine Zusammenstellung von möglich komplementär ausgerichteten Diensten an, um das IAM-System effizient und wirtschaftlich zu halten.

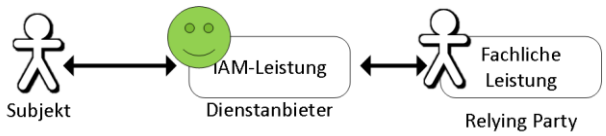


Abbildung 7 Sicht des Dienstanbieters

Abbildung 7 zeigt die Sicht des Dienstanbieters auf das Gesamtsystem. Der Dienstanbieter stellt seine IAM-Leistung der Relying Party zur Verfügung. Mit Hilfe dieser IAM-Leistung kann das Subjekt die fachliche Leistung der Relying Party nutzen.

Führung	Die Führung möchte ein funktionierendes und stabiles IAM-System, das allen Stakeholdern gerecht wird. Er führt die daran beteiligten IAM-Dienstanbietern und Relying Parties und garantiert den zuverlässigen Betrieb des IAM-Systems.

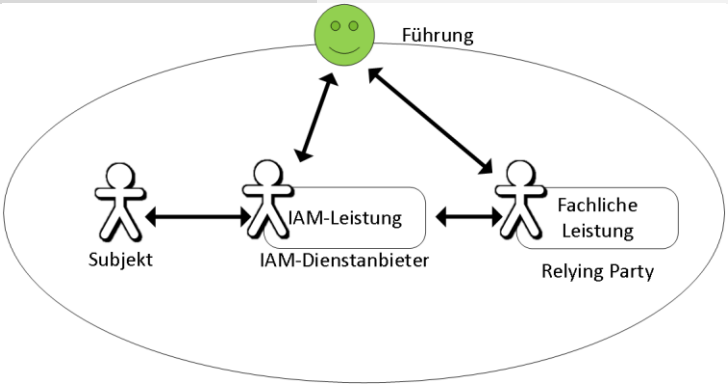


Abbildung 8 Sicht der Führung des gesamten IAM-Systems

Abbildung 8 zeigt die Sicht der Führung des gesamten IAM-Systems. Die Führung möchte das IAM-System und die daran beteiligen Relying Parties und IAM-Dienstanbietern effizient führen, um die Implementierung zu erleichtern und den zuverlässigen Betrieb zu garantieren. Die Führung koordiniert dabei die Anforderungen aller Stakeholder im IAM-System, auch die des Regulators und des Leistungsbezügers.

Regulator	Der Regulator möchte die Interoperabilität (insbesondere bei selbstständig geführten Teilsystemen), Robustheit und Sicherheit des IAM-Gesamtsystems sicherstellen.

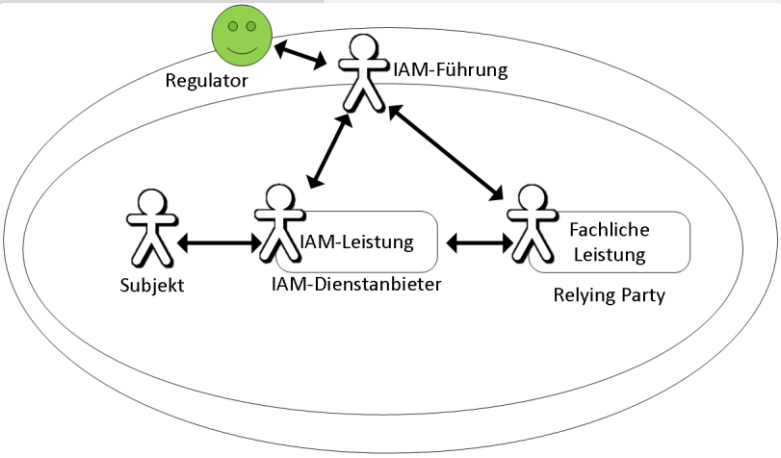


Abbildung 9 Sicht des Regulators

Abbildung 9 zeigt die Sicht des Regulators. Der Regulator möchte durch die Schaffung entsprechender Rahmenbedingungen (Gesetze, Standards, Strategien, etc.) den Einsatz von föderierten IAM-Systemen im organisationsübergreifenden Kontext fördern und gleichzeitig eine hohe Qualität nicht funktionaler Merkmale, wie z. B. Interoperabilität, Zuverlässigkeit und Sicherheit, erreichen.

4 Anforderungen

Die in diesem Kapitel beschriebenen und definierten Prinzipien und Anforderungen definieren und strukturieren die in Kapitel 6 modellierten Prozesse und müssen angewendet oder erfüllt werden, damit ein interoperables und effizientes föderiertes IAM-System aufgebaut werden kann.

Die Prinzipien und Anforderungen können in vier verschiedene Typengruppen eingeteilt werden:

- B… Business (Geschäftsanforderungen),
- D… Data (Informationen und Daten),
- A… Application (Anwendung),
- T… Technology (Technologie).

4.1 Grundprinzipien eines föderierten IAM-Systems

Die Grundprinzipien beschreiben die allgemeinen Architekturprinzipien für die Gestaltung eines föderierten IAM-Systems. Sie geben die Leitplanken bei der Realisierung eines föderativen IAM-Systems vor.

Bezeichnung	Typ	Beschreibung	Begründung
Prinzip-1	A/B	Informationen und Daten MÜSSEN föderiert statt repliziert werden, d.h. dass zur Laufzeit bei Authentisierung und Autorisierung direkt auf die Daten der autoritativen Quelle zugegriffen wird, ohne dass diese als Kopie vorgehalten werden müssen.	Aktualität und Konsistenz der Daten, Kosten (Vereinfachung der Prozesse), geringere Fehleranfälligkeit
Prinzip-2	A/B	Soweit von der Vertrauensstufe her möglich, SOLLTEN bestehende E-Identities, Authentifizierungs- und Attributbestätigungen von anderen Stellen übernommen werden (Föderation).	Wiederverwendbarkeit und daraus resultierenden Effizienz
Prinzip-3	A	Für die *Authentifikation* und den *Zugang* SOLLTEN die *Relying Party* von ihr entkoppelte (IAM-)Dienste nutzen.	Kosten, Modularität, Erweiterbarkeit (neue Technologien)
Prinzip-4	A	Der *Autorisierung* für einen *Zugriff* auf eine schützenswerte *Ressource* MUSS die *Authentifikation* des zugreifenden *Subjekts* vorausgehen.	Feststellung der Identität des Subjekts als Grundlage einer Autorisierung
Prinzip-5	A/D	Zur Berechtigung SOLLTEN vorrangig regelbasierte Verfahren, die sich auf Attribute abstützen (ABAC), als antragsbasierte Verfahren (Genehmigung von Rollen, RBAC) verwendet werden.	Antragsbasierte Verfahren bedürfen einer vorgängigen Übertragung der Identität an den Berechtigungsverwalter
Prinzip-5.1	A	Der *Zugang* MUSS ausschliesslich auf	Unabhängigkeit der

Bezeichnung	Typ	Beschreibung	Begründung
		Grund der angegebenen *Attribute* gewährt werden.	Zugangsentscheidung von Daten der Ressource, Modularität
Prinzip-6	B	Organisationsübergreifende Effektivität des IAM MUSS auf gegenseitigem spezifischem Vertrauen in die Partner basieren.	Föderation ohne Vertrauen nicht möglich
Prinzip-7	A/D	Wenn fachlich nicht notwendig, SOLLTEN keine Informationen eines zugreifenden *Subjekts*, ausser die für den Zugriffsentscheid notwendigen, an die *Ressource* weitergegeben werden.	Need-to-Know-Prinzip, Schutz der Privatsphäre
Prinzip-8	B	Die Einhaltung der rechtlichen, organisatorischen/architektonischen und technischen Vorgaben (insbesondere des Datenschutzes, sowie allen organisationsspezifischen Sicherheitsvorgaben) SOLLTE zu jeder Zeit gewährleistet sein.	Compliance, Interoperabilität
Prinzip-9	B	Das IAM SOLLTE möglichst kostengünstig, effektiv und wirtschaftlich betrieben und verwaltet werden.	Kosten
Prinzip-10	B	Um eine effektive Zusammenarbeit zu gewährleisten, SOLLTE das IAM auf einer international interoperablen IAM-Architektur basieren. [4]	Interoperabilität

4.2 Anforderungen an das föderierte IAM-System

Dieser Abschnitt beschreibt die generischen Anforderungen aller Stakeholder an ein föderiertes IAM-System im Schweizer E-Government.

Bezeichnung	Typ	Beschreibung	Begründung / Prinzip
IAM-1	T/A	Das IAM SOLLTE auf einer international interoperablen IAM-Architektur basieren. [4]	Prinzip-1 Prinzip-10
IAM-1.1	T/A	Das IAM MUSS in andere IAM einfach integrierbar[3] sein. Auf internationaler Ebene SOLLTE es einfach integrierbar sein.	Prinzip-10
IAM-1.2	T/A	Das IAM MUSS die Fähigkeit haben, bestehen-	Prinzip-10

[3] Durch die Integration von IAM-Systemen können E-Identities über Domänengrenzen hinweg genutzt werden. Das Ziel einer solchen Integration ist die Befähigung der Subjekte einer Domäne auf die Ressourcen einer anderen Domäne zuzugreifen, ohne dass die Identitätsinformationen (E-Identities und zugehörige Attribute) mehrfach verwaltet oder repliziert werden müssen, d.h. die E-Identities müssen föderiert werden.

Bezeich-nung	Typ	Beschreibung	Begründung / Prinzip
		de IAM-Lösungen einfach zu integrieren.	
IAM-2	A/D	Die *Authentifikation* und *Berechtigung* für den *Zugang* SOLLTEN auf **standardisierten** *Authentifizierungsmitteln* und *Attributen basieren*.	Prinzip-3 Prinzip-5.1 Prinzip-9 Prinzip-10
IAM-3	T/A	Die IAM-Systeme MÜSSEN modular und SOLLTEN skalierbar aufgebaut sein.	Wiederverwend-barkeit, Wart-barkeit Prinzip-9 Prinzip-10
IAM-4	A	Die technischen Services MÜSSEN über standardisierte Schnittstellen zusammenarbeiten, welche offene Standards gemäss ihrer Spezifikation (z. B. SAML, OIDC) benutzen.	Prinizip-10
IAM-5	T	Die je nach Schutzbedürfnissen notwendigen, unterschiedlich starken Authentisierungs- und Autorisierungsverfahren KÖNNEN auf derselben IAM-Infrastruktur realisiert werden.	Wiederverwend-barkeit Prinzip-9 Prinzip-10
IAM-6	D	Die Menge der E-Identities, Authentifizierungsmittel und Attribute SOLLTE minimal gehalten und womöglich konsolidiert werden.	Benutzerfreund-lichkeit Prinzip-9
IAM-7	A	Der Transport der Daten MUSS zwischen den IAM-Dienstanbietern und RPs auf Protokollebene abgesichert sein (z. B. mit TLS).	Sicherheit, Schutz der Privatsphäre Prinzip-8
IAM-8	A	Die technischen Services, welche Authentifizierungs- und Attributbestätigungen erstellen oder konsumieren, MÜSSEN ihre Zeit mit einem zugelassenen Zeitserver synchronisieren.	Sicherheit, Robustheit Prinzip-10
IAM-9	B/A	Die von den Geschäftsservices erstellten Authentifizierungs- und Attributbestätigungen MÜSSEN auf ihre Authentizität und Integrität überprüft werden können (z. B. mit Hilfe der Signatur oder durch Rückfragen).	Sicherheit, Trust Prinzip-6
IAM-10	A/B	Es MUSS gewährleistet sein, dass jederzeit nachvollzogen und nachgewiesen werden kann, welches *Subjekt* wann auf welche *Ressource* zugegriffen hat.	Nachvoll-ziehbarkeit, Prinzip-8
IAM-11	B/A/T	Es MUSS entsprechend der Sicherheitsanforderung sichergestellt werden, dass Authentifizierungs- und Attributbestätigungen nur von berechtigten Instanzen gelesen werden können.	Schutz der Privatsphäre, Prinzip-8

4.3 Anforderungen der Stakeholder

Die Anforderungen der Stakeholder an die verschiedenen Rollen in einem IAM-System sind in Tabelle 3 überblicksmässig dargestellt. Sie werden im Folgenden einzeln aufgeführt und referenzieren sowohl die Grundprinzipien (Kap. 4.1) und Anforderungen (Kap. 4.2) eines föderierten IAM-Systems wie auch die Anforderungen anderer Stakeholder.

Rollen **Stakeholder**	**Subjekt**	**Relying Party**	**IAM-Dienst-anbieter**	**IAM-Führung**	**IAM-Support**	**IAM-Regulator**
Leistungs-bezüger	(A)	A	A		A	A
Leistungs-erbringer	A		A	A	A	A
Dienstanbieter	(A)		A	A		A
Führung		A	A	A	A	A
Regulator				A		A

Tabelle 3 Anforderungen der Stakeholder an die Rollen

4.3.1 Anforderungen des Leistungsbezügers

Die Anforderungen des Leistungsbezügers (LB) werden von natürlichen Personen, Organisationen, Services oder Dingen gestellt, die auf Informationen und Services der *Ressourcen* zugreifen wollen.

Bezeichnung	**Typ**	**Beschreibung**	**Begründung**	**Referenz**
LB-1	A/D	Wenn das Subjekt auf eine schützenswerte Ressource zugreift, MUSS sich das Subjekt authentisieren.	Authentifizierung als Grundlage der Autorisierung, Datenschutz	**Prinzip-4**
LB-1.1	B/A/T	Das Subjekt MUSS sich minimal mit der geforderten Vertrauensstufe authentisieren. Es DARF sich mit einer höheren Vertrauensstufe authentisieren.	Kosten, Benutzerfreundlichkeit, Schutz der Privatsphäre	**Prinzip-7, Prinzip-5**
LB-2	D	Ein eindeutiger Identifikator gegenüber der Ressource MUSS nur dann vom Subjekt verwendet werden, wenn die Nutzung der Ressource das fordert.	Schutz der Privatsphäre	**Prinzip-7**
LB-2.1	D	Einen zufälligen Identifikator (z. B. eine Transient ID) gegenüber der Ressource SOLLTE vom Subjekt bei der Nutzung verwendet werden.	Schutz der Privatsphäre (Unlinkability)	**Prinzip-7**
LB-3	D	Es MÜSSEN nur die Attribute vom Subjekt bei der Authentifikation übermittelt werden, die zur Berechtigung der	Need-to-Know-Prinzip, Schutz der Privatsphäre	**Prinzip-7**

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
		Ressource notwendig sind.		
LB-3.1	D	Weitere Attribute KÖNNEN vom Subjekt übermittelt werden, wenn die Ressource diese für die Funktionserfüllung benötigt.	Schutz der Privatsphäre	**Prinzip-7**
LB-4	B/A	Die IAM-Dienstanbieter (IdP, AA), welche die E-Identities und Attribute verwalten, KÖNNEN vom Subjekt gewählt werden.	Selbstbestimmung, Wahlfreiheit	**Prinzip-2**
LB-5	D	Die Anzahl der benötigten E-Identities, die das Subjekt haben muss, SOLLTE möglichst gering gehalten werden.	Kosten, Benutzerfreundlichkeit, Kontextabdeckung	**IAM-6**
LB-6	B	Die Anzahl von Authentifizierungsmittel und Attribute verschiedener Qualitäten KANN vom Subjekt selbst bestimmt werden.	Selbstbestimmung, Wahlfreiheit	
LB-7	B	Das Authentifizierungsmittel (während der Authentisierung), welches die minimal geforderte Qualität erfüllt, KANN vom Subjekt selbst bestimmt werden.	Selbstbestimmung, Wahlfreiheit	**Prinzip-2**
LB-8	B	Die Beschaffung von E-Identities und Authentifizierungsmitteln SOLLTE einfach und günstig sein.	Kosten	**Prinzip-9**
LB-9	A	Die Benutzung von E-Identities und Authentifizierungsmitteln SOLLTE einfach und unkompliziert sein.	Benutzerfreundlichkeit	
LB-10	B	Ein anderes Subjekt SOLL die Fähigkeit haben, kontextbezogen und zeitlich begrenzt als Stellvertreter zu handeln.	Delegation von Berechtigungen	
LB-11	B/A	Der Weitergabe von Attributen MUSS das Subjekt zustimmen können, ausser das Recht zur Weitergabe ist gesetzlich verankert oder anderswo geregelt.	Schutz der Privatsphäre	**Prinzip-8**
LB-12	B/A	Das Subjekt MUSS bei Vermeidung und Recovery des Missbrauchs einer E-Identity unterstützt werden. [4]	Benutzerfreundlichkeit, Sicherheit	**Führ-3**
LB-13	B/A/T	*IAM-Dienstanbieter MÜSSEN* das vernünftig Machbare unternehmen, um den Missbrauch der *E-Identity* des *Subjekts* zu verhindern. [4]	Schutz der Privatsphäre, Sicherheit	**LE-10, Führ-3**
LB-14	A	Der IAM-Support MUSS das Subjekt beim Lösen von Problemen, die eine	Benutzerfreundlichkeit	**Führ-6**

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
		erfolgreiche Nutzung der Ressource verhindern, unterstützen.		
LB-15	A	Die vom Subjekt freigegebenen Attribute SOLLTEN nur von den berechtigten Instanzen gelesen werden können.	Schutz der Privatsphäre	**IAM-11**
LB-16	B	Die Nutzung der IAM-Dienste zur Laufzeit MUSS jederzeit möglich sein.[4]	Verfügbarkeit	
LB-17	D	Wenn die Ressource, auf die das Subjekt zugreifen möchte, subjektbezogene, sensible Daten enthält, muss die RP dafür sorgen, dass nur die berechtigten Subjekte Zugriff erhalten.	Schutz der Privatsphäre, Datenschutz	**Prinzip-4**

4.3.2 Anforderungen der Leistungserbringer

Dieser Abschnitt beschreibt die von den Leistungserbringern (LE) gestellten Anforderungen.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
LE-1	B/A/T	Der Missbrauch von *Ressourcen* SOLLTE ausgeschlossen sein.	Sicherheit	
LE-2	A	Der *Zugriff* auf schützenswerte *Ressourcen* MUSS auf autorisierte *Subjekte* eingeschränkt sein.	Sicherheit (Access Control)	**Prinzip-4**
LE-2.1	A	Falls das *Subjekt* keine Rechte für die aufzurufende schützenswerte *Ressource* hat, MUSS der Aufruf an die *E-Ressource* verworfen und/oder entsprechend umgeleitet werden.	Sicherheit, Benutzerfreundlichkeit	
LE-3	B/A	Der Aufwand für die Verwaltung der *E-Ressourcen* SOLLTE minimal sein.	Kosten	**Prinzip-9**
LE-4	B/A	Der Aufwand für die Verwaltung der *Berechtigungen* (*Zugangsregeln* und *Zugriffsrechte*) SOLLTE minimal sein.	Kosten	**Prinzip-9**
LE-5	D	Die Menge der unterstützten *E-Identities* und *Attribute* MUSS minimal gehalten und SOLLTE womöglich konsolidiert werden.	Kosten	**Prinzip-9, IAM-6, LB-5**

[4] Die Ressource sollte jederzeit nutzbar sein.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
LE-6	B	*E-Identities* und *Attribute* MÜSSEN bei Veränderungen zeitnah gepflegt werden.	Aktualität	
LE-7	A	Authentifizierungs- und Attributbestätigungen KÖNNEN durch *IAM-Dienstanbieter* unterschiedlicher Qualität ausgestellt werden. [4]	Interoperabilität	**Prinzip-2**
LE-8	B	Für Subjekte SOLLTEN in der Authentifizierung- und/oder Attributbestätigung subjektidentifizierende Attribute vorhanden sein.	Wiedererkennung des Subjekts	
LE-9	B	Das *Subjekt* und die IAM-Dienstanbieter MÜSSEN den Verdacht eines Missbrauchs einer *E-Identity* melden. [4]	Sicherheit	
LE-10	B/A/T	*IAM-Dienstanbieter MÜSSEN* das vernünftig Machbare unternehmen, um den Missbrauch der *E-Identity* des *Subjekts* zu verhindern. [4]	Schutz der Privatsphäre, Sicherheit	**LB-13, Führ-3**

4.3.3 Anforderungen der Dienstanbieter

Dieser Abschnitt beschreibt die Anforderungen der Dienstanbieter.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
Dienst-1	B/A	Der Aufwand für die Administration der *E-Identities* (Authentifizierungsmittel und *Attribute*) SOLLTE im Verhältnis zur angestrebten Qualität minimal sein.	Kosten	**Prinzip-9, LB-8**
Dienst-2	D	Der Zusammenhang zwischen der *E-Identity* und den dazugehörigen *Authentifizierungsmitteln* MUSS zu jedem Zeitpunkt gewährleistet sein.	Nachvollziehbarkeit	**IAM-10**
Dienst-3	B	Die IAM-Führung MUSS die Stabilität der prozessualen, organisatorischen/architektonischen und technischen Aspekte des IAM-Systems und die Weiterentwicklung sicherstellen.	Kosten, Investitionsschutz	**Prinzip-9**

4.3.4 Anforderungen der Führung

Dieser Abschnitt beschreibt die Anforderungen der Führung.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
Führ-1	B/A	Die IAM-Dienstanbieter und Relying Parties SOLLTEN sich auf eine Menge von Authentifizierungsmitteln und Attributen einigen.	Interoperabilität, Benutzerfreundlichkeit, Führbarkeit	**IAM-2, IAM-6**
Führ-2	T	Die IAM-Dienstanbieter und Relying Parties MÜSSEN standardisierte Schnittstellen verwenden.	Interoperabilität	**IAM-4**
Führ-3	B/A	Die verschiedenen IAM-Dienstanbieter und Relying Parties MÜSSEN zusammenarbeiten, um das Subjekt bei Vermeidung und Recovery des Missbrauchs seiner E-Identity zu unterstützen.	Benutzerfreundlichkeit, Sicherheit	**LB-12, LB-13, LE-10**
Führ-4	B/D	Die verschiedenen IAM-Dienstanbieter und die Relying Parties MÜSSEN zusammenarbeiten, so dass jederzeit nachvollzogen werden kann, welches *Subjekt* wann auf welche *Ressource* zugegriffen hat.	Nachvollziehbarkeit	**IAM-10**
Führ-5	B	Der IAM-Regulator MUSS die erforderlichen rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen für das betroffene IAM-System definieren.	Rechtskonformität, Sicherheit, Robustheit	**Prinzip-8 Reg-1**
Führ-5.1	B	Die verschiedenen IAM-Dienstanbieter und die Relying Parties SOLLTEN die vom IAM-Regulator definierten Rahmenbedingungen einhalten.	Rechtskonformität, Sicherheit, Robustheit	**Prinzip-8**
Führ-6	A	Der IAM-Support MUSS das Subjekt effizient, kundenfreundlich, günstig und nachvollziehbar beim Lösen von Problemen, die eine erfolgreiche Nutzung der Ressource verhindern, unterstützen.	Benutzerfreundlichkeit, Kosten	**LB-14**

4.3.5 Anforderungen des Regulators

Dieser Abschnitt beschreibt die Anforderungen der IAM-Regulatoren.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
Reg-1	B	Die verschiedenen IAM-Dienstanbieter und Relying Parties SOLLTEN die definierten rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen einhalten.	Compliance	**Prinzip-8 Führ-5**
Reg-2	B	Die Einhaltung der definierten rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen MÜSSEN durch entsprechende Evidenzen belegt werden können.	Compliance	**Prinzip-8**
Reg-3	B	Bei Nichteinhaltung MUSS die IAM-Führung eine begründete Ausnahme beantragen und bewilligen lassen.	Risikomanagement	**Prinzip-8**

5 Informationsarchitektur

Nachstehendes Modell stellt die wichtigen Begriffe des *IAM* und ihre Beziehungen in einer Übersicht als UML-Klassendiagramm dar. Weil die Elemente des *IAM*-Informationsmodells an sehr vielen Orten (nicht nur im *IAM*) verwendet werden, ist es hier wichtig, differenzierte Begriffe zu verwenden, damit Syntax und Semantik für alle Beteiligten eindeutig und unmissverständlich definiert sind. Abbildung 10 zeigt das Informationsmodell zum organisationsübergreifenden IAM.

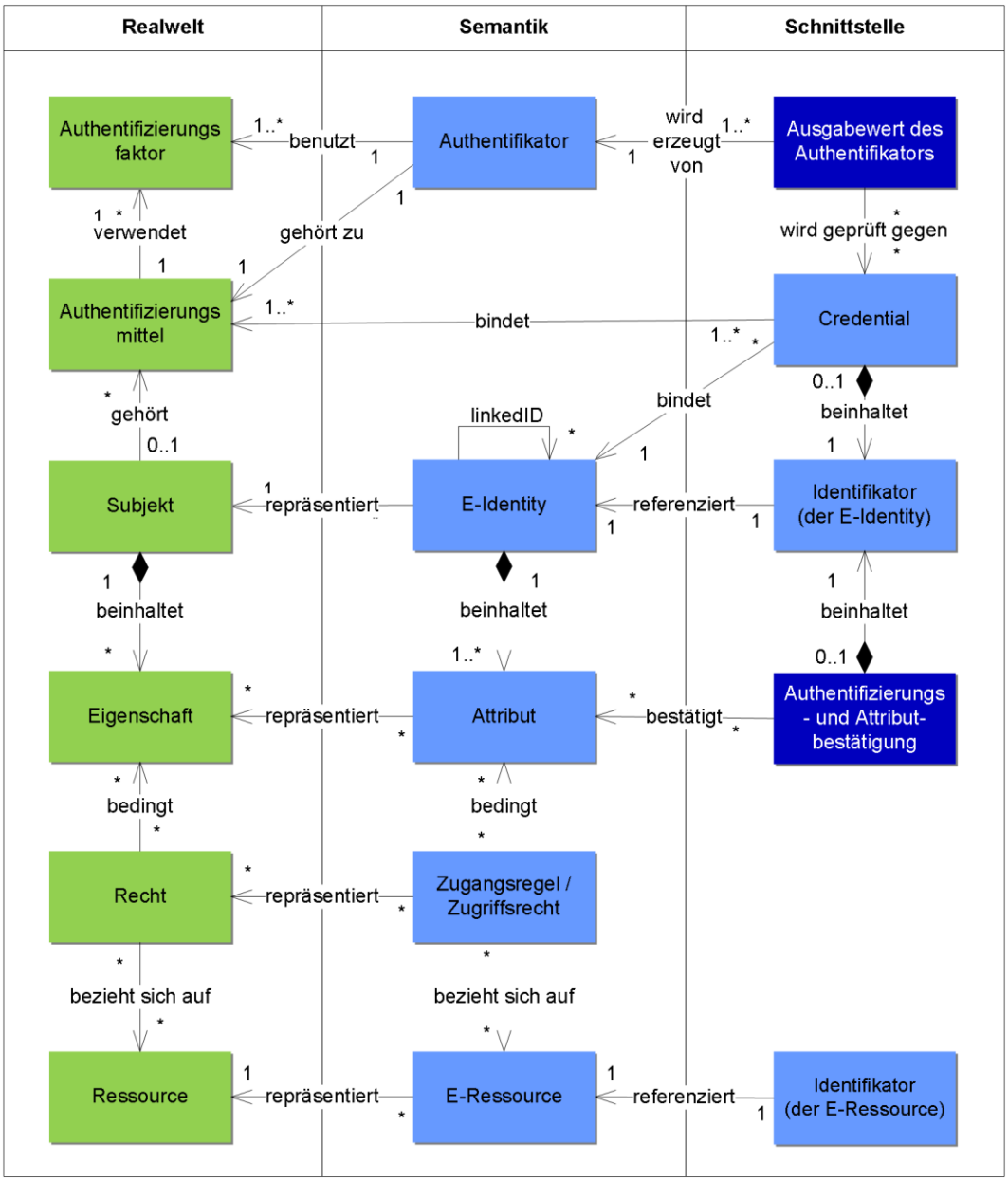


Abbildung 10 Informationsmodell

Allgemein ist es üblich, zwischen dem Fachbereich und den Informationssystemen für die Elemente der realen Welt die gleichen Bezeichner zu verwenden. Weil im *IAM* die Unterschiede zwischen der semantischen Sicht (der beteiligten Informationssysteme) und der rea-

len Welt wesentlich sind, werden hier für unterschiedliche Elemente auch unterschiedliche Bezeichner verwendet. Das Informationsmodell in Abbildung 10 zeigt links (in grün) die Elemente der realen Welt, in der Mitte das semantische Modell (der Informationssysteme), und rechts die Schnittellenobjekte, die zum Informationsaustausch zwischen Informationssystemen verwendet werden. Objekte, die zur Definitionszeit entstehen, sind entspr. der Farbverwendung aus Tabelle 1 hellblau dargestellt, Objekte der Laufzeit in dunkelblau.

Das semantische Modell in der Mitte macht keine Aussagen über die Verteilung der Information über Informationssysteme.

Zur Definitionszeit (siehe Prozesse in Abschnitt 6.2 und Geschäftsservices in Abschnitt 7.2) werden Objekte der realen Welt mit ihren Eigenschaften und Beziehungen in die Informationssysteme (Semantik) abgebildet.

Zur Laufzeit (siehe Prozesse in Abschnitt 6.1 und Geschäftsservices in Abschnitt 7.3) werden Schnittstellenobjekte auf Basis der Inhalte des semantischen Modells erstellt und zwischen Informationssystemen ausgetauscht.

Die nachfolgende Tabelle beschreibt kurz[5] die in der Abbildung 10 vorkommenden Elemente und ihre Beziehungen.

Realwelt	
Ressource	Service oder Daten, auf welche ein *Subjekt* zugreifen kann, wenn es sich *authentisiert* hat und es auf der Basis der benötigten *Attribute autorisiert* wurde. Dies schliesst physische Ressourcen wie Gebäude und Anlagen, deren Benutzung über IT-Systeme gesteuert wird, ein.
Recht	Die *Rechte* sind *spezifische abstrakte Eigenschaften*, welche das *Subjekt* besitzen muss, um auf eine *Ressource* zugreifen zu dürfen. Diese können z. B. in Gesetzen oder Verträgen festgelegt sein.
Eigenschaften	*Eigenschaften* sind charakteristische Merkmale oder charakteristisches Verhalten eines *Subjekts*, die in ihrer Summe für das *Subjekt* spezifisch sind.

[5] Die vollständigen Beschreibungen mit Abbildungen und Beispielen sind im eCH-0219 [1] zu finden.

Subjekt

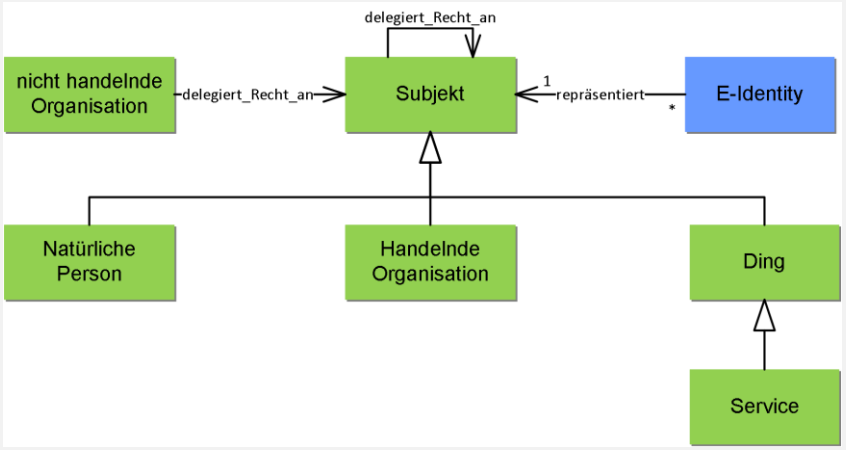


Abbildung 11 Subjekt Definition

Ein Subjekt ist eine *natürliche Person*, eine handelnde *Organisation*, ein *Service* oder ein *Ding*, das auf eine *Ressource* zugreift oder zugreifen möchte.

Ein Subjekt wird durch *E-Identities* in der digitalen Welt repräsentiert.

Ein Subjekt kann *Rechte* an ein weiteres Subjekt delegieren.

Eine *Organisation* ist eine Gruppe aus mehreren natürlichen Personen oder Dingen. Eine Organisation kann (Unter-)Organisationen enthalten.

Dabei wird zwischen *handelnden* und *nicht handelnden* Organisationen unterschieden. Handelnde Organisationen (z. B. Gruppen-Identitäten) können sich authentifizieren und Zugriff zu Ressourcen erhalten. Nicht handelnde Organisationen (z. B. juristische Personen) können sich nicht selbst authentifizieren, sondern nur über das dazugehörige Subjekt (z. B. eine natürliche Person), an das sie ihre Rechte delegieren.

Eine *juristische Person* ist eine spezielle *Organisation*, die von einer anerkennenden Behörde anerkannt wird. Die Anerkennung beruht auf einen Vertrag zwischen der anerkennenden Behörde und der juristischen Person. Einer juristischen Person muss immer mindestens eine natürliche Person zugeordnet sein.

Ein *Ding* ist eine existierende oder abstrakte Einheit, die eindeutig identifizierbar ist.

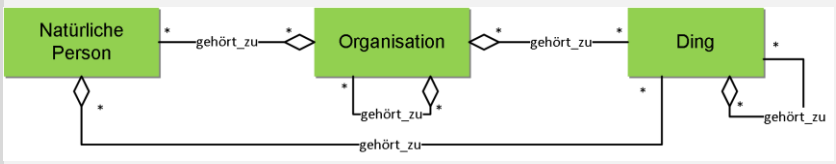


Abbildung 12 Zugehörigkeit der Subjekte

	Dinge können weitere Dinge enthalten. Ein Ding kann zu einer *Organisation* oder zu einer *natürlichen Person* gehören. Ein *Service* ist ein spezielles Ding, das über ein *Netzwerk* erreichbar und darin digital identifizierbar ist.
Authentifizierungsmittel	Etwas, das ein *Subjekt* besitzt und unter seiner Kontrolle hat (ein kryptographischer Schlüssel, ein Geheimnis oder ein spezifisches Verhalten). Ein Authentifizierungsmittel kann einen (*single-factor authenticator*) oder auch mehrere unabhängige Authentifizierungsfaktoren (*multi-factor authenticator*) benutzen.
Authentifizierungsfaktor	Informationen und/oder Prozesse, die zur Authentifizierung eines *Subjektes* verwendet werden können. Authentifizierungsfaktoren können auf vier verschiedenen Merkmalen (besitzabhängig, kenntnisabhängig, inhärent oder verhaltensbasiert) oder Kombinationen davon beruhen.
Semantik	
E-Ressource	Digitale Repräsentation einer *Ressource*. Eine *E-Ressource* hat einen *Identifikator* (eindeutiger Name, oft URL/URI), welche innerhalb eines *Namensraumes* eindeutig einer *Ressource* zugewiesen werden kann.
Zugangsregel / Zugriffsrecht	Ressourcenverantwortliche definieren die *Zugangsregeln* und *Zugriffsrechte* für ihre *E-Ressourcen*. Die *Zugangsregeln* und *Zugriffsrechte* definieren die Bedingungen, unter denen ein *Subjekt* zu einer *Ressource* Zugang erhält (*Grobautorisierung*) und auf sie zugreifen darf (*Feinautorisierung*), z. B. nach erfolgreicher Authentifizierung und Bestätigung bestimmter *Attribute*.
Attribut	Semantisches Abbild einer einem *Subjekt* zugeordneten *Eigenschaft*, die das *Subjekt* näher beschreibt. Der *Identifikator* ist ebenfalls ein speziell verwendetes *Attribut*.
E-Identity	Repräsentation eines *Subjekts*. Eine *E-Identity* (*digitale Identität*) hat einen *Identifikator* (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen *Attributen*, welche innerhalb eines *Namensraumes* (und damit einer *Domäne*) eindeutig einem *Subjekt* zugewiesen werden können. Ein *Subjekt* kann mehrere *E-Identities* haben.[6]

[6] Die Aussage gilt (im Rahmen von eCH-0107) für organisationsübergreifende Systeme. Es wird allerdings empfohlen, bezüglich Eindeutigkeit auch organisationsintern keine Einschränkungen zu machen.

linkedID (Relation)	Im organisationsübergreifenden Kontext erlaubt die Relation *linkedID*, E-Identities aus verschiedenen *Domänen* miteinander in Beziehung zu setzen. *E-Identities* können mit *linkedIDs* zu einem beliebigen gerichteten Graphen verkettet werden. Die konkrete Umsetzung von eCH-0107 kann die Form zusätzlich einschränken (z. B. statt Graph nur Baumstruktur) und regelt entsprechend ihrer Fähigkeiten die Interpretation (Semantik) des Graphen. (vgl. 7.3.3 *Broker Service*).
Authentifikator	Funktionales Abbild des *Authentifizierungsmittels* der Realwelt. Mit der Funktion eines Authentifikators wird aus einem Eingabewert und einem geheimen Wert ein Ausgabewert erzeugt.
Schnittstelle	
Authentifizierungs- und Attributbestätigung	Eine Bestätigung der erfolgreichen *Authentifikation* eines *Subjektes* (*Authentifizierungsbestätigung*, *Authentication Assertion*) oder eine Bestätigung eines Wertes eines *Attributs* (*Attribute Assertion*). Enthält einen *Identifikator*.
Identifikator	Eine Zeichenkette, welche eine *E-Identity* oder eine *E-Ressource* innerhalb eines *Namensraumes (Domäne)* eindeutig bezeichnet.
Credential	Stellt eine Menge von Daten dar, mit der eine *E-Identity* an ein *Authentifizierungsmittel* gebunden wird, welches vom *Subjekt* besessen und kontrolliert wird.
Ausgabewert des Authentifikators	Wird durch eine mathematische Funktion (*Authentifikator* oder Authentifizierungsfunktion) aus einem geheimen Wert (z. B. privater Schlüssel), einem oder mehreren optionalen Aktivierungswerten (z. B. PIN oder biometrischer Informationen), und einem oder mehreren optionalen Eingabewerten (z. B. Zufallswerten oder Challenges) generiert.

Tabelle 4 Beschreibung der Elemente des Informationsmodels

6 Prozesse

Abbildung 13 zeigt eine Übersicht über die Geschäftsprozesse. Sie dient zur Veranschaulichung der Tätigkeiten, welche für eine erfolgreiche Kooperation zwischen den Rollen in einem IAM-System (siehe Definitionen in Kapitel 3.1) notwendig sind. Die blau dargestellten Prozesse bilden die Kernprozesse, die grau dargestellten bilden die Führungs- und Steuerungsprozesse.

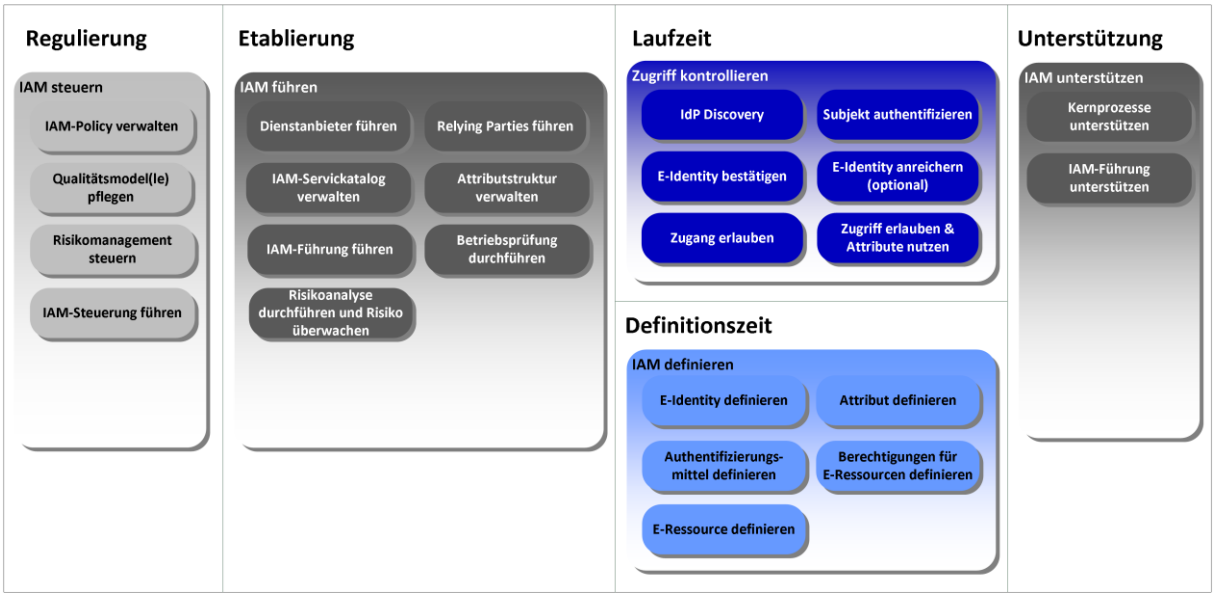


Abbildung 13 IAM-Prozesslandkarte

An diesen Prozessen beteiligen sich die verschiedenen Rollen gemäss Kapitel 3.1. Die nachstehenden Abschnitte beschreiben die Geschäftsprozesse mit ihren Teilprozessen.

Der erwähnte Prozesseigner ist typischerweise die Rolle, die die Verantwortung des Prozesses hat. Die Führung bestimmt und orchestriert aber auf Grund der Architektur und Topologie die Zugehörigkeit der Prozesse zu den Rollen.

Die Tätigkeiten sind zum Teil als ‘konditional’ oder ‘optional’ gekennzeichnet. ‘konditional’ bedeutet, dass die Tätigkeit vom Resultat einer anderen Tätigkeit oder einer ‘optionalen’ Tätigkeit abhängig ist. ‘optional’ gekennzeichnete Tätigkeiten können je nach definierter IAM-Architektur und/oder IAM-Policy ausgeführt werden.

6.1 Zugriff kontrollieren (Laufzeit)

Zugriff kontrollieren umfasst die Prozesse der Laufzeit. Ziel von *Zugriff kontrollieren* ist die kontrollierte und garantierte Einhaltung der Regeln für den *Zugriff* eines *Subjekts* auf eine *Ressource*. Beim *Zugriff* des *Subjekts* wird dieses *authentifiziert* und schliesslich, sofern berechtigt, *autorisiert*, auf die *Ressource* zuzugreifen. In einem föderierten IAM-System, in dem der Identity Provider und Relying Party über ein Netzwerk getrennte Systeme sind, muss die bei der Authentifizierung bestätigte E-Identity des Subjekts zusätzlich föderiert werden (Prozess *Identität bestätigen*).

Die Teilprozesse von *Zugriff kontrollieren* bauen in einer festgelegten Reihenfolge aufeinander auf (siehe Abbildung 14).

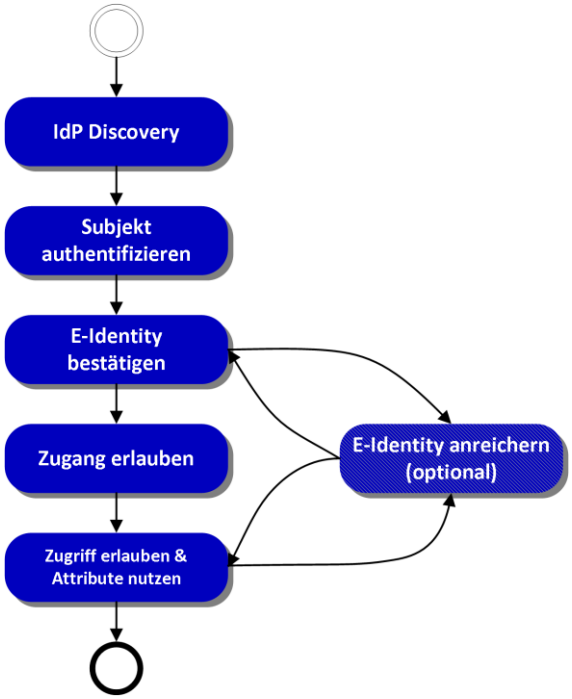


Abbildung 14 Ablaufdiagramm *Zugriff kontrollieren*

Im Sinne einer zuverlässigen Informationsbereitstellung stellt *Zugriff kontrollieren* sicher, dass nur genau die *Subjekte* auf die *Ressource Zugriff* erhalten, die *Zugriff* haben dürfen. Allen andern wird der *Zugriff* auf die *Ressource* oder bereits der *Zugang* zur *Ressource* verweigert.

Die Geschäftsservices, die die Prozesse zur Laufzeit unterstützen, sind in Abschnitt 7.3 beschrieben.

6.1.1 IdP Discovery

IdP Discovery	Bereitstellung einer Auswahl von IdPs für das Subjekt.

Prozesseigner: RP oder Vermittler

Anforderungen: LB-1.1, LB-7, LB-16, LE-10, Führ-3

Tätigkeiten:

- Der Prozesseigner wählt oder stellt eine Auswahl an IdPs zur Verfügung, von welcher das Subjekt einen wählen kann.
- Das Subjekt wählt einen IdP aus, von welchem er überzeugt ist, dass er sich authentifizieren kann.
    - (konditional) Falls das Subjekt keinen IdP auswählen kann (z. B. Liste ist leer, IdP nicht in der Liste vorhanden), muss dem Subjekt entsprechend unterstützt werden. Allenfalls den Prozess *Kernprozesse unterstützen* (6.5.1) anstossen.

6.1.2 Subjekt authentifizieren

Subjekt authentifizieren	Vorgang der zeitnahen Überprüfung einer behaupteten *E-Identity* eines *Subjekts* durch einen Identity Provider.

Prozesseigner: IdP

Anforderungen: LB-1, LB-9, LB-13, LB-16, LE-10, Führ-3

Tätigkeiten:

- Das *Subjekt* verwendet ein ihm zur Verfügung gestelltes und unter seiner Kontrolle befindliches *Authentifizierungsmittel*. (Credential Discovery)
- Das *Authentifizierungsmittel* generiert mit Hilfe des *Authentifikators* einen Ausgabewert aus den Eingaben des Subjekts. Das *Authentifizierungsmittel* übergibt den generierten Ausgabewert an einen Verifier zur Überprüfung.
- Der Verifier prüft den generierten Ausgabewert vom Authentifizierungsmittel mit dem *Credential* der behaupteten E-Identity. Ist die Prüfung positiv, ist die Authentifizierung erfolgreich und das Subjekt ist authentifiziert. Ist die Prüfung negativ, ist die Authentifizierung erfolglos und das Subjekt ist nicht authentifiziert.
- Der Prozess registriert und dokumentiert alle Aktionen und getroffenen Entscheidungen (Logging).

6.1.3 E-Identity bestätigen

E-Identity bestätigen	Erzeugen und übergeben der Bestätigung der E-Identity durch den IdP oder Vermittler an die RP.

Prozesseigner: IdP oder Vermittler (IAM-Führung bestimmt und orchestriert die Zuständigkeiten)

Anforderungen: LB-2, LB-2.1, LB-13, LB-16, LE-2, LE-8, LE-10, Führ-3

Beim Prozess *E-Identity bestätigen* wird je nach verwendetem Identity Federation Modell (siehe auch Anhang E) von einer anderen Rolle übernommen:

Tätigkeiten:

- Der Prozesseigner überprüft, ob die RP berechtigt ist, eine Authentifizierungsbestätigung anzufordern. Falls die Überprüfung erfolgreich ist, ist die RP berechtigt, Authentifizierungsbestätigungen zu erhalten. Falls die Überprüfung erfolglos ist, ist die RP nicht berechtigt und der Prozess wird abgebrochen.
- (optional) Der Prozesseigner holt das Einverständnis des Subjekts ein, die Authentifizierungsbestätigung an den aufrufenden Service (RP) zu übermitteln. Falls das Subjekt das Einverständnis gibt, wird die Authentifizierungsbestätigung an die RP übermittelt. Falls das Subjekt das Einverständnis nicht gibt, wird der Prozess abgebrochen.
- Der Prozesseigner erzeugt Authentifizierungsbestätigung mit Zeitstempel, Signatur, Identifikator (gemäss Anforderungen RP, Subjekt und IAM-Policy) und optionaler Verschlüsselung.

- (optional) Der Prozesseigner wählt eine AA, welche in der Definitionszeit mit der E-Identity verlinkt wurde.
- (optional) *E-Identity anreichern* (6.1.4) anstossen.
    - (optional bei Vermittler) Der Vermittler kann *E-Identity anreichern* (6.1.4) mehrmals ausführen und die Attribute aggregieren.
- (optional bei Vermittler) Der Vermittler transformiert die Protokolle gemäss der IAM-Führung erstellten Richtlinien.
- Der Prozesseigner übergibt die Authentifizierungsbestätigung an die RP.
- (konditional) Falls der Prozess *E-Identity anreichern* (6.1.4) angestossen wurde, übergibt der Prozesseigner die Attributbestätigung an die RP.
- In Abhängigkeit der verlangten Sicherheitsstufe muss die RP das Subjekt nach einer bestimmten Zeitdauer (unabhängig von ihren eigenen Richtlinien) erneut durch den IdP authentifizieren lassen (Re-Authentifizierung).
- Der Prozess registriert und dokumentiert alle Aktionen und getroffenen Entscheidungen (Logging).

Anmerkungen:

Falls der IdP und AA auf dieselbe Instanz fällt, wird dies als IdP/AA bezeichnet. In diesem Fall wird normalerweise die Authentifizierungs- und Attributbestätigungen vom IDP/AA erzeugt und beantworten.

6.1.4 E-Identity anreichern (optional)

E-Identity anreichern	Anreichern von Attributen zu der entsprechenden E-Identity.

Prozesseigner: AA

Anforderungen: LB-11, LB-13, LB-15, LB-16, LE-8, LE-10, Führ-3

Tätigkeiten:

- Der Prozesseigner überprüft, ob der aufrufende Service berechtigt ist, eine Attributbestätigung anzufordern. Falls die Überprüfung erfolgreich ist, ist der aufrufende Service berechtigt Attributbestätigung zu erhalten. Falls die Überprüfung erfolglos ist, werden die Attributwerte nicht übermittelt und/oder eine Fehlermeldung/Exception wird übergeben.
- Die Prozesseigner bereitet die entsprechenden Attribute auf.
- (konditional) Die AA holt das Einverständnis des Subjekts ein, die Attributbestätigung an den aufrufenden Service zu übermitteln. Falls das Subjekt das Einverständnis gibt, wird die Attributbestätigung übermittelt. Falls das Subjekt das Einverständnis nicht gibt, werden die Attributwerte nicht übermittelt und/oder eine Fehlermeldung/Exception wird übergeben.
- Die AA erzeugt eine Attributbestätigung mit Zeitstempel, Signatur, Identifikator (gemäss Anforderungen aufrufender Service, Subjekt und IAM-Policy) und optionaler Verschlüsselung.
- Der Prozesseigner übergibt die Attributbestätigung an den aufrufenden Service.

- Der Prozess registriert und dokumentiert alle Aktionen und getroffenen Entscheidungen (Logging).

Anmerkungen:

Die AA kann integraler Bestandteil von einem IdP sein. In diesem Fall spricht man von einem IdP/AA.

6.1.5 Zugang erlauben

Zugang erlauben	Grobautorisierung anhand der Zugangsregeln.

Prozesseigner: Vermittler oder RP

Anforderungen: LB-13, LB-16, LE-1, LE-10, Führ-3

Beim Prozess *Zugang erlauben* wird je nach verwendetem Identity Federation Modell (siehe auch Anhang E) von einer anderen Rolle durchgeführt.

Tätigkeiten:

- Vorbedingung einer *Grobautorisierung* ist die erfolgreiche *Authentifizierung* des *Subjekts*.
- Der Prozesseigner ermittelt die *Zugangsregeln* für den *Zugang* auf die *E-Ressource.*
- Der Prozesseigner überprüft, ob der Zugang autorisiert ist. Ist die Überprüfung positiv, erlaubt die zugehörige Rolle den *Zugang*. Falls die Überprüfung negativ ist, hat das Subjekt keinen Zugang.
- Der Prozess registriert und dokumentiert alle Aktionen und getroffenen Entscheidungen (Logging).

6.1.6 Zugriff erlauben und Attribute nutzen

Zugriff erlauben und Attribute offenlegen	Prüfen der *Zugriffsberechtigung* einer *grobautorisierten E-Identity* auf eine *E-Ressource* und Erteilen des *Zugriffs* auf eine E-*Ressource* zur Laufzeit. Offenlegen von Attributen des Subjektes.

Prozesseigner: RP

Anforderungen: LB-3, LB-3.1, LB-16, LE-1, LE-2, LE-2.1, LE-8

Tätigkeiten:

- Vorbedingung für einen Zugriff ist eine erfolgreiche Grobautorisierung.
- Die RP überprüft die Aktualität und Authentizität der Authentifizierungsbestätigung. Ist die Überprüfung positiv, ist die Authentifizierung erfolgreich und das Subjekt ist authentifiziert. Falls die Überprüfung fehlschlägt, ist das Subjekt nicht authentifiziert und der Zugriff wird verweigert.

- Die RP überprüft die Aktualität und Authentizität der erhaltenen Attributbestätigung. Ist die Überprüfung positiv, sind die Attributwerte gültig und aktuell. Falls die Überprüfung fehlschlägt, ist es in der Verantwortung der RP entsprechend zu reagieren.
- Die RP ermittelt die *Zugriffsrechte* für den *Zugriff* auf die *E-Ressource*. Daraus werden die benötigten *Attributwerte* zur *E-Identity* abgeleitet.
- Die RP überprüft, ob die benötigten Attributwerte (auch für die Erfüllung ihrer fachlichen Funktion) vorhanden sind.
    - (konditional) Der Prozesseigner wählt eine AA, welche in der Definitionszeit zu der mit der E-Identity in Verbindung gebracht wurde.
    - (konditional) Teilprozess *E-Identity anreichern* (6.1.4) anstossen.
- Sind die benötigten Attributwerte vorhanden, erlaubt die RP den *Zugriff*. Das Subjekt greift anschliessend auf die *Ressource* zu. Falls die benötigten Attributwerte nicht vorhanden sind, so ist das Subjekt nicht zugriffsberechtigt und erhält eine entsprechende Fehlermeldung.
- Der Prozess registriert und dokumentiert alle Aktionen und getroffenen Entscheidungen (Logging).

6.2 IAM definieren (Definitionszeit)

Während der Definitionszeit werden alle notwendigen Bedingungen geschaffen, damit zur Laufzeit bestimmt werden kann, ob ein *Subjekt* auf eine schützenswerte *Ressource* zugreifen darf. Die Abläufe der Definitionszeit müssen stattfinden, bevor *das Subjekt* die *Ressource* benutzt. Die Qualität von *Zugriff kontrollieren* wird sehr direkt durch die Umsetzung von *IAM definieren* beeinflusst.

IAM definieren wird typischerweise ausgelöst, wenn das Subjekt eine E-Identity benötigt oder wenn dem Subjekt Rechte für den Zugriff auf eine Ressource fehlen.

Die Teilprozesse von *IAM definieren* bauen aufeinander auf (siehe Abbildung 15).

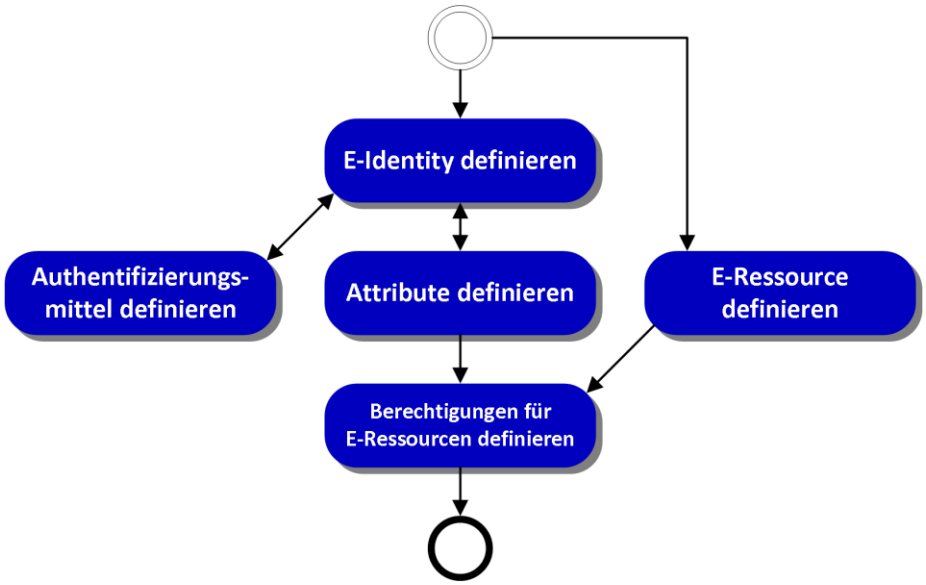


Abbildung 15 Ablaufdiagramm *IAM definieren*

Die Geschäftsservices, die die Prozesse der Definitionszeit unterstützen, werden im Abschnitt 7.2 genauer beschrieben.

6.2.1 E-Identity definieren

E-Identity definieren	Umfasst die Prozesse zum Registrieren, Aktualisieren und Deaktivieren von *E-Identities*.

Prozesseigner: RA oder Subjekt (bei Selbstregistrierung)

Anforderungen: LB-4, LB-5, LB-8, LB-9, LB-10, LE-5, LE-6, Dienst-1

Tätigkeiten:

- (optional) Das Subjekt wählt die RA aus der durch die IAM-Führung (6.3.1 Dienstanbieter führen) definierten Menge aus.
- (optional) Das Subjekt wird gemäss der gewünschten Vertrauensstufe durch die RA identifiziert und seine Beweismittel verifiziert. Ist die Überprüfung positiv, registriert die RA die zugehörige *E-Identity.* Falls die Überprüfung negativ ist, kann die E-Identity nicht mit der gewünschten Vertrauensstufe registriert werden.
- (konditional) Möchte das Subjekt eine juristische Person vertreten, muss die RA die Bindung zur juristischen Person anhand von Beweismitteln verifizieren. Bei erfolgreiche Überprüfung werden entsprechende Attributwerte beantragt.
- (optional) Die RA erhebt Daten, um die Anwesenheit des Subjekts bei der Registrierung zu einem späteren Zeitpunkt beweisen zu können.
- Bei Selbstregistrierung (Subjekt registriert sich selbst) entfällt die Vorlage von Beweismitteln und deren Überprüfung. Attribute können selbstdeklariert sein.
- (optional) Der Prozesseigner verlinkt *E-Identities* miteinander.
- Die Prozesseigner aktualisiert (z. B. bei Step-Up Registrierung) und deaktiviert *E-Identities*. Er stösst die nächsten Prozesse an (*Attribute definieren* und *Authentifizierungsmittel definieren*).

Anmerkungen:

Die *E-Identity* ist das zentrale Element jeder *IAM*-Umgebung. Ein registriertes *Subjekt* hat innerhalb einer *Domäne* immer mindestens eine *E-Identity*.

6.2.2 Attribut definieren

Attribut definieren	Erfassen, Aktualisierung und Löschung von *Attributwerten*.

Prozesseigner: AA

Anforderungen: LB-6, LE-5, LE-6, Dienst-1, Führ-1

Tätigkeiten:

- Vorbedingung zum Definieren von Attributwerten ist eine vorhandene E-Identity (*E-Identity definieren* 6.2.1), der die Attributwerte zugewiesen werden können.
- Das Subjekt oder die RA des CSPs beantragt während der (Selbst-)Registrierung einen neuen *Attributwert* oder die Aktualisierung eines bestehenden *Attributwertes* bei der AA. Die RA ist für die Überprüfung der Attributwerte zuständig.
- (optional) Die RA der AA erhebt Attributwerte gemäss der gewünschten Qualitätsstufe.
- (nur RBAC) Die RA kann dem Subjekt (Rollen-)Attributwerte zuweisen, die dem Subjekt vom Berechtigungsverwalter zugeteilt wurden (RBAC/antragsbasiertes Verfahren). Ein entsprechender Attributwert wird beantragt.
- (optional) Das Subjekt kann seine Rechte zeitlich begrenzt und kontextbezogen an ein anderes Subjekt übertragen.
- Die AA teilt der *E-Identity* den *Attributwert* zu oder aktualisiert ihn.
- Die AA löscht ggf. *Attributwerte*.

Anmerkungen:

Je nach Organisation und Identity Federation Modell kann die RA für die CSP und AA dieselbe sein. Die IAM-Führung bestimmt wie die Verantwortungen aufgeteilt werden.

Ein *Attributwert* repräsentiert eine einem *Subjekt* zugeordnete *Eigenschaft*, die das *Subjekt* näher beschreibt. Der Prozess, wie diese *Eigenschaften* zu erheben und prüfen sind, muss entsprechend der verlangten Qualität dokumentiert werden.

6.2.3 Authentifizierungsmittel definieren

Authentifizierungsmittel definieren	Erstellen, Vergabe und Erneuerung von *Authentifizierungsmitteln* für eine E-Identity.

Prozesseigner: CSP

Anforderungen: LB-6, LB-8, LB-9, Dienst-1, Dienst-2, Führ-1

Tätigkeiten:

- Vorbedingung ist eine vorhandene E-Identity, der die Authentifizierungsmittel zugewiesen werden können.
- Der CSP erstellt, erhebt und vergibt *Authentifizierungsmerkmale* (z. B. Passwörter, Authentisierungszertifikat) oder bindet Authentifizierungsmittel an die E-Identity des Subjektes, die bereits unter Kontrolle des Subjektes sind.
- (optional) Der CSP publiziert die öffentlichen Elemente der *Authentifizierungsmittel* (z. B. öffentlicher Schlüssel) zur *E-Identity*.
- Der CSP händigt das *Authentifizierungsmittels* (ev. mehrere) gemäss gewünschter Vertrauensstufe an das *Subjekt* aus.

- Der CSP erneuert bzw. ersetzt benutzerfreundlich *Authentifizierungsmittel*.
- Der CSP revoziert *Authentifizierungsmittel*.

6.2.4 E-Ressource definieren

E-Ressource definieren	Identifikation, Registrierung und Löschen von *E-Ressourcen*.

Prozesseigner: IAM-Führung (RP)

Anforderungen: LB-16, LE-1, LE-3

Tätigkeiten:

- Die IAM-Führung (RP) identifiziert *Ressourcen* und registriert die zugehörige *E-Ressource* (mit *Identifikator*).
- Die IAM-Führung (RP) legt den *Schutzbedarf* der E-Ressource fest.
- Die IAM-Führung (RP) löscht oder deaktiviert die *E-Ressource*, sowie dessen Identifikator.

Anmerkungen:

- Eine *Relying Party* hat innerhalb einer *Domäne* immer mindestens eine *E-Ressource*.

6.2.5 Berechtigungen für E-Ressourcen definieren

Berechtigungen für E-Ressourcen definieren	Zuweisen, Aktualisieren und Löschen von *Zugangsregeln* zur *Grobautorisierung* und *Zugriffsrechten* zur *Feinautorisierung* der *E-Identities* für den Zugriff auf *Ressourcen*.

Prozesseigner: RP

Anforderungen: LB-17, LE-1, LE-4

Tätigkeiten:

- Der Prozesseigner verwaltet *Zugangsregeln* und *Zugriffsrechte* unter Verwendung der verfügbaren *Attribute* von *E-Identities,* Kontext des Zugriffs (Lokation, Zeitpunkt, Sicherheitsniveau usw.) und optional eigenen Daten (nur bei Zugriffsrechten).
- Der Prozesseigner weist *Zugangsregeln* und *Zugriffsrechte* zu einer oder mehreren *E-Ressourcen* zu.
- Der Prozesseigner aktualisiert und löscht *Zugangsregeln* und *Zugriffsrechte.*
- (optional) Der Prozesseigner kann *Zugangsregeln* an den Vermittler auslagern.

6.3 IAM führen (Etablierung)

Der Geschäftsprozess *IAM führen* beinhaltet, unter Berücksichtigung der Rahmenbedingungen der IAM-Steuerung und nur innerhalb eines organisatorischen Kontextes, die notwendigen Aktivitäten für die Erreichung der definierten IAM Ziele, die Etablierung und Verwaltung der (ausführenden) Geschäftsprozesse und der „Roadmap“ für die Weiterentwicklung des IAM-Systems.

Diese Prozesse beschreiben die Abläufe für die Definition der notwendigen Vorgaben und Rahmenbedingungen für den Betrieb der *IAM* Umgebung, wie z. B. das Definieren des Angebots, das Definieren der Regeln und Abläufe, dem Festlegen der Revision der Ausführung etc.

6.3.1 Dienstanbieter führen

Dienstanbieter führen	Beziehungsaufnahme, -pflege und -beendung mit den IAM-Dienstanbietern des IAM-Systems inkl. der Etablierung der Vertrauensbeziehungen

Prozesseigner: IAM-Führung (IAM-Gesamtsystem)

Anforderungen: Führ-5, Führ-5.1, Reg-1

Tätigkeiten:

- Definieren, welche IAM-Dienstanbieter (IdP, AA, CSP, RA, Vermittler) in den Verbund aufgenommen werden.
- *IAM-Dienstanbieter* in den Verbund aufnehmen und entfernen (z. B. wegen End-Of-Life oder Nichteinhalten der Sicherheitsvorgaben).
- Vertrags- und/oder SLA Management mit den verschiedenen IAM-Dienstanbietern oder Akzeptanz der geltenden AGBs von IAM-Dienstanbietern.
- Festlegung der IAM-Organisation (Rollen) sowie ihrer Beziehung untereinander (Zusammenarbeit).
- (konditional) Falls die IAM-Steuerung im Prozess *IAM-Policy verwalten* (6.4.1) den Vertrauensanker nicht festgelegt hat, muss der Vertrauensanker über die Auswahl der Certificate Authority (CA) festgelegt werden.
- Bestimmen und Nachführen der Vertrauensstufen für die Authentifizierung.
- (Optional) Bestimmen und Nachführen der Qualitätsstufen der Attribute.
- Auswirkungsanalyse von Änderungen an den Vertrauensbeziehungen.

6.3.2 Relying Parties führen

Relying Parties führen	Beziehungsaufnahme, -pflege und -beendung mit den *Relying Parties (RP)* inkl. der Etablierung der Vertrauensbeziehungen

Prozesseigner: IAM-Führung (IAM-Gesamtsystem)

Anforderungen: Führ-5, Führ-5.1, Reg-1

Tätigkeiten:

- Aufnahme von RPs prüfen, z. B. Erfüllung der Sicherheitsanforderungen basierend auf dem Schutzbedarf prüfen.
- Vertrags- und/oder SLA-Management mit den RPs.
- RPs in den Verbund aufnehmen und entfernen (z. B. wegen End-Of-Life, Weiterentwicklung der E-Ressource oder Nichteinhalten der Sicherheitsvorgaben). Prozess *E-Ressource definieren* (6.2.4) anstossen
- Prüfen der notwendigen Attribute (Vorhandensein und Qualität) und allenfalls Prozess *Attributstruktur verwalten* (6.3.3) anstossen.
- Auswirkungsanalyse vor Änderungen an den Vertrauensbeziehungen.
- (Optional) Im Fall, dass es mehrere Domänen gibt, Zugehörigkeit bestimmen.

6.3.3 Attributstruktur verwalten

Attributstruktur verwalten	Definition und Weiterentwicklung der Attributdefinition.

Prozesseigner: IAM-Führung (AA)

Anforderungen: LE-7, Führ-1

Tätigkeiten:

- Attributquellen suchen und prüfen.
- (konditional) Falls keine Attributquelle vorhanden ist, muss der Prozess für Attributwertbestätigung entsprechend der gewünschten Qualitätsstufe definiert werden.
- Meta-Attribute definieren, harmonisieren und nachführen.
- Attribute klassifizieren (Bsp. Persönliche- und Enterprise-Attribute).

6.3.4 Betriebsprüfung durchführen

Betriebsprüfung durchführen	Prüfen der korrekten Umsetzung und Betriebes des IAM-Systems.

Prozesseigner: IAM-Führung

Anforderungen: Reg-1, Reg-2

Tätigkeiten:

- Auditieren und kontrollieren der Umsetzung der Vorgaben, Qualitätsanforderungen, Regeln und Regularien.
- Reporting aller relevanten Aktivitäten.

- Massnahmen zur Verbesserungen definieren und/oder Prozesse *IAM-Führung führen* (6.3.7) anstossen.

6.3.5 IAM-Servicekatalog verwalten

IAM-Servicekatalog verwalten	Erstellen und Pflegen des IAM-Servicekatalogs

Prozesseigner: IAM-Führung (Gesamtsystem) und IAM-Führung (Dienstanbieter)

Anforderungen: Dienst-3

Tätigkeiten:

- Definieren der IAM-Service-Strategie.
- Definieren und Nachführen des Service-Katalogs und die zu realisierenden IAM-Architekturen.
- Marktanalyse für das Betreiben der Services (intern und extern)
- Roadmap für die Weiterentwicklung der IAM-Services.
- Informationsaustausch und Kommunikation mit den Relying Parties.
- Sicherstellen der Finanzierung für den Betrieb und für die Weiterentwicklung.
- Abwickeln von Weiterentwicklungs-Anfragen und allenfalls Prozess *IAM-Führung führen* (6.3.7) anstossen.

6.3.6 Risikoanalyse durchführen und Risiko überwachen

Risikoanalyse durchführen und Risiko überwachen	Durchführen von Risikoanalyse und Risikobeurteilung. Definieren von risiko-mitigierenden Massnahmen und Risiko-Überwachung. Festhalten der Resultate.

Prozesseigner: IAM-Führung

Anforderungen: Reg-1, Reg-3

Tätigkeiten:

- Durchführen von Risikoanalysen und Festhalten der Resultate, damit Gefahren zeitnah erkannt werden können..
- Risikobeurteilung und Schutzbedarfsanalyse des IAM-Systems: Die Schutzbedarfsanalyse gewährleistet angepasste Sicherheitsanforderungen (so viel Sicherheit wie nötig, nicht so viel wie möglich).
- Risiko-mitigierende Massnahmen definieren und auslösen.
- Implementieren des Informations- und Datenschutzkonzepts, sowie Feedback an IAM-Regulator bezüglich des Informations- und Datenschutzkonzeptes.

- (Optional) Abstützung des Risikomanagements auf ein Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001, ISM3[7] oder nach ISO 31000 [5]. Abstützung des Risikomanagements auf ein Framework wie COBIT.
- Abstimmung mit dem IAM-Regulator.

6.3.7 IAM-Führung führen

IAM Führung führen	Festlegung der Zusammenarbeit der (IAM-)Führungen im IAM-Gesamtsystem.

Prozesseigner: IAM-Führung (IAM-Gesamtsystem)

Anforderungen: Dienst-3, Führ-5

Tätigkeiten:

- Festlegung der Zusammenarbeit der IAM-Führungen im IAM-Gesamtsystem.
- Definition und kontinuierliche Verbesserung der Kern-, Support- und Führungsprozesse.
- Erstellen und Bereitstellen von stufengerechten Kommunikationsmittel für diverse Stakeholder.
- Bestimmen des Zeitservers.
- Definieren, Aktualisieren und Widerrufen der Vertrauensbeziehungen (Trust) zwischen IAM-Dienstanbietern und Relying Parties. Festlegen, wie die Qualität- und Vertrauensstufen zwischen IdP/AA (oder Vermittler) und RP übermittelt werden.
- Zertifizieren von CSPs.
- Pflegen der Metadaten zu den IAM-Dienstanbietern und RPs.
- Führung der internen IAM-Dienstanbieter.

6.4 IAM steuern (Regulierung)

Der Geschäftsprozess *IAM steuern* beinhaltet, unter Berücksichtigung der organisatorischen Rahmenbedingungen und nur innerhalb eines organisatorischen Kontexts, die notwendigen Aktivitäten für die Definition der IAM Ziele, der notwendigen Rahmenbedingungen und die Masterplanung für die Führung des IAM-Gesamtsystems.

Diese Prozesse beschreiben die Abläufe für die Definition der notwendigen Vorgaben und Rahmenbedingungen für die Führung der IAM-Umgebung, wie z. B. das Definieren der Regeln und standardisierten Abläufe, dem Festlegen der Revision der Führung etc.

[7] ISM3 ist eine ISMS komplett auf ISO 27001 abbildbar, nimmt aber zusätzlich die Maturität der Organisation in Betracht.

6.4.1 IAM-Policy verwalten

IAM Policy verwalten	Festlegung der *IAM*-Policy und der IAM-Architektur des IAM-Systems.

Prozesseigner: IAM-Regulator

Anforderungen: Führ-2, Reg-2

Tätigkeiten:

- Ableiten und Nachführen der IAM-Strategie.
- Definieren der IAM-Architektur.
- Definition der *Rollen* mit entsprechenden Aufgaben, Kompetenzen und Verantwortung.
- Erarbeiten der notwendigen Basiskonzepte basierend auf den IAM-Architekturen, z. B. Identitätstypenkonzept und Rechtetypenkonzept.
- Erarbeiten und aktualisieren der relevanten Vorgaben: Identifikation der geltenden gesetzlichen, unternehmensinternen und vertraglichen Richtlinien / Regularien.
- Definieren und Nachführen von Hilfsmitteln für die Anwendung der IAM-Architekturen und Vorgaben. Bsp. Vertrauensstufen-Rechner.
- Definition der Nachvollziehbarkeitsanforderungen, z. B. das Ablegen der relevanten Dokumente und die Aufbewahrungsfristen der relevanten Daten (siehe auch ISO 29115 [6] Kapitel „Record-keeping/recording).
- Definieren der relevanten standardisierten Kern-, Support- und Führungsprozessen. Spezialisierung zu diesem Dokument.
- (optional) Festlegen der Vertrauensanker über die Auswahl der Certificate Authority (CA). Dies die IAM-Führung delegiert werden.
- Festlegen des Lebenszyklus von E-Identities, Attributen, Berechtigungen, IAM-Dienstanbietern und RPs.
- (konditional) Festlegen des Lebenszyklus einer Verknüpfung von natürlichen und juristischen Personen (z. B. Aktivierung, Aussetzung, Erneuerung, Widerruf) (siehe auch eIDAS 2015/1502 [7], Abschnitt 2.1.4).
- (Optional) Maturitätsmodell und Maturitätsstufen festlegen (z. B. nach eCH-0172 [8]).
- Überprüfen, ob die Richtlinien eingehalten werden. Ausnahmen, die die IAM-Führung beantragt, überprüfen.

6.4.2 Qualitätsmodel(le) pflegen

Qualitätsmodel(le) pflegen	Festlegen, wie die Qualität der Authentifizierung eines Subjektes und die Qualität der Attribute bestimmt, überprüft und verglichen werden kann.

Prozesseigner: IAM-Regulator

Anforderungen: Prinzip-5, IAM-1, LE-7, Reg-2

Tätigkeiten:

- Qualitätsmodell für die Authentifizierung von Subjekten, dessen Kriterien und dessen Unterteilung definieren (z. B. nach eCH-0170 [9]).
- Falls es Attribute gibt, sollte das Qualitätsmodell der Attributwertbestätigungen, dessen Kriterien und dessen Unterteilung definiert werden (z. B. nach eCH-0171 [10]).
- (Optional) Die Interoperabilität zwischen den Qualitätsmodellen festlegen.

6.4.3 Risikomanagement steuern

Risikomanagement steuern	Kontext etablieren und Identifizieren der Risiken. Welche Risiken müssen bei der Etablierung, Definitionszeit, Laufzeit und der Unterstützung beachtet werden? Leitplanken für die IAM-Führung, welche Risiken gemanagt werden müssen.

Prozesseigner: IAM-Regulator

Anforderungen: Führ-5, Reg-1, Reg-3

Tätigkeiten:

- Definieren der IAM-Sicherheitsziele
- Kontext etablieren; Die Festlegung des Kontexts definiert den Umfang des Risikomanagementprozesses und legt die Kriterien fest, anhand derer die Risiken bewertet werden.
- Definieren, wie viel Risiko die Organisation bereit ist zu nehmen (Risikobereitschaft) und wie viel Risiko die Organisation nehmen kann (Risikotoleranz)
- Risikoidentifikation durchführen, z. B. nach ISO 31000 [5]. Überprüfung der wichtigsten organisatorischen Risikokategorien, die bei der Festlegung des Kontexts berücksichtigt wurden, Erstellung einer Übersicht mit potenziellen Risiken, die sich auf das Unternehmen auswirken können.
- Abgleich und Integration mit dem Organisationsrisikomanagementsystem und Ziele.
- Erstellung des Informations- und Datenschutzkonzepts (inkl. Hilfsmittel) für die Implementierung durch die IAM-Führung.
- Analyse der Risikoberichte der IAM Führung und Freigabe dieser Berichte.

- Kontinuierliche Verbesserung des Informations- und Datenschutzkonzepts, z. B. analog ISO 27001 [11]. Aufgrund der Ist-Situation werden periodisch Verbesserungsmöglichkeiten identifiziert, allenfalls basierend auf der Risikobereitschaft Massnahmen geplant, umgesetzt und überprüft.
- Überwachen von bekannten/publizierten externen Sicherheitsvorfälle und Risikobeurteilungsaufträge an die IAM-Führung(en) erteilen.
- (Optional) Abstützung des Risikomanagements auf ein Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001, O-ISM3[7] oder nach ISO 31000 [5] Abstützung des Risikomanagements auf ein Framework wie COBIT.

6.4.4 IAM-Steuerung führen

IAM Steuerung führen	Integration der IAM Steuerung im Gesamtsystem und die Definition und kontinuierliche Verbesserung der IAM-Steuerungsprozesse.

Prozesseigner: IAM-Steuerung

Anforderungen: Führ-5

Tätigkeiten:

- Identifikation / Festlegung der Zusammenarbeit von *Steuerungs- und Führungsdomänen*: Bei der Föderation erfolgt *IAM* in der Regel über mehrere *Domänen*. Die Organisation und Abläufe zwischen den *Domänen* sind klar zu regeln.
- Veränderungen in den Regulatorien und Vorgaben verfolgen und allfällige, daraus resultierende Massnahmen identifizieren.
- Bestimmung der Methoden, Notationen, externen Standards und Frameworks, die im IAM-Gesamtsystem anzuwenden sind.
- Interoperabilität im IAM-Gesamtsystem, bezüglich Methoden, Notationen, usw. gewährleisten.
- Kontinuierliche Verbesserung von *IAM steuern*. Aufgrund der Ist-Situation werden periodisch Verbesserungsmöglichkeiten identifiziert, allenfalls basierend auf der Risikobereitschaft Massnahmen geplant, umgesetzt und überprüft.
- Unterstützende / befähigende Aufgaben (Intern / Rahmenbedingungen) ausführen, wie z. B. Konventionen für Dokumentation der IAM-Policy festlegen und Abgleich mit den Organisationskonventionen.

6.5 IAM unterstützen

Der Geschäftsprozess *IAM unterstützen* beinhaltet, unter Berücksichtigung der organisatorischen Rahmenbedingungen und nur innerhalb eines organisatorischen Kontexts, die notwendigen Aktivitäten für die Unterstützung für den Aufbau und Betrieb einer IAM Umgebung. Dies sind zusätzliche Prozesse, welche in den Kern- und Führungsprozess nicht vorhanden sind.

6.5.1 Kernprozesse unterstützen

Kernprozesse unterstützen	Der Prozess *Kernprozesse unterstützen* umschliesst die Aktivitäten zum Aufnehmen, Verwalten, Verfolgen und schliesslich Lösen von Problemen, die zur Lauf- oder Definitionszeit auftreten können.

Prozesseigner: IAM-Support

Anforderungen: LB-12, LB-14, LE-9, Führ-4, Führ-6

Tätigkeiten:

- Annahme und Bearbeitung von Problemfällen in Interaktion zwischen Subjekt, Ressource und allen beteiligten Dienstanbietern.
- Einrichten und Betrieb eines Monitoring- (zur Überwachung von Ereignissen, z. B. Serviceausfall) und Tracking-Systems zur Bearbeitung und Nachvollziehen von Problemfällen.
- Unterstützung und Einleiten von Massnahmen im Falle eines sicherheitsrelevanten Ereignisses (z. B. Cyberangriff).
- Unterstützung bei Verdacht auf Missbrauch einer E-Identity.
- Gewährleisten der Interoperabilität von mehreren Monitoring- und Tracking-Systemen.
- Integrieren Support-Prozessen anderer IAM-Dienstanbieter.

6.5.2 Führungsprozesse unterstützen

Führungsunter unterstützen	Der Prozess *Führungsprozesse unterstützen* umschliesst die Aktivitäten für die Unterstützung und Beratung der IAM-Führung während der Etablierung.

Prozesseigner: IAM-Support (Regulator)

Anforderungen: Führ-4

Tätigkeiten:

- Kommunikation und Schulung der IAM-Policy.
- Erstellen von stufengerechten Kommunikationsmitteln für die diversen Stakeholder.
- (Optional) Unterstützung bei IAM-Projekten und Spezialvorhaben.
- IAM-Führung beraten.

7 Geschäftsservices

Nachfolgend werden alle *IAM*-Services, welche von den verschiedenen Rollen (siehe Kapitel 3.1) angeboten werden, beschrieben. Es handelt sich dabei um Geschäftsservices und nicht um technische Service-Komponenten, d.h. bei einer Realisierung können ein oder auch mehrere Geschäftsservices von einer technischen Service-Komponente implementiert oder auch ein Geschäftsservice auf mehrere technischen Service-Komponenten verteilt werden.

Die Modelle dieses Kapitels beschreiben sowohl die Laufzeit, wenn ein Subjekt versucht auf eine Ressource zuzugreifen, als auch die Definitionszeit, während der die verschiedenen (Meta)-Daten erfasst und gepflegt werden. Geschäftsservices zur Unterstützung der Prozesse *IAM steuern, IAM führen* und *IAM unterstützen* (vgl. Abschnitt 7) sind in diesem Standard nicht dargestellt.

In den Abbildungen werden die Services der Definitionszeit (hellblau dargestellt) und die Services der Laufzeit (dunkelblau dargestellt) optisch von den Realweltobjekten (grün dargestellt) abgetrennt.

Das *Identitäts- und Berechtigungsmanagement* der hier vorgestellten *IAM*-Geschäftsservices ist nicht Inhalt dieses Standards. Grundsätzlich kann jede Verwendung eines Services nach den Realweltobjekten *Subjekt* und *Ressource* aufgelöst betrachtet werden und der vorliegende Standard rekursiv angewandt werden. Ob dies sinnvoll ist, muss im konkreten Anwendungsfall entschieden werden.

7.1 Realweltobjekte

Die Realweltobjekte und ihre Aufgaben werden nachfolgend genauer beschrieben. Sie sind in allen Modellen immer hellgrün dargestellt.

7.1.1 Subjekt

Subjekt	Eine *natürliche Person*, eine handelnde *Organisation*, ein *Service* oder ein *Ding*, das auf eine *Ressource* zugreift oder zugreifen möchte. Ein Subjekt wird durch *E-Identities* repräsentiert.

Aufgaben (zur Laufzeit):

- *Authentisiert* sich.
- (optional, nur für natürl. Personen) Gibt die Authentifizierungsbestätigung für die RP frei.
- (optional, nur für natürl. Personen) Gibt den Versand der *Attribute* frei.
- Greift auf *Ressourcen* zu.

7.1.2 Ressource

Ressource	Service oder Daten, auf welche ein *Subjekt* zugreifen kann, wenn es sich *authentisiert* hat und es auf der Basis der benötigten *Attribute autorisiert* wurde.

Aufgaben (zur Laufzeit):

- Stellt dem *Subjekt* ihre fachliche Leistung (Funktionalität) zur Verfügung (die dem *Identifikator* entsprechenden Informationen oder Services)

7.2 Services zur Definitionszeit

In Abbildung 16 sind die Services zur Definitionszeit (in den Modellen hellblau), die zur Verwaltung der verschiedenen Objekte benötigt werden, dargestellt. Die erste Gruppe bezieht sich auf das Subjekt. Die zweite Gruppe definiert Objekte in Abhängigkeit der *Ressource*.

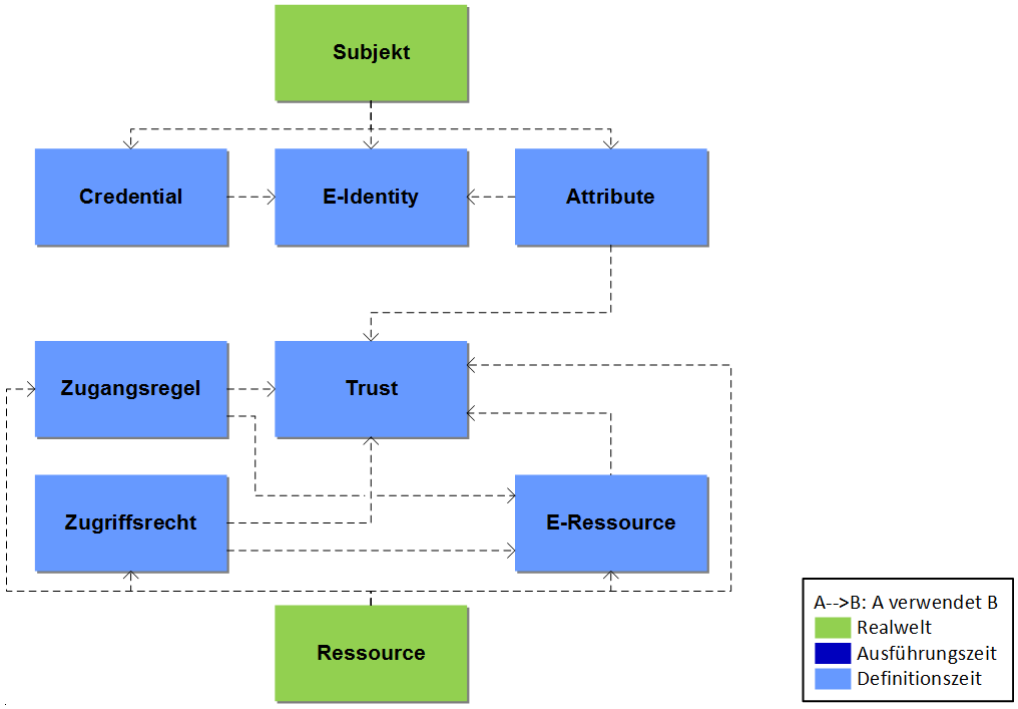


Abbildung 16 Geschäftsservices – Definitionszeit

7.2.1 E-Identity Service

E-Identity Service	Der *E-Identity Service* stellt zu *Subjekten E-Identities* aus und verwaltet sie.

Schnittstellen:

In: Subjekt,

(*E-Identities)*

Out: *E-Identities*

Aufgaben:

- Ermöglicht die Registrierung von *Subjekten*
- Stellt Funktionen zur Ausgabe, Pflege und Verwaltung von *E*-Identities und deren Beziehungen bereit.

- Stellt die Überprüfung der Identität des *Subjekts* anhand definierter Regeln abhängig von der angestrebten Qualität sicher (Vertrauenskette zwischen *E-Identity* und *Subjekt*).
- Kennt andere *E-Identity Services* und ermöglicht die Pflege der *linkedID* zu anderen *E-Identities* des *Subjekts*.
- Stellt in geeigneter Weise die Qualität und Aktualität der *E-Identity* sicher.
- Begrenzt die Lebensdauer von *E-Identities* und unterstützt die *Subjekte* bei der Erneuerung ihrer *E-Identities*.
- Kann *E-Identities* widerrufen/deaktivieren.
- Unterstützt *Profile* zur Trennung von Verantwortungen (Segregation of Duties, SoD).
- Gewährt zur Definitionszeit vertrauenswürdigen *Credential Services* und *Attribute Services* elektronischen Zugang zu den *E-Identities*.
- Gewährt zur Laufzeit vertrauenswürdigen *Authentication Services* und *Attribute Assertion Services* elektronischen Zugang zu den *E-Identities*.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.

7.2.2 Credential Service

Credential Service	Der *Credential* Service gibt *Authentifizierungsmittel* aus und verwaltet sie. Er ermöglicht eine benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln. Ein *Authentifizierungsmittel* bezieht sich auf eine *E-Identity* und ist auf ein bestimmtes *Subjekt* ausgestellt.

Schnittstellen:

In: E-Identity,

Authentifizierungsfaktoren,

(Authentifizierungsmittel)

Out: *Authentifizierungsmittel, Credential*

Aufgaben:

- Registriert *Authentifizierungsmittel* unter allfälliger Verwendung von *Authentifizierungsfaktoren* des *Subjekts*
- Stellt Funktionen zur Ausgabe, Verwaltung und Zustellung der *Authentifizierungsmittel* zur Verfügung.
- Ermöglicht eine benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln.
- Verwendet für kryptografische Schlüssel ein Schlüsselmanagement (nicht Teil des IAM-Geschäftsservices).

- Stellt die Vertraulichkeit, Integrität und Verfügbarkeit der Credentials sicher
- Ermöglicht die Überprüfung der Gültigkeit der verwalteten *Authentifizierungsmittel* und der Zugehörigkeit zu einer *E-Identity* bzw. dem zugehörigen *Subjekt*.
- Begrenzt die Lebensdauer der ausgegebenen *Authentifizierungsmittel* und unterstützt die *Subjekte* in der Erneuerung ihrer *Authentifizierungsmittel*.
- Kann *Authentifizierungsmittel* widerrufen.
- Gewährt zur Laufzeit vertrauenswürdigen *Authentication* Services elektronischen Zugang zu den *Credentials*.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.

7.2.3 Attribute Service

Attribute Service	Der *Attribute* Service pflegt zeitnah ein oder mehrere *Attribute* für definierte *Subjekte*.

Schnittstellen:

In: *E-Identity*, Eigenschaften des Subjektes

Out: *Attribute*

Aufgaben:

- Stellt Funktionen zur Pflege und Verwaltung der Informationen bereit, welche nötig sind, um bestimmen zu können, ob ein *Subjekt* eine definierte *Eigenschaft* erfüllt oder nicht (z. B. "Hans Meier ist Vermesser des Kantons Bern").
- Bildet die *Eigenschaften* als *Attribute* ab und verbindet die *Attribute* mit der *E-Identity* des Subjekts, dabei werden die Metadaten der Attribute des *Trust Service* verwendet.
- Ermöglicht Mutationen von *Attributen* inkl. deren Widerruf
- Stellt in geeigneter Weise die Qualität und Aktualität der *Attribute* sicher (kann z. B. deren Lebensdauer beschränken)
- Muss allenfalls auch Identitätsinformationen vom *E-Identity Service* abfragen können (z. B. Verifikation der *E-Identity*).
- Definiert die Metadaten und die Semantik der *Attribute* der *E-Identities*.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.

Anmerkungen:

- *Attribute* beschreiben immer die zugehörige *E-Identity*, können aber durch den gemeinsamen Kontext von *Subjekten* (z. B. gemeinsamer Arbeitgeber) gegeben sein. Diese *Attribute* sind in der Pflege vom Lifecycle der *E-Identity* unabhängig. Nur die Beziehung der *E-Identity* zu diesen *Attributen* hängt vom Lifecycle der *E-Identity* ab.

7.2.4 Trust Service

Trust Service	Der *Trust* Service pflegt die akzeptierten, vertrauenswürdigen *IAM-Dienstanbieter* und Relying Parties.

Schnittstellen:

In: Informationen darüber wer wem bezüglich was vertraut,

Metadaten der RPs und IAM-Dienstanbieter,

Metadaten der Attribute der AAs

Out: Trust,

Metadaten der RPs und IAM-Dienstanbieter,

Aufgaben:

- Registriert, pflegt und verwaltet die Vertrauensbeziehungen (inkl. deren Lebenszyklus) der Ressourcen (*Relying Party*) zu den *IAM-Dienstanbietern* und den *IAM-Dienstanbietern* untereinander.
- Macht Vertragsdefinitionen.
- Definiert die Trust-Anchor über die Auswahl der Credential Service Provider (CSP).
- Registriert die Services der *IAM-Dienstanbieter* und deren Qualität (z. B. autoritative Datenquellen).
- Wählt die Metadaten und die Semantik der *Attribute* der *E-Identities* und der *E-Ressourcen* für den *Broker* Service und die anderen Metadaten-abhängigen Geschäftsservices.
- Kennt andere *Trust* Services und kann ihre Informationen nutzen.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.

7.2.5 E-Ressource Service

E-Ressource Service	Der *E-Ressource* Service stellt zu *Ressourcen E-Ressourcen* aus und verwaltet sie.

Schnittstellen:

In: *Ressource* einer Relying Party

Out: *E-Ressource und Metadaten*

Aufgaben:

- Stellt Funktionen zur Definition und Verwaltung von *E-Ressourcen* bereit.
- Eine *Ressource* kann durch mehrere *E-Ressourcen* repräsentiert sein.
- Ordnet jeder *E-Ressource* genau einen eindeutigen *Identifikator* zu.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.

- (optional) Klassifiziert E-Ressourcen entsprechend ihres Schutzbedarfes bezüglich Vertraulichkeit, Integrität und Verfügbarkeit

7.2.6 Zugangsregel Service

Zugangsregel Service	Der *Zugangsregel Service* verwaltet die Regeln für den Zugang zu einer *E-Ressource*. Die Regeln sind auf der Basis von *Authentisierung* oder *Attributen* definiert.

Schnittstellen:

In: Trust-Beziehungen,

E-Ressourcen,

Art und Qualität der Attribute (Metadaten der Attribute),

Art und Qualität der Authentifizierung

Out: *Zugangsregeln*

Aufgaben:

- Stellt Funktionen zur Verwaltung der *Zugangsregeln* bereit, die den Zugang zu den *E-Ressourcen* regeln (*Grobautorisierung*). Die *Zugangsregeln* enthalten Angaben zur *Authentisierung* und zu *Attributen* (inklusive deren Qualität), die ein *Subjekt* entsprechend dem Schutzbedarf erfüllen muss.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.
- (optional) Greift in den Zugangsregeln auch auf den Schutzbedarf der angeforderten Ressource (z. B. Klassifizierungsstufe) sowie Kontextinformationen (z. B. Bedrohungslage) zu.

7.2.7 Zugriffsrecht Service

Zugriffsrecht Service	Der *Zugriffsrecht* Service verwaltet die Rechte für die Nutzung einer *E-Ressource*. Die Rechte sind auf der Basis von *Authentisierung*, *Attributen,* Kontext des Zugriffs (Lokation, Zeitpunkt, Sicherheitsniveau usw.) oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen) definiert.

Schnittstellen:

In: Trust-Beziehungen,

E-Ressourcen,

Art und Qualität der Attribute (Metadaten der Attribute),

Art und Qualität der Authentifizierung

Out: *Zugriffsregeln*

Aufgaben:

- Stellt Funktionen zur Verwaltung der Informationen bereit, welche Bedingungen (Autorisierung und/oder Attribute, Kontext des Zugriffs oder Informationen aus eigenen Modellen) ein *Subjekt* entsprechend dem Schutzbedarf in welcher Qualität erfüllen muss, damit es auf die Funktionen und/oder Daten der *Ressource* zugreifen darf (*Feinautorisierung*).
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.

7.3 Services zur Laufzeit

Die Geschäftsservices zur Laufzeit (in den Modellen dunkelblau) sind in Abbildung 17 dargestellt. Die Abbildung enthält alle Services, die zur Abwicklung der Prozesse *Subjekt authentifizieren* und *E-Identity autorisieren* zur Laufzeit verwendet werden.

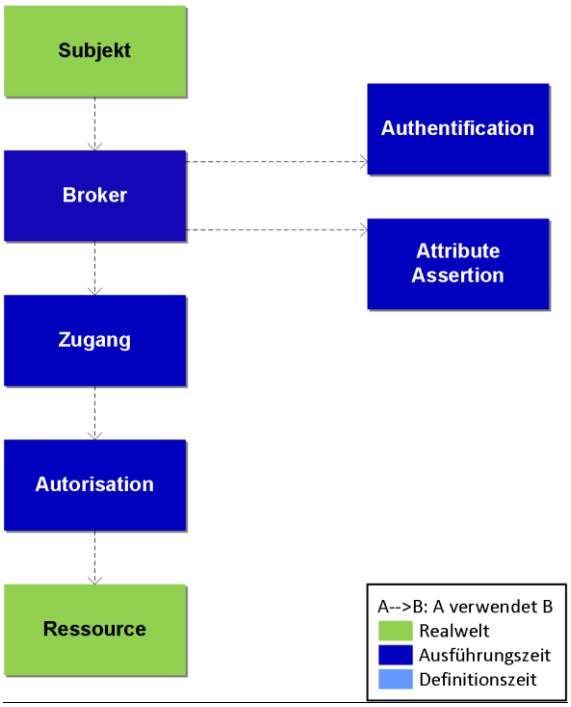


Abbildung 17 Geschäftsservices – Laufzeit

7.3.1 Authentication Service

Authentication Service	Der *Authentication* Service überprüft mittels der *Authentifizierungsmittel*, ob der Zugreifende (*Subjekt*) der ist, der er behauptet zu sein.

Schnittstelle:[8]

[8] Bei den Services zur Laufzeit werden in der Schnittstelle, die Daten angeben, die zur Laufzeit als Informationen benötigt werden (In-Schnittstelle) bzw. die nach der Ausführung des Services zur Verfügung stehen (Out-Schnittstelle). Werden zur Ausführung zusätzliche Informationen aus der Definitionszeit oder weitere Services der Laufzeit benötigt, so werden die entspr. Services angegeben (Braucht-Schnittstelle).

In: Authentifizierungs-Anfrage (*Authentication Request)*,
(*Identifikator)*,
Authentifizierungsfaktoren

Out: *Authentifizierungsergebnis* (Angabe, ob die Überprüfung des *Subjekts* positiv ausgefallen ist oder nicht), (Identifikator),
Art und Qualität der Authentifizierung

Braucht*: Credential Service, Logging Service*

Aufgaben:

- Überprüft, ob der aufrufenden Service berechtigt ist, eine Authentifizierung zu veranlassen.
- Überprüft, die Ausgabewerte der Authentifikatoren mit Hilfe der Credentials. Ist die Prüfung positiv, ist die Authentifizierung erfolgreich und die behauptete E-Identity wird mit entsprechender Qualität der Authentifizierung (z. B. entsprechend den Vertrauensstufen nach eCH-0170 [9]) bestätigt.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.
- (optional) Holt das Einverständnis des *Subjekts* (Einschränkung auf natürliche Personen) ein, das *Authentifizierungsergebnis* an den aufrufenden Service zu übermitteln.
- (optional) Etabliert eine zeitlich befristete sichere Verbindung zum *user agent* des Subjekts (z. B. Browser oder App).
- (optional) Kann das Authentifizierungsergebnis an Services übermitteln, so lange die sichere Verbindung zum *user agent* des Subjekts besteht (unterstützt Single Sign-On)

7.3.2 Attribute Assertion Service

Attribute Assertion Service	Der Attribute Assertion Service stellt die *Attributbestätigungen* über eine definierte Schnittstelle aus.

Schnittstelle:

In: Attribute-Request,
Identifikator,
(Authentifizierungsbestätigung)

Out: *Attributbestätigung* (Angabe, ob die Überprüfung der Beziehung zwischen einem *Attribut* und dem *Subjekt* positiv ausgefallen ist, oder nicht).

Braucht: *Attribute Service, Logging Service*

Aufgaben:

- Überprüft, ob der aufrufenden Service berechtigt ist, eine Attributbestätigung anzufordern.
- (optional) Stellt sicher, dass die Attributbestätigung für ein Subjekt nur auf Basis eines gültigen Authentifizierungsergebnisses des Authentication Service ausgestellt wird.

- Generiert berechnete und abgeleitete Attributwerte aus *Attributen* (z. B. over18).
- Bestätigt elektronisch mit entsprechender Qualität (siehe Qualitätsmodell zur Attributbestätigung eCH-0171 [10]), ob ein bestimmtes *Attribut* einem *Subjekt* zugewiesen ist oder nicht.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.
- (optional) Holt das Einverständnis des *Subjekts* (Einschränkung auf natürliche Personen und persönliche Attribute) ein, die *Attributbestätigungen* an den aufrufenden Service zu übermitteln (Zustimmung).

7.3.3 Broker Service

Broker Service	Dieser Service vermittelt zwischen dem *Subjekt*, *Ressourcen* und den Services der Ausführungszeit, föderiert Authentifizierungs- und Attributbestätigungen.

Schnittstelle:

In: Authentifizierungs-Anfrage (*Authentication Request)*,
(Attribute-Request),
(*Identifikator)*

Out: *Authentifizierungsbestätigungen,*
(Attributbestätigungen)

Braucht*: Trust Service, Authentication Service, Attribute Assertion Service, Logging Service, E-Identity Service*

Aufgaben:

- Vermittelt die Services und *Metadaten* (Discovery)
- Überprüft, ob der aufrufenden Service berechtigt ist, *Authentifizierungs- und Attributbestätigungen* anzufordern.
- Kontaktiert die gemäss Trust vertrauenswürdigen *Authentication Services* zur *Authentifikation* des *Subjekts* und bestätigt im positiven Fall die Authentizität des aufrufenden *Subjekts (z. B.* mit einer *Authentifizierungsbestätigung* der entsprechenden Qualität)
- (optional) Holt das Einverständnis des *Subjekts* (Einschränkung auf natürliche Personen) ein, das *Authentifizierungsergebnis* an den aufrufenden Service zu übermitteln (Zustimmung; erfolgt allenfalls zusammen mit der Zustimmung zur Übermittlung der *Attributbestätigungen*).
- (optional) Kontaktiert ausgehend von der durch den *Identifikator* referenzierten E-Identity rekursiv entlang den *linkedID*-Beziehungen weitere gemäss Trust vertrauenswürdigen *Authentication Services* zur *Authentifikation* des *Subjekts*.
- (optional) Kontaktiert die gemäss *Trust* vertrauenswürdigen *Attribute Assertion* Services und forderte eine Bestätigung der gewünschten *Attribute* in der gewünschten

Qualität. Die gewünschten Attribute können per Attribute-Request angefordert werden oder den Metadaten der Relying Party entnommen werden.

- (optional) Kontaktiert ausgehend von der durch den *Identifikator* referenzierten E-Identity rekursiv entlang den *linkedID*-Beziehungen die gemäss *Trust* vertrauenswürdigen *Attribute Assertion* Services und forderte eine Bestätigung der gewünschten Attribute in der gewünschten Qualität.
- (optional) Stellt die gewünschten Authentifizierungs- und Attributbestätigungen zusammen und übergibt diese dem aufrufenden Service. Dabei sind verschiedene Ausbaustufen, von einfachem Vermittler (Proxy) bis komplexen *Broker*-Diensten, möglich (siehe Anhang E).
- (optional) Kann vom *Attribute Assertion Service* die Verantwortung übernehmen, beim *Subjekt* das Einverständnis einzuholen, die Authentifizierungs- und Attributbestätigungen an den aufrufenden Service zu übermitteln (Zustimmung).
- Auslesen von notwendigen Authentifikations- (*Authentication* Services) und Attributpartnern (*Attribute Assertion* Services) aus dem Metadirectory.
- Kennt andere *Broker* Services und nutzt diese entsprechend den in *Trust* definierten Vertrauensbeziehungen.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.
- (optional) Kann die Log-Informationen der verwendeten Laufzeit-Services zusammenführen, um Nutzungsprobleme oder Fehler in der Identity Federation aufzuklären.

7.3.4 Zugang Service

Zugang Service	Der Service überprüft die Einhaltung der *Zugangsregeln* und erlaubt dem *Subjekt* den Zugang, wenn die entsprechenden Regeln erfüllt sind.

Schnittstelle:

In: *Identifikator* einer *E-Ressource, Authentifizierungs- und Attributbestätigungen*

Out: *false oder true + Authentifizierungsergebnis, (Authentifizierungs- und Attributbestätigunge)*

Braucht: *Zugangsregel Service, Logging Service, Broker Service*

Aufgaben:

- Informiert das *Subjekt* über benötigte Sicherheitsinformationen (z. B. benötigte Attribute, geforderter Qualität-Level) bezüglich des *Zugriffs*.
- Erlaubt den Zugang zur *Ressource*, wenn die geforderte *Authentifizierung* erfolgreich war und die geforderten *Attribute* in der gewünschten Qualität bereitgestellt wurden. Diese Funktionalität wird auch als *Grobautorisierung* bezeichnet.
- Gibt die *Authentifizierungsbestätigungen* und die *Attributbestätigungen* an den *Autorisation* Service weiter.

- Verwendet einen *Logging Service*, um Zugangsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.

7.3.5 Autorisation Service

Autorisation Service	Der Service überprüft zur Ausführungszeit die Einhaltung der Rechte für die Nutzung der *E-Ressource* und erlaubt dem *Subjekt* die Nutzung der *Ressource*, wenn es die entsprechenden Rechte besitzt.

Schnittstelle:

In: *Authentifizierungsbestätigungen*,
Attributbestätigungen,
Identifikator einer *E-Ressource*

Out: Security Token (mit allen für den Zugriff auf die Ressource relevanten Informationen, insb. Attributbestätigungen)

Braucht: *Zugriffsregel Service, Logging Service*

Aufgaben:

- Überprüft, ob die übergebenen Bestätigungen inklusive deren geforderten Qualität den *Zugriffsrechten* entsprechen und erlaubt ggf. die Nutzung der entsprechenden Funktionen der *Ressource* (*Feinautorisierung*).
- Erzeugt ein Security Token für das autorisierte *Subjekt* mit den im Zugriffskontext relevanten und bestätigten *Attributen*.
- Begrenzt die Lebensdauer des Security Tokens.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.
- (optional) Arbeitet mit dem Lizenzmanagement zusammen, z. B. um den Zugriff zu verweigern, wenn die maximale Anzahl von gleichzeitigen Benutzern erreicht ist.

7.3.6 Logging Service

Logging Service	Der Service dokumentiert zur Laufzeit die Verwendung eines Services und stellt der Support-Organisation die notwendigen Informationen bereit, um Nutzungsprobleme oder Fehler aufzuklären.

Schnittstelle:

In: Nutzungsdaten eines Service

Out: Logs

Braucht: -

Aufgaben:

- Wird von anderen Services verwendet.
- Sammelt und speichert die Nutzungsdaten eines Services in standardisierter Form

- Gibt die Nutzungsdaten eines Services in standardisierter Form (Logs) an berechtigte Services weiter.
- (optional) Bietet rechtlich verifizierte und verifizierbare Audit- und Monitoring-Funktionen zur vollständigen Nachvollziehbarkeit

7.4 Gesamtmodell

In Abbildung 18 werden alle IAM-Geschäftsservices zusammen dargestellt. Man erkennt, dass die Laufzeitservices zur Erfüllung ihrer Funktionalitäten auf die Daten der Services der Definitionszeit zugreifen. Auf die Darstellung des Laufzeitservices *Logging Services*, der von allen anderen Services genutzt wird, wurde aus Übersichtlichkeitsgründen verzichtet.

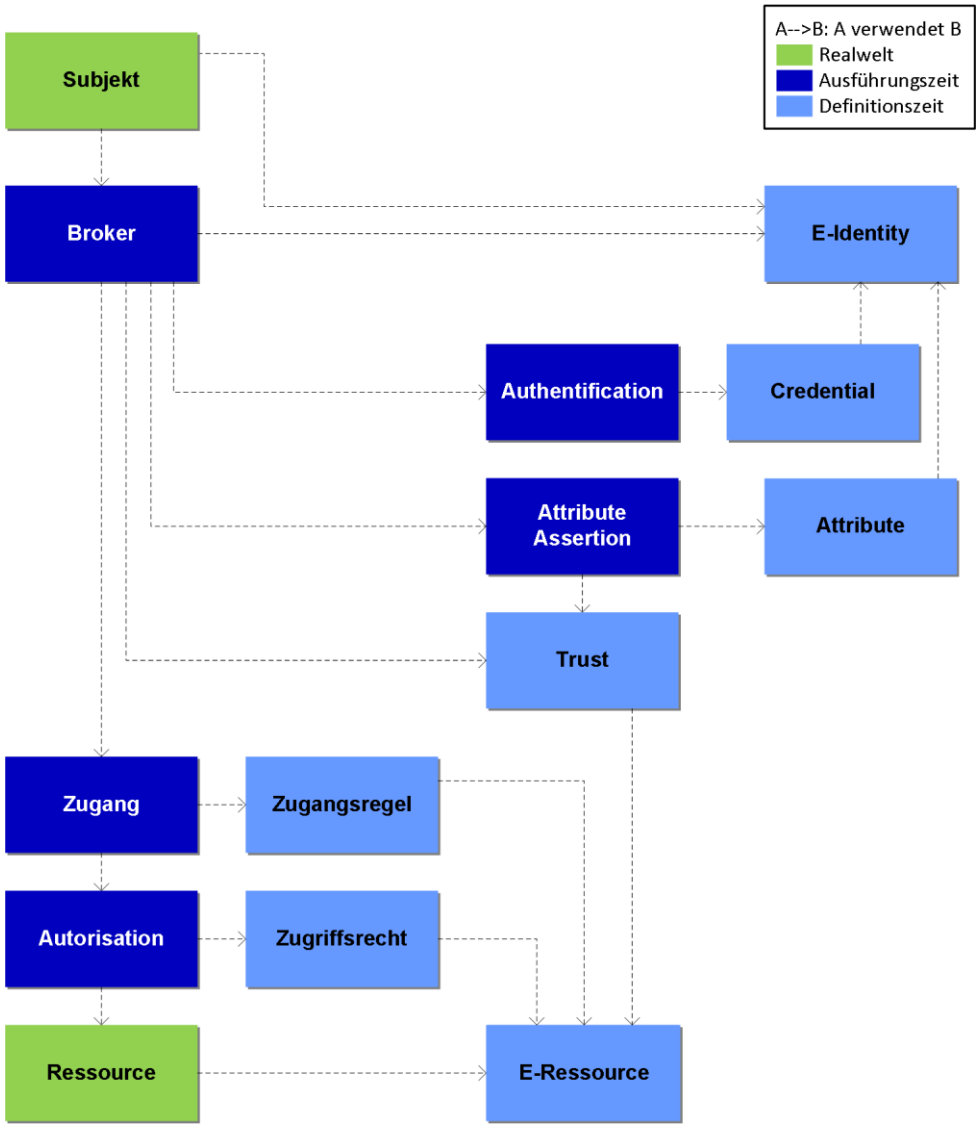


Abbildung 18 Geschäftsservices – Übersicht

7.5 Prozessunterstützung durch Geschäftsservices

In diesem Abschnitt wird an den Laufzeitprozessen dargestellt, wie die Services zusammenarbeiten. Die Zusammenarbeit der Services zur Erbringung der Definitionsprozesse ist ein-

fach und in Abbildung 16 und in den Services bereits direkt angesprochen. Diese werden deshalb hier nicht dargestellt.

7.5.1 IdP Discovery

Abbildung 19 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *IdP Discovery*.

Abbildung 19 Prozessunterstützung *IdP Discovery*

IdP Discovery folgt dem nachstehenden Ablauf:

- Der *Broker Service* prüft, welche *Authentification* und (wenn nötig) *Attribute Assertion* Service gemäss *Trust Service* die Anforderungen des aufrufenden Service erfüllen und stellt eine Auswahl zur Verfügung.
- Das *Subjekt* wählt einen *Authentification Service* (IdP) von der Auswahl aus.

7.5.2 Subjekt authentifizieren

Abbildung 20 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *Subjekt authentifizieren*.

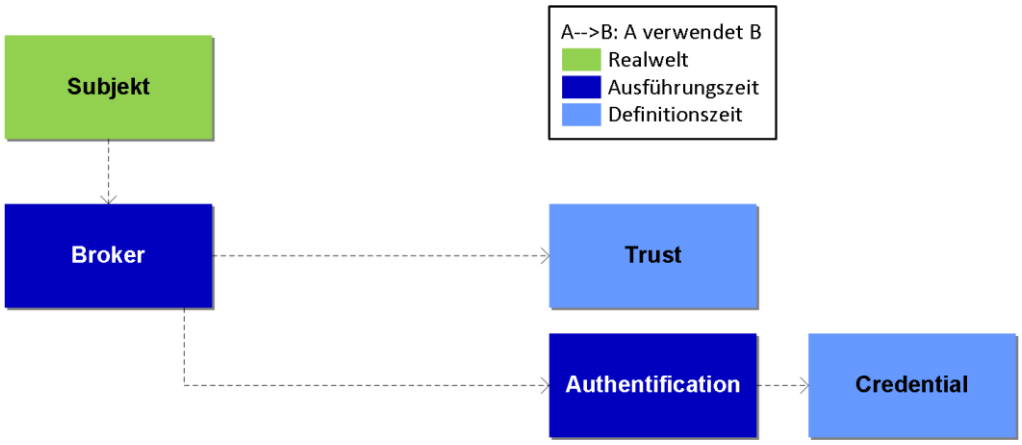


Abbildung 20 Prozessunterstützung *Subjekt authentifizieren*

Subjekt authentifizieren folgt dem nachstehenden Ablauf:

- Der *Broker Service* delegiert die *Authentifizierung* des *Subjekts* an den gewählten *Authentification* Service.

- Das *Subjekt* authentisiert sich gegenüber dem *Authentication* Service. Dieser prüft den generierten Ausgabewert des Authentifikators gegen das *Credential* der behaupteten E-Identity. Ist die Prüfung positiv, ist die Authentifizierung erfolgreich.

7.5.3 E-Identity bestätigen

Abbildung 21 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *E-Identity bestätigen*.

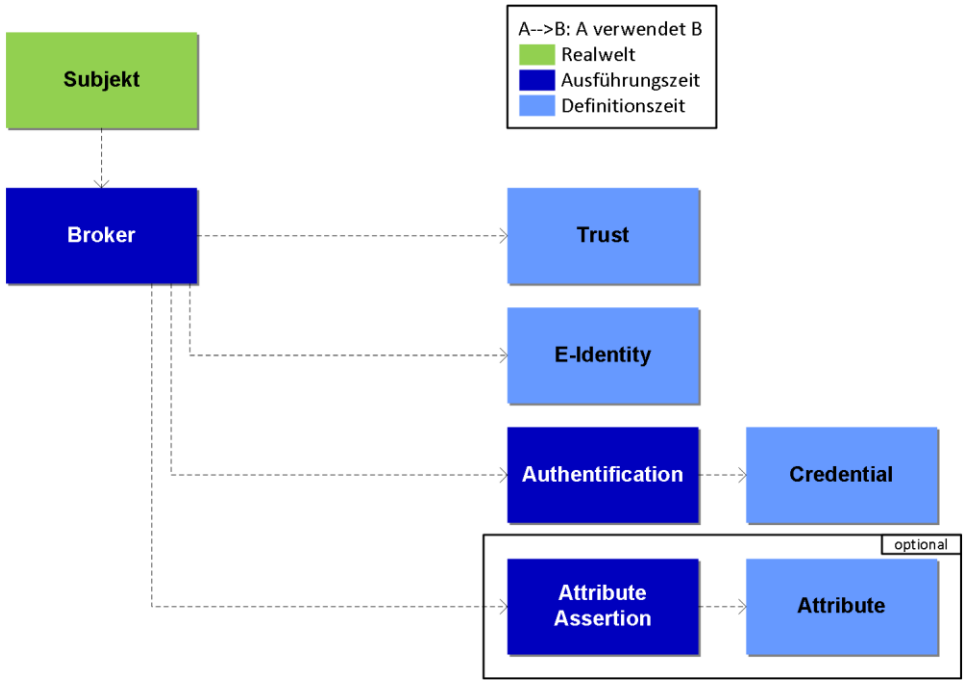


Abbildung 21 Prozessunterstützung *E-Identity bestätigen*

E-Identity bestätigen folgt dem nachstehenden Ablauf:

- Nach erfolgreicher Authentifizierung wird überprüft, ob der aufrufende Service Attribute benötigt.
- (optional) Falls Attribute benötigt werden, wird die *Attribute Assertion* Service-Auswahl auf die reduziert, die gemäss den verlinkten *E-Identities* (linkedID) der *E-Identity* Service Informationen zur *E-Identity* führen.
    - Die E-Identity wird gemäss Geschäftsservice *E-Identity anreichern (vgl. Abschnitt 7.5.4)* mit Attributen angereichert.
- Der *Broker Service* erzeugt Authentifizierungs- und Attributbestätigung und übergibt diese dem aufrufenden Service

7.5.4 E-Identity anreichern

Abbildung 22 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *E-Identity anreichern*.

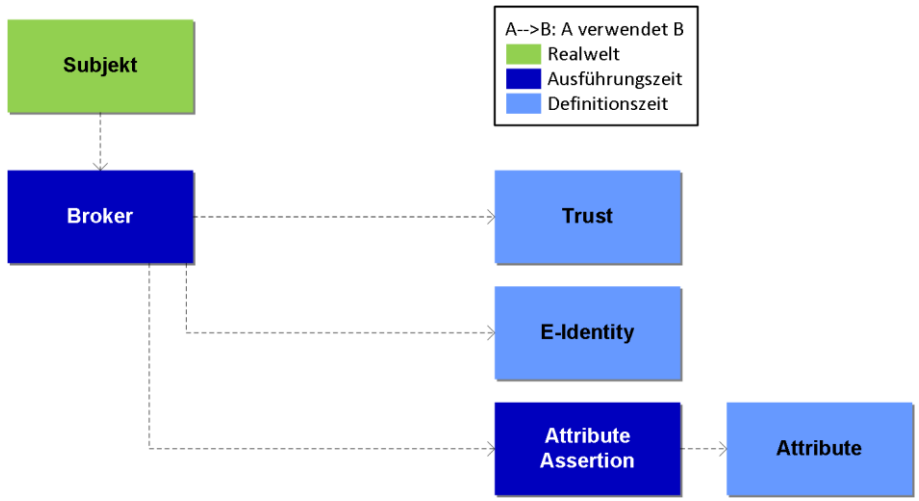


Abbildung 22 Prozessunterstützung *E-Identity anreichern*

E-Identity anreichern folgt dem nachstehenden Ablauf:

- Der *Broker Service* fragt die entsprechenden *Attribute Assertion* Service an, die entsprechenden *Attribute* zu bestätigen.
- (optional) Der *Broker Service* holt die Bestätigung vom Subjekt (nur bei natürlichen Personen) des Ergebnisses der Authentifizierung und die ermittelten Attribute an den aufrufenden Service zu übergeben.

7.5.5 Zugang erlauben

Abbildung 23 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *Zugang erlauben.*

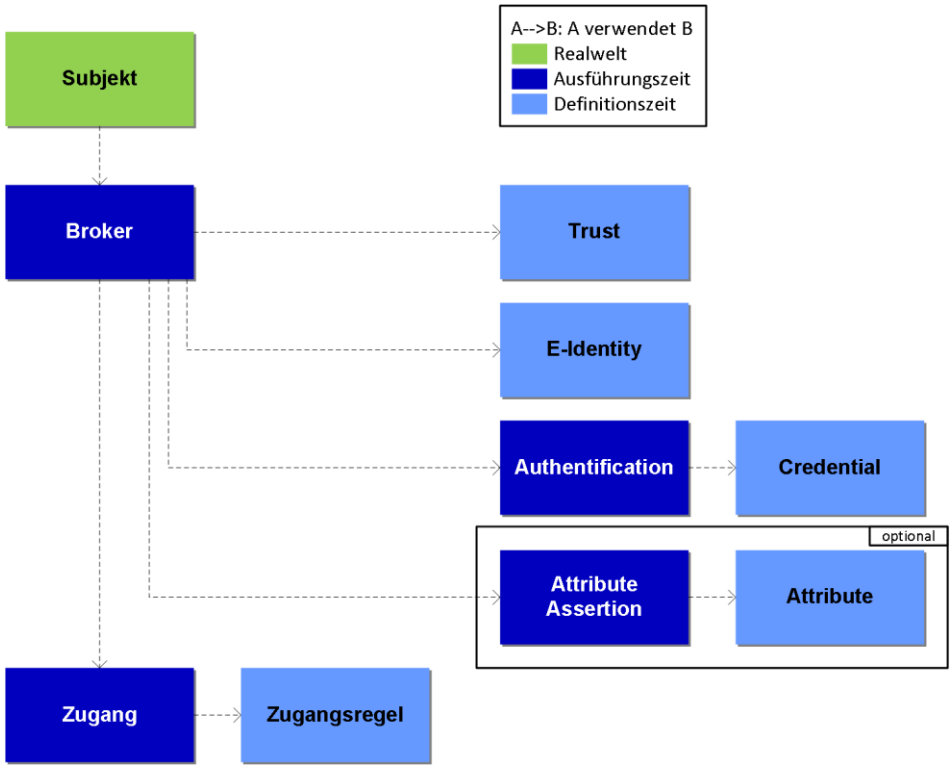


Abbildung 23 Prozessunterstützung *Zugang erlauben*

Zugang erlauben folgt dem nachstehenden Ablauf:

- *Zugang* Service prüft die Zugangsregeln für diese E-Ressource und verlangt vom Broker, entsprechend den Anforderungen das Subjekt zu authentifizieren und die Attribute zur *E-Identity* zu bestätigen (vgl. Abschnitte 7.5.3 und 7.5.4)
- *Zugang Service* prüft das Zugangsrecht basierend auf den *Authentifizierungs- und Attributbestätigungen.*
- *Zugang* Service gewährt den *Zugang* auf die *Ressource* und übergibt die *Authentifizierungs- und Attributbestätigungen.*

7.5.6 Zugriff erlauben und Attribute nutzen

Abbildung 24 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *Zugriff erlauben und Attribute nutzen.*

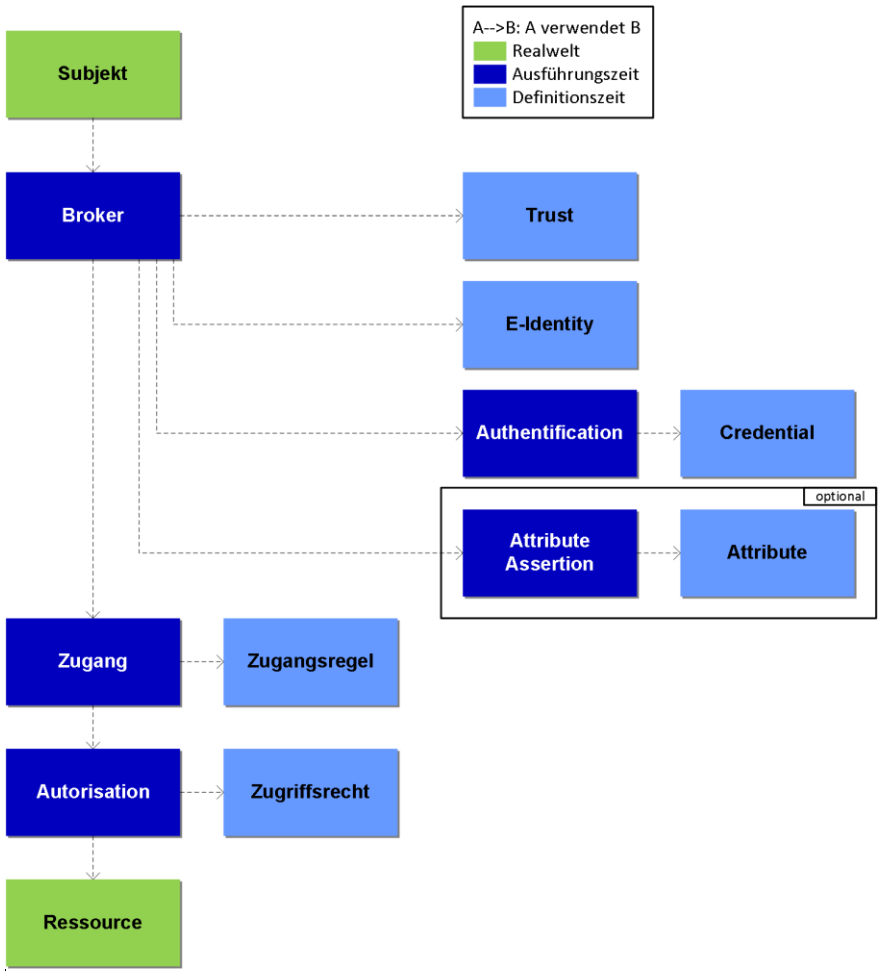


Abbildung 24 Prozessunterstützung *Zugang erlauben und Attribute nutzen*

Zugriff erlauben und Attribute nutzen folgt dem nachstehenden Ablauf:

- *Autorisation* Service prüft die Zugriffsregeln für diese E-Ressource und verlangt vom *Zugangs Service*, entsprechende *Authentifizierungs-* bzw. *Attributbestätigungen*.

- *Autorisation Service* prüft das Zugriffsrecht basierend auf den *Authentifizierungs- und Attributbestätigungen,* Kontext des Zugriffs oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen).
- *Autorisation* Service gewährt den *Zugriff* auf die *Ressource* und übergibt die *Authentifizierungs- und Attributbestätigungen.* Die Attribute können nun entsprechend genutzt werden.

7.6 Zuordnung Service zu Informationselemente

Nachfolgende Tabelle stellt die Beziehung zwischen den Geschäftsservices und den Elementen der Informationsarchitektur (Semantik und Schnittstelle) dar. Services in der Definitionszeit bearbeiten (B) Objekte und deren Beziehungen zueinander. Services der Laufzeit lesen (L) Objekte und deren Beziehungen zueinander. Einzelne Services verwenden allerdings nur die Metadaten (M) anderer Services.

		Informationselement										
		E-Identity[9]	**Attribut**[10]	**Zugangsregel**	**Zugriffsrecht**	**E-Ressource**	**Credential**	**Identifikator einer E-Identity**	**Ausgabewert des Authentikator**	**Authentifizierungs-bestätigung**	**Attributbestätigung**	**Identifikator einer E-Ressource**
Geschäftsservice	E-Identity	B	B[11]					B				
	Credential	L					B	L				
	Attribute	L	B					L				
	Trust	M	M			M						
	E-Ressource					B						B
	Zugangsregel	M	M	B		L						
	Zugriffsrecht	M	M	L	B	L						
	Authentication	L					L	L	B			
	Attribut Assertion		L					L		L	B	
	Broker	L						L	L	LB[12]	LB[12]	
	Zugang			L		L		L		L	L	L
	Autorisation				L	L		L		L	L	L

B = Bearbeiten (Create/Read/Update/Delete), L = Lesen (Read), M = liest nur Metadaten

Tabelle 5 Beziehung zwischen Services und Semantik des Informationsmodells

[9] inkl. Beziehung linkedID
[10] inkl. Beziehung zu E-Identity
[11] B für Identifikator (ist auch ein Attribut)
[12] B, wenn Broker selber kombinierte *Authentifizierungs- und Attributbestätigungen* ausstellt

7.7 Zuständigkeiten für Geschäftsservices

Tabelle 6 zeigt auf, welcher Stakeholder idealtypisch welchen IAM-Service zur Definitions- und Laufzeit anbietet. Diese Geschäftsservices sind in Kapitel 7 näher beschrieben. Die hier vorgeschlagene Aufteilung optimiert bezüglich Wiederverwendung der Services in einer *Identity Federation*. Die *Relying Party* gibt deshalb möglichst viel Betriebsverantwortung an *IAM*-Dienstanbieter.

		Stakeholder					
		IAM-Dienstanbieter					Relying Party
		IdP	AA	CSP	RA	Vermittler	
Geschäftsservices	E-Identity				X		
	Credential			X			
	Attribute		X				
	Trust					X	
	E-Ressource						X
	Zugangsregel					X	
	Zugriffsrecht						X
	Authentication	X					
	Attribute Assertion		X				
	Broker					X	
	Zugang					X	
	Autorisation						X

Tabelle 6 Beziehung zwischen Geschäftsservices und Stakeholder

8 IAM für das IoT

Ein Ding im vorliegenden Kontext ist ein physischer Gegenstand, der aktiv und autonom über ein Netzwerk mit Ressourcen kommuniziert. Mehrere Dinge, die im selben Netzwerk verknüpft sind, bilden ein Internet der Dinge (*Internet of Things*, IoT). Beispiele sind Roboter, aktive Elemente der Gebäudeautomation, moderne (zukünftig auch selbstfahrende) Autos oder generell Sensorknoten unterschiedlichster Art.

Das Konzept des IoT stammt aus den achtziger Jahren. Autonom agierende Dinge gibt es schon seit längerem (z. B. Alarmierungssysteme), die grosse praktische Relevanz des IoT wird sich aber erst im Zuge der weiteren Miniaturisierung und Automatisierung von Fabrikations-, Transport- und Steuerungssystemen erweisen.

Die langfristigen Auswirkungen des IoT auf die Gestaltungsprinzipien der Identitäts- und Zugriffsverwaltung (IAM) sind noch nicht absehbar. Dieses Kapitel zeigt auf, in welchen Bereichen solche Auswirkungen zu erwarten sind.

8.1 Spezielle Eigenschaften von Dingen

Dinge (bzw. *Things*) sind Realweltobjekte, die auf Ressourcen zugreifen. In der Informationsarchitektur des vorliegenden Standards sind sie als Subjekte mit einer spezifischen Eigenschaft abgebildet. Sie unterscheiden sich insbesondere in den folgenden Punkten von natürlichen Personen:

- Dinge können zu einer natürlichen Person oder zu einer Organisation gehören, nachfolgend als Besitzer (des Dings) bezeichnet. Der Besitzer ist für seine Dinge verantwortlich und haftet für deren Aktivitäten im IoT[13].
- Dinge können nur Daten benützen, die in elektronischer Form verfügbar sind. Alle zur Laufzeit relevanten Daten wie Authentifizierungsfaktoren (z. B. PIN) und Entscheide (z. B. Freigabe von Attributen) müssen deshalb zur Definitionszeit konfiguriert werden.
- Dinge sind häufig aus anderen Dingen zusammengesetzt wie beispielsweise ein Gebäude, das Lifte enthält, die wiederum ein Alarmierungssystem enthalten. Oder ein Fahrzeug mit Bordcomputer mit Navigationsgerät und Fahrtenschreiber.
- Die Lebensdauer von Dingen kann sehr unterschiedlich sein und von wenigen Stunden (evtl. Minuten) bis zu vielen Jahren reichen.
- Die Anzahl der Dinge ist langfristig nicht limitiert. Schätzungen gehen von 1‘000 bis 5‘000 Dingen pro Mensch aus. Die skalierbare Verwaltung dieser Dinge erfordert einen hohen Automatisierungsgrad.

[13] Der Besitzer kann eventuell auf den Hersteller des Dings Regress nehmen, was hier aber nicht weiter vertieft wird.

8.2 Auswirkung auf die IAM Informationsarchitektur

Grundsätzlich sind die IAM Geschäftsservices auch auf Dinge anwendbar.

Aufgrund ihrer speziellen Eigenschaften der Dinge ergeben sich aber verschiedene Aspekte, die bei der Implementierung der IAM Geschäftsservices zusätzlich oder anders betrachtet werden sollten. Viele dieser Aspekte betreffen die IAM Informationsarchitektur und speziell die Verwaltung von komplexen Beziehungen zwischen den Subjekten:

Aspekt	Grundsatz, Beschreibung und Umsetzung im IAM
Besitzer	Dinge im IoT sollten immer einen Besitzer haben. Der Besitz kann befristet sein (z. B. Miete von Autos oder Ferienwohnungen) oder dauerhaft bis auf Widerruf (der Normalfall). Es kann auch Dinge mit mehreren Besitzern geben (z. B. ein Kühlschrank, der Lebensmittel für alle Bewohner einer Wohngemeinschaft nachbestellt). Das Konzept des „Besitzers“ (von Dingen) erfordert eine zusätzliche Beziehung im Rahmen der Informationsarchitektur (vergleiche hierzu die Definition „Subjekt“ in der Informationsarchitektur). *Bemerkung*: Diese zusätzliche Beziehung kann ggf. auch unabhängig vom IoT genutzt werden, um Abhängigkeiten zwischen Subjekten zu verwalten (z. B. Verwaltung von separaten E-Identities für IT-Administrator Tätigkeiten).
„On behalf“ Zugriff	Dinge nutzen Ressourcen „on behalf“ ihres Besitzers. Das Auto sucht sich einen freien Parkplatz oder eine Tankstelle, das Mobiltelefon aktualisiert lokale Daten, der Kühlschrank bestellt Milch. Dies erfordert die Möglichkeit, dass eine natürliche Person oder eine Organisation Attribute ihrer E-Identity temporär oder dauerhaft auf die E-Identities ihrer Dinge übertragen kann.

Eigene und übertragene Attribute	Dinge haben eigene und übertragene Attribute. Eigene Attribute sind statisch inhärent (z. B. Seriennummer, Produktionsdatum) oder dynamisch (z. B. aktueller Standort, aktueller Energieverbrauch, derzeit aktiver Authentisierungsschlüssel). Übertragene Attribute stammen vom Besitzer wie beispielsweise dessen Organisationszugehörigkeit, Postadresse oder Bankverbindung. Für die Übertragung von Attributen an Dinge müssen Regeln definiert werden. Beispiele für solche Übertragungsregeln könnten sein: • Attribute können nur von natürlichen Personen übertragen werden (bei Organisationen: Durch einen hierzu autorisierten Vertreter). • Es ist ersichtlich, dass ein Attribut übertragen wurde und von wem. • Übertragene Attribute werden entzogen, sobald sie dem Übertragenden entzogen werden. • Bei der Übertragung eines Attributs wird definiert, ob die Übertragung auch transitiv wirkt (insb. bei zusammengesetzten Dingen relevant). *Bemerkung*: Die Übertragung von Attributen kann ggf. auch unabhängig vom IoT genutzt werden, um Stellvertretungen zu verwalten.
Besitzer Wechsel	Dinge können den Besitzer wechseln. Langlebige Dinge (z. B. Investitionsgüter) können im Verlauf ihrer Lebensdauer mehrfach den Besitzer wechseln. Eigene (inhärente und dynamische) Attribute bleiben beim Besitzerwechsel unverändert. Übertragene Attribute müssen gelöscht und vom neuen Besitzer ggf. erneut übertragen werden. Ausserdem ist sicherzustellen, dass zu jedem Zeitpunkt ein Besitzer definiert ist.
Ersatz von Dingen	Dinge können ersetzt werden. Kurzlebige Dinge (z. B. Verbrauchsmaterial) können 1:1 ersetzt werden. Eigene (inhärente und dynamische) Attribute werden beim Ersatz neu definiert. Übertragene Attribute müssen automatisch auf das Ersatz-Ding übertragen werden können.
Zusammengesetzte Dinge	Dinge können aus Dingen zusammengesetzt sein. Komplexe Dinge sind aus Dingen zusammengesetzt, wobei keine Beschränkung in der Verschachtelungstiefe besteht. Ein Ding kann sogar zu mehreren übergeordneten Dingen gehören wie beispielsweise ein intelligenter Stromzähler, der sowohl zu einem Gebäude als auch zum regionalen Verbund des Netzbetreibers gehört. Das IAM muss in der Lage sein, auch komplexe Beziehungen von Dingen untereinander abzubilden.

8.3 Auswirkung auf die IAM Geschäftsservices

Die speziellen Eigenschaften von Dingen wirken sich auch auf IAM Geschäftsservices aus:

Aspekt	Grundsatz, Beschreibung und Umsetzung im IAM
Integriertes Authentifizierungsmittel	Dinge haben ein integriertes Authentifizierungsmittel. Damit ein Ding autonom und ohne manuelle Interaktion einer natürlichen Person aktiv werden kann, müssen alle für die Authentifizierung zur Ausführungszeit erforderlichen Daten in elektronischer Form verfügbar sein. Dies betrifft insbesondere kryptographische Schlüssel mit den dazugehörigen Aktivierungsdaten (z. B. PIN). Der Authentication Service zur Authentifizierung von Subjekten muss die spezifischen Eigenschaften von Dingen berücksichtigen. *Bemerkung*: Physical unclonable functions (PUF) sind mit biometrischen Verfahren vergleichbar und könnten einen interessanten Lösungsansatz für die Authentifizierung von Dingen aufzeigen.
Automatische Registrierung inkl. Inventarisierung	Dinge können sich automatisch registrieren. Damit die langfristig zu erwartende sehr grosse Anzahl von Dingen verwaltet werden kann, sind weitgehend automatisierte Verwaltungsprozesse erforderlich. Dies betrifft insbesondere die Registrierung und Inventarisierung von Dingen, wenn sie ins Internet der Dinge neu aufgenommen (oder später wieder aus diesem entfernt) werden. Der E-Identity Service und der Credential Service müssen die spezifischen Eigenschaften von Dingen berücksichtigen und insbesondere Automatisierung ermöglichen.

9 Privacy

Dieses Kapitel beschreibt Anforderungen zum Schutz der Privatsphäre des Subjektes, die über die subjektbezogenen Anforderungen in Kapitel 4.3.1 hinausgehen. Der Schutz der Privatsphäre ist entscheidend für das Vertrauen in das IAM-System, besonders bei Szenarien, bei denen Bürger auf staatliche oder behördliche Ressourcen zugreifen (C2G-Szenarien).

Des Weiteren werden Richtlinien zur Verwaltung und Verarbeitung von subjektbezogenen Daten gegeben.

9.1 Anforderungen an Sicherheit und zum Schutz der Privatsphäre

In diesem Kapitel werden zunächst die allgemeinen Anforderungen an Sicherheit und zum Schutz der Personendaten eines Subjektes in einem föderierten IAM-System aufgelistet. Je nach Rahmenbedingungen und gewähltem Identity Federation Modell sollten dann die gewünschten Anforderungen bei der Umsetzung mitberücksichtigt werden. Das gilt besonders für Modelle mit zentralem Vermittler.

ID	Name	Allgemeine Beschreibung	Typische Anwendungsszenarien
R1	Nichtbeobachtbarkeit (Unobservability)	Ein Subjekt kann auf eine Ressource oder einen Dienst zugreifen, ohne dass unberechtigte Dritte dies feststellen können.	Ein an einem Authentisierungsvorgang beteiligter IdP/AA soll ohne Drittpartei nicht feststellen können, ob und wann ein bestimmtes Subjekt auf eine Ressource zugegriffen hat. Umgekehrt kann auch die Anforderung bestehen, dass eine beteiligte RP nicht feststellen können soll, bei welchem IdP/AA sich ein bestimmter Benutzer authentisiert hat.[14] Eine in einem Authentisierungsvorgang unbeteiligter Externer soll nicht feststellen können ob und wann ein bestimmter Benutzer auf einen IdP/AA eine RP bzw. auf eine bestimmte Ressource zugegriffen hat (z. B. durch zeitliche Korrelation)
R2	Unverkettbarkeit (Unlinkability)	Ein Benutzer kann mehrmals auf eine Ressource zugreifen, ohne dass unbe-	Ein Benutzer soll auf unterschiedliche RP's bzw. auf Ressourcen zugreifen können, ohne dass die Identität durch

[14] Diese Anforderung wird in der Praxis vielfach nicht verlangt. Eine RP muss i.d.R prüfen können, bei welchem IdP/AA sich ein Benutzer authentisiert hat, um das notwendige Vertrauen aufbauen zu können.

ID	Name	Allgemeine Beschreibung	Typische Anwendungsszenarien
		rechtigte Dritte diese Ereignisse verbinden können.	Korrelation der Identitätsdaten durch die beteiligten RP's oder durch Dritte aufgedeckt werden kann.
R3	Vertraulichkeit (Confidentiality)	Ausser einer ausstellenden Instanz (IdP/AA) und der konsumierenden RP, sowie dem Subjekt selbst, können keine an einem Authentisierungsvorgang beteiligte Dienste personenidentifizierende Information einsehen.	Ein am Authentisierungsvorgang beteiligter Vermittler oder eine nicht-vertrauenswürdige Software auf dem Client des Benutzers, sollen personenidentifizierende Informationen (vermittelte Attribute) und optional die Identität des Benutzers nicht einsehen bzw. feststellen können.
R4	Datenherkunft und Datenunversehrtheit (Authenticity & Integrity)	Eine Applikation kann die Herkunft und Unversehrtheit von Identitätsinformationen eines Benutzers bis zu ihrer Quelle zurück überprüfen.	Eine RP kann überprüfen, ob Identitätsinformationen von einem berechtigten Vermittler stammen. Eine RP kann feststellen, ob die Authentifizierungs- und Attributbestätigungen von einer ihr bekannten autoritativen Quelle (IdP/AA) stammen. Eine RP kann sich davon überzeugen, dass der Überbringer einer Authentifizierungs- und Attributbestätigung der rechtmässige Inhaber ist[15].
R5	Einwilligung/Freigabe (Consent)	Die Freigabe von Identitätsinformationen an einen anfragenden Dienst kann ohne Einwilligung der natürlichen Person nicht erfolgen.	Ein Vermittler oder eine Client-Software fordert vom Benutzer die Freigabe von personenidentifizierenden Informationen und Attributen ein.
R6	Nachvollziehbarkeit (Auditability)	Die zu einem bestimmten Authentisierungsvorgang vermittelten Identitätsinformationen und ihre Metadaten liegen vor.	Die vermittelten Identitätsinformationen und ihre Metadaten können zentral eingesehen oder unter Mitwirkung aller beteiligter Entitäten im Nachhinein zusammengestellt werden.

Tabelle 7: Anforderungen an Sicherheit und zum Schutz der Privatsphäre

[15] Diese allgemein formulierte Anforderung beinhaltet auch den Assertion Diebstahl über einen Browser. Diese Anforderung kann z.Zt. nur mit SAML und dem Holder-of-Key Profil (HoK) sinnvoll umgesetzt werden.

9.2 Verwaltung und Verarbeitung von Daten von Subjekten

Dieses Kapitel gibt eine Richtlinie, was es zu beachten gibt, wenn Daten von Subjekten verwaltet und verarbeitet werden. Die wichtigste Voraussetzung ist, dass der Benutzer jederzeit sicherstellen kann, auf welche Art seine Daten verwendet werden. Dieses Kapitel beschreibt, bei welchen Szenarien welche Massnahmen für den Datenschutz zu beachten sind. Dies soll die Vertrauenswürdigkeit der Dienstanbieter stärken.

Minimierung der Datensammlung und des Datenbestands

Subjektidentifizierende Attribute dürfen von der RA für die Identifizierung und Überprüfung eines Subjektes gesammelt werden.
Ein Vermittler darf nur die Attribute an eine RP weitergeben, welche von der RP explizit angefordert wurden. In spezifischen Fällen ist es nicht nötig Attribute völlig offen zu legen. Beispielsweise wenn die RP nur wissen will, ob das Subjekt 18 Jahre oder älter ist, sollte nicht das explizite Geburtsdatum weitergegeben werden.
Ausserdem darf eine RP nur die Attribute vom Subjekt anfragen, die sie für die Erfüllung ihrer Funktion benötigt. Das Anfragen unnötiger Attribute kann das Vertrauen schwächen.

Verhindern von Profiling

Das Verknüpfen von Daten, die auf ein Subjekt zurückführen können, sollte auf ein Minimum reduziert werden. Das Erstellen von Persönlichkeitsprofilen sollte durch organisatorische und technische Massnahmen verhindert werden.

Kenntnisnahme und Einwilligung

Das Subjekt muss immer informiert werden, welche Attribute in welcher Form verwendet werden. Wenn Attribute weitergegeben werden (z. B. bei Föderierung) muss das Subjekt mindestens beim ersten Mal die explizite Zustimmung geben.

Nutzungsbeschränkung

Ein Dienstanbieter muss zu jederzeit Auskunft geben können, welche Daten aus welchem Grund angefragt und bearbeitet werden. Subjektbezogene Daten dürfen nicht ohne Einverständnis des Subjekts an Dritte weitergegeben werden.

Regress

Die CSP verfügt über Mechanismen, um Anfragen von Subjekten, ob Daten des Subjekts vorhanden sind, beantworten zu können. Das Subjekt hat die Möglichkeit auf eine einfache Art und Weise Anfragen zu stellen.

Datenschutz- und Risikoanalyse

Datenschutz- und Risikoanalysen sollen helfen den Schutzbedarf einer Ressource einzuschätzen und entsprechende Massnahmen zu konzipieren, um den Schutz der Daten nach gängiger Praxis und/oder gesetzlichen Bestimmungen zu gewährleisten.

Datenschutzmassnahmen

Ausgearbeitete Datenschutzmassnahmen sollen die Vertrauenswürdigkeit der Dienstanbieter wahren. Die Datenschutzmassnahmen sollen entsprechend des Schutzbedarfes der Daten und an die im Umfeld etablierten Prozesse angepasst sein.

10 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche **eCH** referenziert, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen, ist, soweit gesetzlich zulässig, wegbedungen.

11 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

[1] A. Laube-rosenpflanzer, A. Spichiger, T. Kessler, A. Müller, and M. Kunz, “eCH-0219 - IAM-Glossar,” vol. 1.0, 2017.

[2] W. Müller and H. Lindner, “eCH-0122 – Architektur E-Government Schweiz : Grundlagen Dokument,” vol. 1.0, pp. 1–26, 2014 [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0122

[3] Wikipedia, “IT Infrastructure Library.” [Online]. Available: https://de.wikipedia.org/wiki/IT_Infrastructure_Library

[4] “Protokoll Expertenworkshop ‘Sicherheitsopportunitäten für den Wirtschaftsstandort Schweiz’ vom 8.11.2012 (zu Strategie Informationsgesellschaft),” 2012.

[5] International Standards Organisation, “ISO 31000 - Risk management,” *ISO 31000:2009 - Risk Management*. p. 1, 2009 [Online]. Available: http://www.iso.org/iso/home/standards/iso31000.htm

[6] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenberg, “ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework,” 2011.

[7] Europäische Union, “Durchführungsverordnung (EU) Nr. 2015/1502 der Kommission vom 8. September 2015,” no. September, 2012.

[8] H. Häni and U. Kienholz, “eCH-0172 IAM-Maturitätsmodell,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=a26d17d1-fe03-4226-97ab-9beefef22856

[9] A. Laube-Rosenpflanzer, G. Hassenstein, M. Kunz, T. Gruoner, A. Spichiger, and T. Selzam, “eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten,” vol. 2.0, 2017 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=54cce841-215f-4887-9382-25620dcbf9b1

[10] M. Topfel, T. Jarchow, A. Spichiger, and R. Bernold, “eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=a26d17d1-fe03-4226-97ab-9beefef22856

[11] ISO/IEC, “ISO/IEC 27001:2013” [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[12] A. Laube-rosenpflanzer, G. Hassenstein, S. Agosti, M. Vinzens, U. Pfenninger, and D. Leiser, “eCH-0168 SuisseTrustIAM technische Architektur und Prozesse,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=31499686-813d-4589-b794-11015fbf2059

[13] A. Laube-rosenpflanzer and G. Hassenstein, “eCH-0174 SuisseTrustIAM - Implementierung mit SAML 2.0,” vol. 1.0, 2015 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=5d8ee101-aba3-4061-aba0-aaed23b1f04f

Anhang B – Mitarbeit & Überprüfung

Gruoner Torsten	ISB
Hassenstein Gerhard	Berner Fachhochschule, TI
Heerkens Marc	ISB
Kessler Thomas	Temet
Kunz Marc	Berner Fachhochschule, TI
Laube-Rosenpflanzer Annett	Berner Fachhochschule, TI
Leimer Bojan	Berner Fachhochschule, TI
Spichiger Andreas	Berner Fachhochschule, FBW
	eCH Fachgruppe IAM

Anhang C – Abkürzungen

AA	Attribute Authority
C2G	Citizen to Government
CP	Credential Provider
CSP	Credential Service Provider
eIDAS	electronic IDentification, Authentication and trust Services
IAM	Identity und Access Management
IdP	Identity Provider
IoT	Internet of Things
ISMS	Infomationssicherheitsmanagementsystem
ITIL	IT-Service-Management
LB	Leistungsbezüger
LE	Leistungserbringer
OIDC	OpenID Connect
PIN	Personal Identification Number
PUF	Physical Unclonalbe Function
RA	Registrierungsstelle
RP	Relying Party
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SoD	Segregation of Duties
SSO	Single Sign-On
TLS	Transport Layer Security
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Anhang D – Glossar

In diesem Standard werden ausschliesslich die Begriffe aus dem eCH-Standard eCH-0219 V1.0 [1] verwendet.

Anhang E – Identity Federation Modelle

Sobald mehrere RPs und IdP/AAs im Spiel sind, spricht man von *Identity Federation* Modellen. Auf dieser Ebene sind verschiedene Szenarien möglich, welche sich je nach Ziel und Randbedingungen besser oder schlechter eignen.
Folgende fünf Umsetzungs-Varianten sind Situations-spezifisch optimal. Bei der Umsetzung einer *föderierten IAM*-Lösung gilt es eines dieser Varianten oder deren Mischform zu implementieren.

E.1 – RP-zentriertes Modell

Das *RP-zentrierte Modell* (vgl. Abbildung 25) ist für eine *Relying Party* geeignet, welche eine *Ressource* für eine grössere Anzahl Partnerorganisationen zur Verfügung stellt. Die Subjekte dieser Organisationen können sich bei ihrem Heimat-IdP oder Heimat-IdP/AA (in Abbildung 25 als Vermittler mit angeschlossen IdP und AA) ihrer *Domäne* authentisieren und mit ihren *Attributen* auf die *Ressource* zugreifen. Der grosse Vorteil für die *Relying Party* liegt darin, dass sie die *E-Identities* nicht selbst verwalten muss. Ihr reicht die *Authentifizierungs*- und *Attributbestätigung*, um das *Subjekt* für den *Zugriff* auf die *Ressource* zu berechtigen.

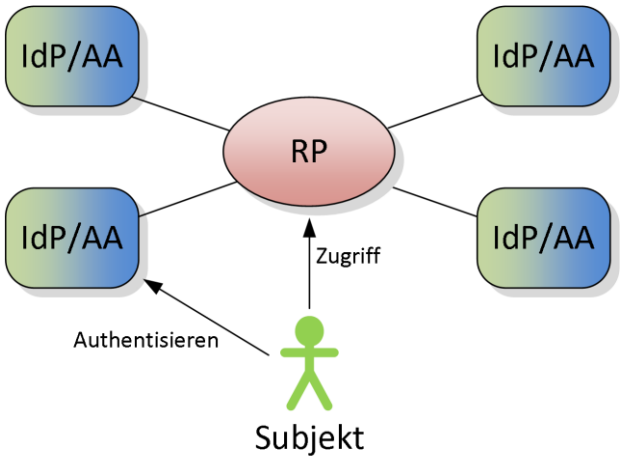


Abbildung 25 RP-zentriertes Modell

E.2 –Vermittler-zentriertes Modell

Das *Vermittler-zentrierte Modell* (vgl. Abbildung 26) wird eingesetzt, wenn mehrere *IAM*-Systeme auf einen einzigen Vermittler mit angeschlossenem IdP und AA konsolidiert werden, welches dann von möglichst vielen *Relying Parties* zur Authentifizierung und *Autorisierung* der *Subjekte* verwendet wird. Innerhalb einer Organisation ist dies meist einfach umzusetzen. Über Organisationsgrenzen hinweg hingegen gibt es vielfach grosse rechtliche Hürden, um dieses Szenario umsetzen zu können.

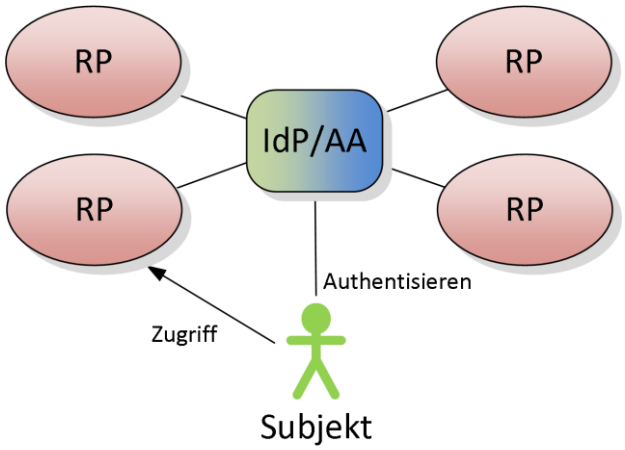


Abbildung 26 Vermittler-zentriertes Modell

E.3 – Cross Domain Modell

In einem *Cross Domain Modell* kann jede Organisation sowohl einen Vermittler mit angeschlossenem *Identity Provider und Attribut-Autorität* betreiben wie auch *Relying Party* sein. Dies ist ein häufiges Szenario, wenn ein *Vermittler-zentriertes Modell* nicht umgesetzt werden kann. Alle Organisationen stellen auf der einen Seite die *E-Identities* ihrer *Subjekte* gegen aussen zur Verfügung und betreiben auf der anderen Seite selbst *Ressourcen*, welche über die *Cross Domain* Infrastruktur sowohl von internen Subjekten (über den eigenen Vermittler) wie auch von externen *Subjekten* verwendet werden können.

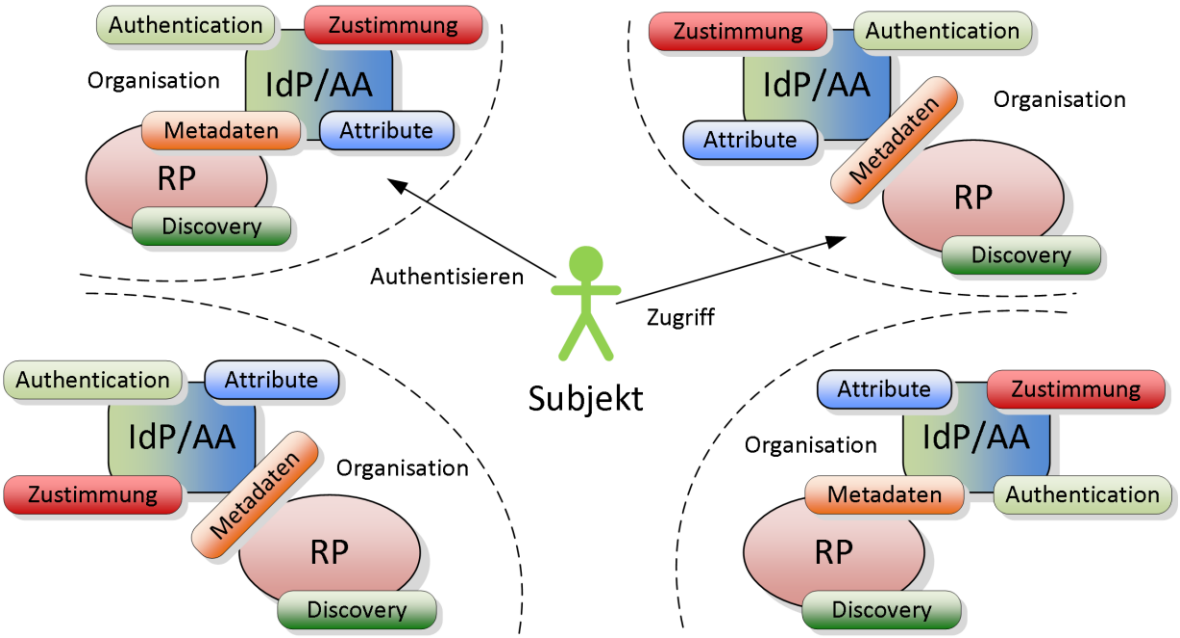


Abbildung 27 Cross Domain Modell

Jede Organisation tauscht im *Cross Domain Modell* Peer-to-Peer ihre *Metadaten* und *Identity Provider* Discovery-Informationen aus. Wenn der Verbund der Organisationen zu gross wird, skaliert dies schlecht. Deshalb werden diese Dienste vielfach zentralisiert und von einem vertrauenswürdigen Betreiber unterhalten (vgl. Abschnitt E.4).

E.4 – Zentralisierte Metadaten und Discovery

Die Auslagerung der beiden Dienste Metadaten und Discovery, wie in Abbildung 28 dargestellt, stellt ein typisches Szenario dar. Ein zentraler IAM-Dienstanbieter verwaltet und publiziert die Metadaten aller beteiligter Komponenten mit einem Metadata Aggregator (MDA) Service und unterhält zudem einen zentralen Discovery Service (DS).

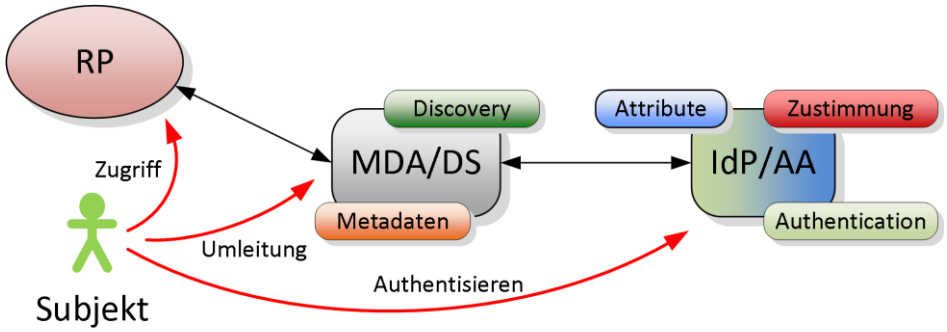


Abbildung 28 Zentralisierte Metadaten und Discovery Service

Es können aber noch weitere Dienste zentralisiert werden, wie das *Hub-'n'-Spoke Modell* in Abschnitt E.5 aufzeigt.

E.5 – Hub-'n'-Spoke Modell

Das Hub-'n'-Spoke[16] Modell basiert auf einem zentralen *Identity Hub*, welchem alle beteiligten Parteien mit ihren Diensten vertrauen. Wie in Abbildung 29 gezeigt, kann dieser *Identity Hub* weitere Dienste von den Parteien übernehmen und zentral ausüben. Der Protokollablauf zur Laufzeit wird in diesem Modell verändert und damit direkter. Die RPs kommunizieren nur noch mit dem zentralen *Identity Hub*. Dieser unterhält eine zentrale Tabelle mit den *E-Identities* der *Subjekte* (Identity Linking). Damit kann er das *Subjekt* bei einem der angegebenen *Identity Provider* authentifizieren lassen, kann Attributinformationen von anderen Vermittlern zusammentragen und stellt diese zu einer aggregierten Antwort an die *Relying Party* zusammen.

[16] Nabe und Speiche

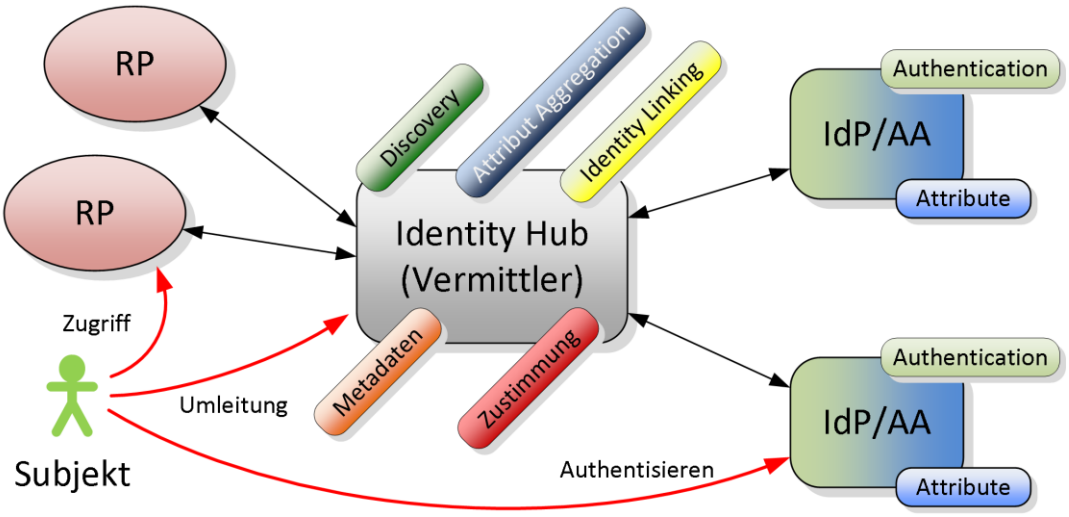


Abbildung 29 Hub-'n'-Spoke Modell

Das in Abbildung 29 dargestellte *Hub-'n'-Spoke Modell* zeigt eine Möglichkeit der Zentralisierung von Diensten auf. Es sind hier ganz verschiedene Ausprägungen der Zentralisierung möglich, wie es auch Mischformen der hier vorgestellten *Identity Federation* Modelle gibt.

Unabhängig von der Art eines eingesetzten *Identity Federation* Modells stellt die (elektronische) Zusammenarbeit über Organisationsgrenzen in jedem Fall eine Herausforderung an die Planung, Vereinheitlichung der Prozesse und Semantik sowie an die Infrastruktur dar. Je grösser ein Organisationsverbund in einer Identity Federation ist, umso mehr muss ein vertragliches Regelwerk die Richtlinien für die Beziehungen der einzelnen Parteien festlegen.

E.6 – Proxied Federation

In einer Proxied Federation, einem Spezialfall des *Hub-'n'-Spoke Modell* (Kapitel E.5), wird die direkte Verbindung von IdP (oder IdP/AA) zur einer RP vermieden, die Kommunikation findet über einen Vermittler (Proxy) statt.

Dieser Proxy agiert auf der einen Seite als RP gegenüber dem IdP und auf der anderen Seite als IdP gegenüber der RP.

Dieses Modell hat mehrere Vorteile. Zum einen wird die technische Integration zw. RP und IdP durch ein gemeinsames, standardisiertes Interface vereinfacht. Zum anderen kann damit die Informationsgebende (IdP/AA) und die Informationskonsumierende Ebene (RP) getrennt werden. Dadurch kann allgemein eine Blindisierung zwischen diesen beiden Ebenen erreicht werden um damit u.a. die Anforderungen an den Schutz der Privatsphäre R1 und R2 aus Kapitel 9.1 erfüllen zu können.

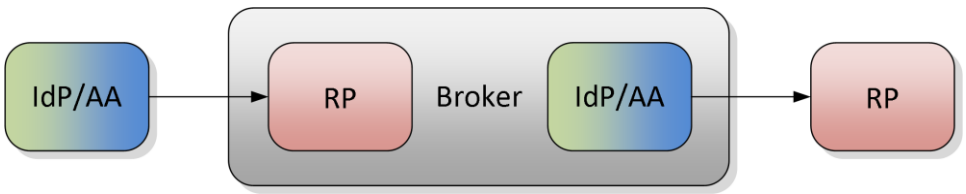


Abbildung 30 Proxied Federation

Anhang F – Änderungen gegenüber Version 2.00

Der vorliegende Standard basiert auf dem Gestaltungsprinzip eCH-0107 v2.00. Es sind in der Überarbeitung aber wesentliche neue Erkenntnisse und Konzepte eingeflossen.

So wurde eCH-0107 in der Version 3.0 in wesentlichen Teilen überarbeitet.

Nachfolgend werden die generellen Änderungen aufgeführt und auf die jeweiligen Inhalte in eCH-0107 Version 2.00 verwiesen.

Grundsätzliches:

- *Der Aufbau der Kapitel wurde nicht grundsätzlich geändert, sondern die einzelnen Kapitel wurden überarbeitet.*
- *V2.0 beschränkt sich konsequent auf das organisationsübergreifendes IAM.*
- *Das Glossar von V2.0 enthielt viele Begriffe aus dem IAM, die nicht im Dokument verwendet wurde. Um in Zukunft eine einheitliche Terminologie bei allen IAM-Standards verwenden zu können, wurde dieses Glossar in einen eigenen Standard (eCH-0219 [1]) ausgelagert. Im Dokument selbst werden nur einige zum Verständnis notwendigen die verwendeten Begriffe zitiert.*

Einleitung [eCH-0107 V2.0 Kapitel 2]

- *Die Einleitung wurde komplett überarbeitet und auf föderiertes IAM in organisations-übergreifenden Kontext fokussiert.*

Kapitel 3 Rollen und Stakeholder [eCH-0107 V2.0 Kapitel 3]

- *Es wird neu zwischen Stakeholder und Rollen im IAM unterschieden; während die Stakeholder den motivierenden Aspekt beschreiben, sind die verschiedenen Rollen die Ausführenden der Prozesse aus Kapitel 6. Die Beziehungen zwischen Stakeholdern und Rollen werden beschrieben.*

Kapitel 4 Anforderungen

- *Die Designprinzipien und allgemeine Anforderungen an ein föderiertes IAMSystem wurden überarbeitet und durch neue Erkenntnisse (z. B. aus eCH-0168* [12]*, eCH-0174* [13]*, eCH-0170* [9]*) ergänzt. Sie wurden neu strukturiert, klassifiziert und begründet.*
- *Die Anforderungen der verschiedenen Stakeholder wurden überarbeitet, erweitert, begründet.*

Kapitel 5 Informationsarchitektur [eCH-0107 v2.00 Kapitel 5]

- *Das Informationsmodell wurde erweitert. Dabei wurden die Ergänzungen aus dem eCH-Standard eCH-0170* [9] *übernommen und in das vorhandene Modell übernommen.*
- *Eine weitere Ergänzung betrifft das Subjekt, das neu zusätzlich* ***Dinge*** *umschliesst, sowie die Unterscheidung von handelnden und nicht handelnden Organisationen. Auch die Delegation von Rechte wird neu addressiert.*

Kapitel 6 Prozesse [eCH-0107 v2.00 Kapitel 5]

- *Die Prozesse wurden aktualisiert, ergänzt und konkretisiert. Neu ist die feinere Unterteilung der Prozesse und die Hinzunahme der unterstützenden Prozesse (Kapitel 6.5). Alle Prozesse wurden durch Anforderungen aus Kapitel 4 motiviert.*

Kapitel 7 Geschäftsservices [eCH-0107 v2.00 Kapitel 6]

- *Die Geschäftsservices wurden wesentlich überarbeitet und auf föderiertes IAM ausgelegt.*
- *Für alle Geschäftsservices wurden die Schnittstellen definiert.*
- *Kapitel 7.5 wurde aufgrund der Aktualisierung der Prozesse in Kapitel 6.1 komplett überarbeitet.*

Kapitel 8 IAM für das IoT [neu]

- *Das Kapitel adressiert die Anforderungen und Auswirkungen des IoT auf die Gestaltungsprinzipien der Identitäts- und Zugriffsverwaltung (IAM).*

Kapitel 9 Privacy [neu]

- Dieses Kapitel beschreibt Anforderungen zum Schutz der Privatsphäre des Subjektes und Richtlinien zur Verwaltung und Verarbeitung von subjektbezogenen Daten.

Das Kapitel **Identity Federation Modells [eCH-0107 v2.00 Kapitel 6]** wurde aktualisiert und in den Anhang E verschoben.