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 thomas.kessler@temet.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

TODO

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 verbunden 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 *Ressourcen* und *Subjekte* 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.

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

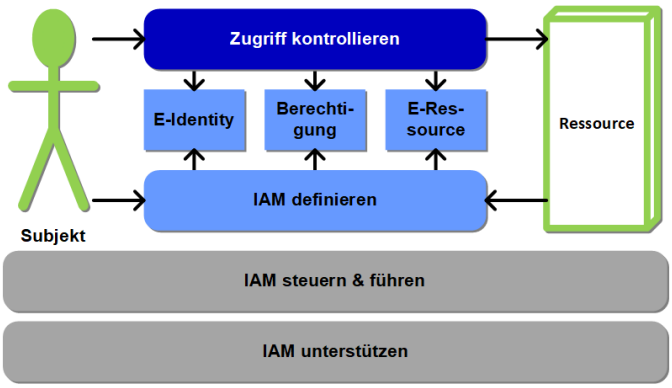


Abbildung 1 IAM im Überblick

Die Elemente *Zugriff kontrollieren* und *IAM definieren* stellen die Kernprozesse dar, welche vom *Subjekt* und der *Ressource* genutzt werden. Diese Kernprozesse werden zu unterschiedlichen Zeitpunkten verwendet, welche durch die hellblaue und dunkelblaue Farbe symbolisiert werden.

grau	Grau visualisiert in diesem Dokument Elemente, die bereits vor der Definitionszeit aktiv sind (z.B. Governance).
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 und führen* beschreibt die Aktivitäten für die Definition der notwendigen Vorgaben und Rahmenbedingungen und die Führung für den Betrieb einer IAM Umgebung.

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

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 [1], der die Architektur des E-Government Schweiz definiert, zu Grunde gelegt.

Der eCH-0107 definiert die Prinzipien, die Regeln und den Ordnungsrahmen für die IAM-Systemgestaltung, welche beim Bereitstellen von organisationsübergreifenden IAM-Lösungen im föderalen E-Government Schweiz zu berücksichtigen sind.

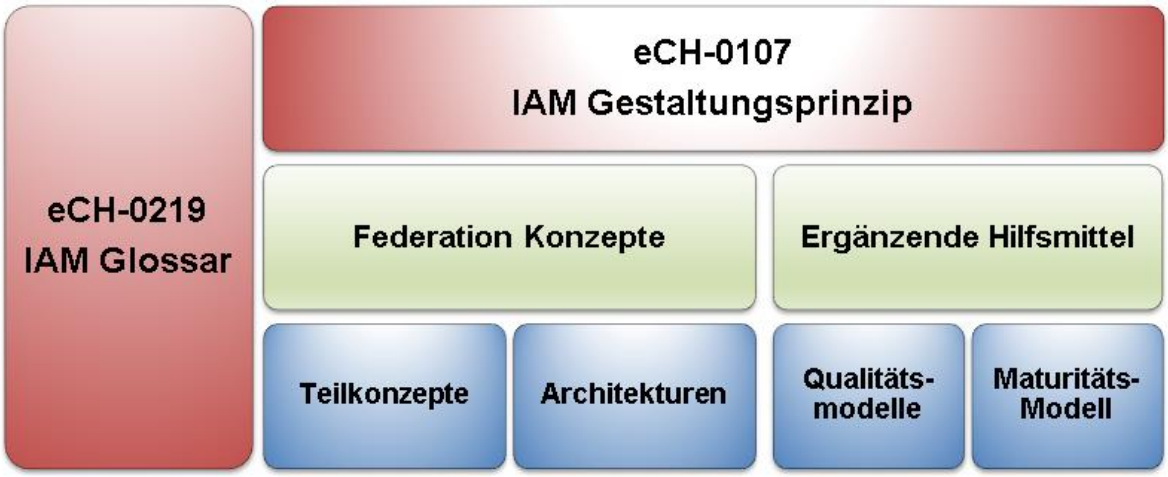


Abbildung 2: Einordnung des eCH-0107 Standards

Unter dem Standard eCH-0107 positionieren sich die Konzepte für föderierte IAM-Lösungen und ergänzende Hilfsmittel. Im IAM Glossar (eCH-0219 [2]) 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.

Die Anforderungen und Design Prinzipien sind beim Bereitstellen von organisationsübergreifenden *IAM*-Lösungen im E-Government Schweiz zu berücksichtigen, damit lokale Anwendungen und Dienste organisationsübergreifend genutzt werden können.

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 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 und die häufigsten Stakeholder 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.

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

TODO

2.2 Schwerpunkte

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

Kapitel 3 identifiziert die wichtigsten Stakeholder und Rollen in einem föderierten *IAM*.

In Kapitel 4 werden die Grundprinzipien und die allgemeinen Anforderungen ein föderierten IAM-Systems 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 vom *IAM*-Anbieter 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 beschriebt 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 und Rollen	Normativ
4 Anforderungen	Normativ
4.3 Anforderungen der Stakeholder	Deskriptiv
5 Informationsarchitektur	Normativ
6 Prozesse	Die Benennungen und deren Definition sind normativ und die Tätigkeiten und Anmerkungen 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 Stakeholder und Rollen

Das Identity und Access Management hat fünf grundlegende Stakeholder, die je nach Kombination und Ausgestaltung unterschiedliche Rollen einnehmen. Die fünf Stakeholder und ihre grundlegende Zusammenarbeit sind in Abbildung 3 dargestellt und werden anschliessend kurz beschrieben. Die Beziehungen zwischen den Stakeholdern zeigen, wer mit wem in Beziehung steht und von wem der Erstkontakt ausgeht.

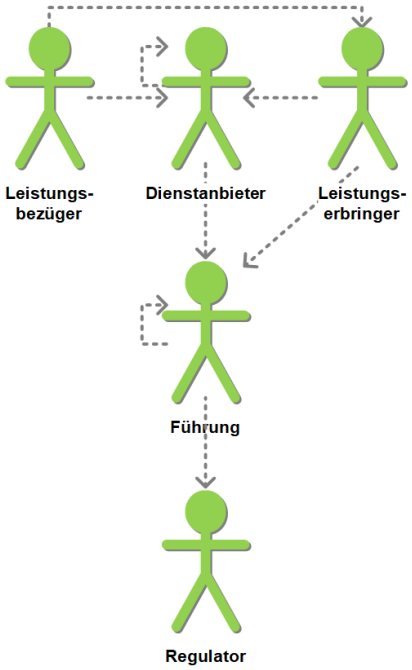


Abbildung 3 Stakeholder und deren Zusammenarbeit

Leistungsbezüger (LB)	Der Leistungsbezüger möchte eine fachliche Leistung[1] in Anspruch nehmen, die in Form einer Ressource von einem Leistungserbringer zur Verfügung gestellt wird. Dazu muss der Leistungsbezüger Dienste für die Authentifizierung und Autorisierung verwenden, die von Dienstanbietern zur Verfügung gestellt werden.
Leistungserbringer (LE)	Der Leistungserbringer stellt Ressourcen zur Verfügung, die von Leistungsbezügern verwendet werden. Zum Schutz der Ressourcen nimmt er gemäss seiner Bedürfnisse (z.B. Risikobereitschaft, Wirtschaftlichkeit) Dienste der Dienstanbieter in Anspruch.

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

Dienstanbieter	Der Dienstanbieter stellt einen oder auch mehrere (IAM-)Dienste zur Verfügungen, die es dem Leistungsbezüger ermöglicht auf Leistungen zuzugreifen und gleichzeitig diese zu schützen.
Führung	Die Führung koordiniert Leistungserbringer und Dienstanbieter, um das IAM-System zu implementieren und zu regelkonform betreiben.
Regulator	Der Regulator möchte durch die Definition der rechtlichen, prozessualen, organisatorischen, semantischen und technischen Rahmenbedingungen für das IAM-System, die Interoperabilität, Robustheit und Sicherheit sicherstellen.

Die Stakeholder können verschiedene Rollen im IAM-System annehmen. Die Rollen werden im Anschluss kurz beschrieben.

Relying Party	Die *Relying Party* vertritt die Interessen der *Ressource*. Sie nutzt IAM-Geschäftsservices und verarbeitet Informationen von *IAM-Dienstanbietern* für den Schutz seiner *Ressourcen*. Sie braucht zur Beurteilung der *Berechtigung* eines Ressourcenzugriffs nähere Informationen zu einem *Subjekt*.
IAM-Dienstanbieter	Der *IAM-Dienstanbieter* ist Betreiber von einem oder mehreren IAM-Geschäftsservices gemäss Kapitel 7. Es werden die folgenden Entitäten unterschieden, die aber oft gemeinsam implementiert werden. Die *Registrierungsstelle* (*RA*) erfasst und prüft die E-Identities der Subjekte. Der *Credential Service Provider* (CSP) vergibt und verwaltet Authentifizierungsmittel für E-Identitäten. Der *Identity Provider* (*IdP*) überprüft zur Laufzeit die E-Identity des Subjekts. Die *Attribut-Autorität* (*AA*) verwaltet die Attribute der Subjekte und gibt Attributbestätigungen aus. Ein *Vermittler* bietet gemeinsame Dienste, wie Metadaten, Discovery oder Identity Linking, für alle anderen Stakeholder in einer Identity Federation an.

IAM-Regulator	Der *IAM-Regulator* (oder *IAM-Steuerung*) definiert die rechtlichen, prozessualen, organisatorischen, semantischen und technischen Rahmenbedingungen, innerhalb derer das IAM abgewickelt werden kann. Er beteiligt alle anderen Rollen in geeigneter Weise an der Definition.
IAM-Führung	Die *IAM-Führung* ist verantwortlich für das Managen der IAM Dienstanbietern und der Relying Parties analog ITIL oder IT4IT in allen Fachbereichen wie z.B. Release-Management, Qualitätsmanagement, IAM-Lieferanten- und -Konsumentenmanagement, Inzident-, Event-, Service-Request-Management. Dies kann sowohl im internen Kontext als auch über Verträge/SLA mit externen IAM-Dienstanbietern und -Konsumenten geschehen.
IAM-Support	Der *IAM-Support* ist verantwortlich für alle Aktivitäten zum Auffinden und Lösen von Problemen, die zur Lauf- oder Definitionszeit auftreten können.
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.

Die Stakeholder können in einem IAM-System unterschiedliche Rollen einnehmen. In Tabelle 3 ist aufgezeigt, welcher Stakeholder welche Rollen übernehmen kann, dabei wird zwischen Hauptrollen (X), Nebenrollen (x) und optionalen Funktionen unterschieden.

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

Tabelle 3 Beziehungen der Stakeholder zu den Rollen

Die Stakeholder haben an die verschiedenen Rollen in einem IAM-System unterschiedliche Anforderungen, die in Tabelle 4 überblicksmässig dargestellt werden. Die konkreten Anforderungen sind in Kapitel 4 aufgeführt.

Rollen / Stakeholder	Subjekt	Relying Party	IAM-Dienst-anbieter	IAM-Führung	IAM-Support	IAM-Regulator
Leistungs-bezüger		X	X		X	(X)
Leistungs-erbringer	(X)		X	X	X	X
Dienstanbieter	(X)	?	X	X	X	X
Führung		X	X			X
Regulator						

Tabelle 4 Anforderungen der Stakeholder an die Rollen

4 Anforderungen

Die in diesem Kapitel beschriebenen und definierten Prinzipien und Anforderungen müssen angewendet oder erfüllt werden, damit ein effektives und effizientes föderiertes IAM 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.

Bezeichnung	Typ	Beschreibung
Prinzip-1	A	Informationen und Daten MÜSSEN föderiert statt repliziert werden.
Prinzip-2	A	Für die *Authentifikation* und den *Zugang* SOLLTEN die *Ressourcen* von ihr entkoppelte Dienste nutzen.
Prinzip-3	A/D	Anstatt Rollen und darauf basierende Berechtigungen zu pflegen, SOLLTEN vorrangig Attribute zur Berechtigung verwendet werden.
Prinzip-4	A	Der *Zugang* SOLLTE auf Grund der angegebenen *Attribute* gewährt werden.
Prinzip-5	A/B	Der *Autorisierung* für einen *Zugriff* auf eine *Ressource* MUSS (sofern fachlich nötig) die *Authentifikation* des zugreifenden *Subjekts* vorausgehen.
Prinzip-6	B	Organisationsübergreifende Effektivität und Effizienz des IAM MUSS auf gegenseitigem spezifischem Vertrauen in die Partner basieren.
Prinzip-6.1	B	Zum Aufbau von Vertrauensbeziehungen (Trusts) mit anderen Domänen und zur Nutzung anderswo definierter E-Identities und Attribute MÜSSEN föderierte Konzepte verwendet werden.
Prinzip-7	A	Soweit von der Vertrauensstufe her möglich, KÖNNEN bestehende E-Identities, Authentifizierungs- und Attributbestätigungen von anderen Stellen übernommen werden (Föderation).
Prinzip-8	A/D	Wenn fachlich nicht notwendig, SOLLTEN keine Informationen eines zugreifenden *Subjekts* an die *Ressource* weitergegeben werden.
Prinzip-9	B	Die Einhaltung der rechtlichen, organisatorischen und technischen Vorgaben (insbesondere des Datenschutzes, sowie alle organisationsspezifischen Sicherheitsvorgaben) SOLLTE zu jeder Zeit gewährleistet sein.

4.2 Anforderungen an das föderierte IAM-System

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

Bezeich-nung	Typ	Beschreibung	Begründung
IAM-1	T/A	Das IAM SOLLTE auf einer international interoperablen Architektur basieren. [3]	Interoperabilität
IAM-1.1	T/A	Das IAM MUSS in andere IAM (auch auf internationaler Ebene) einfach integrierbar sein.	Interoperabilität
IAM-1.2	T/A	Das IAM KANN bestehende IAM-Lösungen einfach integrieren.	Interoperabilität
IAM-2	A/D	Die *Authentifikation* und *Berechtigung* für den *Zugang* SOLLTEN auf standardisierten *Authentifizierungsmitteln* und *Attributen basieren*.	Interoperabilität
IAM-3	T/A	Die IAM-Systeme MÜSSEN modular und SOLLTEN skalierbar aufgebaut sein.	Kosten, Wiederverwendbarkeit, Wartbarkeit
IAM-4	A	Die technischen Services MÜSSEN über standardisierte Schnittstellen zusammenarbeiten, welche offene Standards entsprechend ihrer Spezifikation (z.B. ‚Security Assertion Markup Language' (SAML)) benutzen.	Interoperabilität
IAM-5	T	Die je nach Schutzbedürfnissen notwendigen, unterschiedlich starken Authentisierungsverfahren KÖNNEN auf derselben IAM-Infrastruktur realisiert werden.	Interoperabilität, Kosten, Wiederverwendbarkeit
IAM-6	D	Die Menge der E-Identities, Authentifizierungsmittel und Attribute SOLLTE minimal gehalten und womöglich konsolidiert werden.	Kosten, Benutzerfreundlichkeit
IAM-7	A	Der Transport der Daten MUSS zwischen den Dienstanbietern auf Protokollebene abgesichert sein (z.B. TLS).	Sicherheit, Schutz der Privatsphäre
IAM-8	A	Die technischen Services, welche Authentifizierungs- und Attributbestätigungen erstellen oder konsumieren, MÜSSEN ihre Zeit mit einem zugelassenen Zeitserver synchronisieren.	Interoperabilität, Sicherheit, Robustheit
IAM-9	B/A	Die von den Geschäftsservices erstellten Authentifizierungs- und Attributbestätigungen MÜSSEN auf ihre Authentizität und Integrität überprüft werden können (z.B. mithilfe der Signatur).	Sicherheit
IAM-10	A	Es MUSS gewährleistet sein, dass jederzeit nachvollzogen werden kann, welches *Subjekt* wann auf welche *Ressource* zugegriffen hat.	Nachvollziehbarkeit
IAM-11	B/A/T	Es MUSS sichergestellt werden (z.B. durch Ver-	Schutz der Pri-

Bezeich-nung	Typ	Beschreibung	Begründung
		schlüsselung der Daten), dass Authentifizie-rungs- und Attributbestätigungen nur von be-rechtigten Instanzen gelesen werden können.	vatsphäre

4.3 Anforderungen der Stakeholder

Die Anforderungen der Stakeholder sind 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.

4.3.1 Anforderungen des Leistungsbezügers

Die subjektbezogenen Anforderungen werden von natürlichen Personen, Organisationen, Services oder Dingen gestellt, die auf Informationen und Services der *Ressourcen* zugreifen wollen.

Bezeich eich-nung	Typ	Beschreibung	Begründung	Referenz
LB-1	A/D	Der Leistungsbezüger MUSS sich nur dort authentisieren, wo es notwendig ist.	Need-to-Know-Prinzip	**Prinzip-8**
LB-1.1	B/A/T	Der Leistungsbezüger MUSS sich nur mit der minimal geforderten Vertrau-ensstufe authentisieren.	Kosten, Benutzer-freundlichkeit, Schutz der Pri-vatsphäre	**Prinzip-8**
LB-2	D	Der Leistungsbezüger MUSS nur einen eindeutigen Identifikator verwendet, wenn die Nutzung der Ressource das erfordert.	Schutz der Privatsphäre	**Prinzip-8**
LB-2.1	D	Der Leistungsbezüger SOLLTE einen pseudonymisierten Identifikator bei der Nutzung von Ressourcen verwenden.	Schutz der Privatsphäre (Un-linkability)	**Prinzip-8**
LB-3	D	Der Leistungsbezüger MUSS nur die Attribute übermitteln, die zur Berechti-gung oder zur Funktionserfüllung der Ressource notwendig sind.	Need-to-Know-Prinzip	**Prinzip-8**
LB-4	B/A	Der Leistungsbezüger SOLLTE seinen IAM-Dienstanbieter (IdP, AA) selbst auswählen.	Selbstbestimmung, Wahlfreiheit	
LB-5	D	Der Leistungsbezüger SOLLTE nur ei-ne geringe Anzahl von E-Identities be-nötigen.	Kosten, Benutzer-freundlichkeit, Kon-textabdeckung	**IAM-6**
LB-6	B	Der Leistungsbezüger SOLLTE selbst bestimmen, wie viele Authentifizie-rungsmittel verschiedener Qualität es haben will.	Selbstbestimmung, Wahlfreiheit	

Bezeich eich-nung	Typ	Beschreibung	Begründung	Referenz
LB-7	B	Der Leistungsbezüger SOLLTE bei der Authentisierung selbst bestimmen, welches Authentifizierungsmittel der minimal geforderten Qualität es bei der Authentifizierung verwendet.	Selbstbestimmung, Wahlfreiheit	**Prinzip-7**
LB-8	B	Die Beschaffung von E-Identities und Authentifizierungsmitteln SOLLTE einfach und günstig sein.	Kosten	
LB-9	A	Die Benutzung von E-Identities und Authentifizierungsmitteln SOLLTE einfach und unkompliziert sein.	Benutzerfreundlichkeit	
LB-10	B	Ein anderer Leistungsbezüger KANN als Stellvertreter handeln.	Delegation	
LB-11	B/A	Der Leistungsbezüger MUSS der Weitergabe von Attributen explizit zustimmen, ausser das Recht zur Weitergabe ist gesetzlich verankert oder anderswo geregelt.	Schutz der Privatsphäre	**Prinzip-9**
LB-12	B/A	Der Leistungsbezüger MUSS Unterstützung bei Vermeidung und Recovery des Missbrauchs einer E-Identity erhalten. [3]	Benutzerfreundlichkeit, Sicherheit	
LB-13	B/A/T	*IAM-Dienstanbieter MÜSSEN* das vernünftig Machbare unternehmen, um den Missbrauch der *E-Identity* des *Subjekts* zu verhindern. [3]	Schutz der Privatsphäre, Sicherheit	**LE-13, Führ-3**
LB-14	A	Die IAM-Dienstanbieter und Ressourcen MÜSSEN in Kooperation das Subjekt beim Lösen von Problemen, die eine erfolgreiche Nutzung der Ressource verhindern, unterstützen.	Benutzerfreundlichkeit	**Führ-6**
LB-15	A	Der Leistungsbezüger MUSS davon ausgehen können, dass die von ihm freigegebenen Attribute nur von berechtigten Instanzen gelesen werden können.	Schutz der Privatsphäre	**Prinzip-9**
LB-16	B	Die Nutzung der Ressource ist jederzeit möglich.	Verfügbarkeit	

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 *Ressourcen* SOLLTE nur auf autorisierte *Subjekte* eingeschränkt sein.	Sicherheit (Access Control)	**Prinzip-5**
LE-3	A	Falls das *Subjekt* keine Rechte für die aufzurufende *Ressource* hat, MUSS der Aufruf an die *E-Ressource* verworfen werden und entsprechend umgeleitet werden.	Sicherheit, Benutzerfreundlichkeit	
LE-4	B/A	Der Aufwand für die Verwaltung der *E-Ressourcen* SOLLTE minimal sein.	Kosten	
LE-5	B/A	Der Aufwand für die Verwaltung der *Berechtigungen* (*Zugangsregeln* und *Zugriffsrechte*) SOLLTE minimal sein.	Kosten	
LE-6	D	Die Menge der unterstützten E-Identities und *Attribute* MUSS minimal gehalten und SOLLTE womöglich konsolidiert werden.	Kosten	**IAM-6**
LE-7	A	Authentifizierungs- und Attributbestätigungen KÖNNEN durch *Dienstanbietern* unterschiedlicher Qualität ausgestellt werden. [3]	Interoperabilität	**Prinzip-7**
LE-8	A	Die konsumierten Authentifizierungs- und Attributbestätigungen MÜSSEN vertrauenswürdig sein und ihre Authentizität und Integrität MUSS überprüft werden.	Sicherheit, Trust	**Prinzip-6, IAM-9**
LE-9	B	Für natürliche Personen und *Organisationen* SOLLTE ein eindeutiger *Identifikator* verwendet werden. Im Idealfall kann es sich um einen staatlichen Identifikator handeln. [3]	Wiedererkennung des Subjekts	
LE-10	B	Die Einhaltung der rechtlichen, organisatorischen und technischen Vorgaben (insbesondere des Datenschutzes sowie alle organisationsspezifischen Sicherheitsvorgaben) SOLLTE zu jeder Zeit gewährleistet sein.	Rechtskonformität, Sicherheit, Robustheit	**Prinzip-9**
LE-11	B/D	Die Nachvollziehbarkeit und Nachweisbarkeit, welches *Subjekt* wann auf welche *Ressource* zugegriffen hat, MUSS gewährleistet sein.	Nachvollziehbarkeit	**IAM-10**
LE-12	B	Das *Subjekt* und die IAM-	Sicherheit	

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
		Dienstanbieter MÜSSEN den Verdacht eines Missbrauchs einer *E-Identity* melden. [3]		
LE-13	B/A/T	*IAM-Dienstanbieter MÜSSEN* das vernünftig Machbare unternehmen, um den Missbrauch der *E-Identity* des *Subjekts* zu verhindern. [3]	Schutz der Privatsphäre, Sicherheit	**Sub-13**

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* (Authentifizierungsmitteln und *Attribute*) SOLLTE minimal im Verhältnis zur angestrebten Qualität sein.	Kosten	
Dienst-2	D	Der Zusammenhang zwischen der *E-Identity* und den dazugehörigen Authentifizierungsmitteln MUSS zu jedem Zeitpunkt gewährleistet sein.	Nachvollziehbarkeit	**IAM-10**
Dienst-3	D	Die Menge der *Attribute*, die zur *Berechtigung* des *Subjekts* notwendig sind, SOLLTE minimal sein.	Kosten	**IAM-6**
Dienst-4	B	E-Identities und Attribute MÜSSEN bei Veränderungen zeitnah gepflegt werden.	Aktualität	
Dienst-5	B	Die Führung SOLLTE die Stabilität der prozessualen, organisatorischen, und technischen Aspekte des IAM-Systems, aber die Weiterentwicklung sicherstellen.	Kosten, Investitionsschutz	

4.3.4 Anforderungen der Führung

Dieser Abschnitt beschreibt die Anforderungen der Führung.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz

Bezeich eich-nung	Typ	Beschreibung	Begründung	Referenz
Führ-1	B/A	Die Dienstanbieter und Ressourcen SOLLTEN sich auf eine standardisierte Menge von Authentifizierungsmitteln und Attributen einigen.	Interoperabilität, Benutzerfreund-lichkeit, Führbarkeit	**IAM-2, IAM-6**
Führ-2	T	Die Dienstanbieter und Ressourcen SOLLTEN standardisierte Schnittstellen verwenden.	Interoperabilität	**IAM-4**
Führ-3	B/A	Die verschiedenen Dienstanbieter und die Ressourcen MÜSSEN zusammen-arbeiten, um das Subjekt bei Vermei-dung und Recovery des Missbrauchs seiner E-Identity zu unterstützen.	Benutzerfreund-lichkeit, Sicherheit	**LB-12**
Führ-4	B/D	Die verschiedenen Dienstanbieter und die Ressourcen MÜSSEN zusammen-arbeiten, so dass jederzeit nachvollzie-hen werden kann, welches *Subjekt* wann auf welche *Ressource* zugegrif-fen hat.	Nachvollziehbarkeit	**IAM-10, LB-12, LB-13, LE-13,**
Führ-5	B	Der IAM-Regulator MUSS die erforder-lichen rechtlichen, prozessualen, orga-nisatorischen, semantischen und tech-nischen Rahmenbedingungen für das betroffene IAM-System definieren.	Rechtskonformität, Sicherheit, Ro-bustheit	**Prinzip-9**
Führ-5.1	B	Die verschiedenen Dienstanbieter und die Ressourcen SOLLTEN die vom IAM-Regulator definierten Rahmenbe-dingungen einhalten.	Rechtskonformität, Sicherheit, Ro-bustheit	**Prinzip-9**
Führ-6	A	Die verschiedenen Dienstanbieter und die Ressourcen MÜSSEN gemeinsam das Subjekt beim Lösen von Proble-men, die eine erfolgreiche Nutzung der Ressource verhindern, unterstützen.	Benutzerfreund-lichkeit, Kosten	**LB-14**

4.3.5 Anforderungen des IAM-Regulators

Dieser Abschnitt beschreibt die Anforderungen der IAM-Regulatoren.

Bezeich zeich-nung	Typ	Beschreibung	Begründung	Referenz
Reg-1	B	Die verschiedenen Dienstanbieter und die Ressourcen MÜSSEN die definier-ten rechtlichen, prozessualen, organi-satorischen, semantischen und techni-schen Rahmenbedingungen einhalten und dokumentieren dies entsprechend.	Compliance	**Prinzip-9**

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 4 zeigt das Informationsmodell zum organisationsübergreifenden IAM.

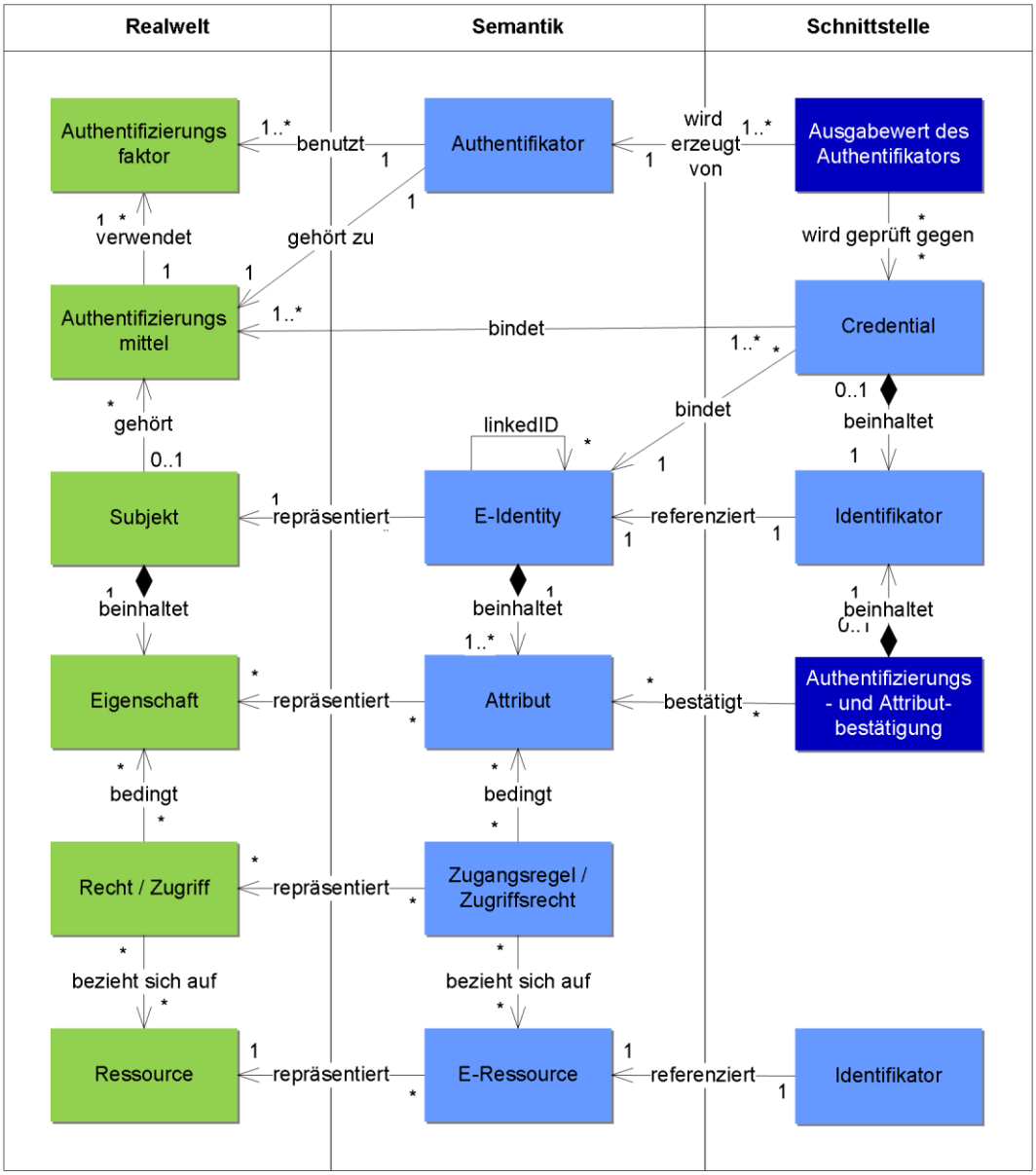


Abbildung 4 Informationsmodell

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 realen Welt wesentlich sind, werden hier für unterschiedliche Elemente auch unterschiedliche Bezeichner verwendet. Das Informationsmodell in Abbildung 4 zeigt links (in grün) die Ele-

mente 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.

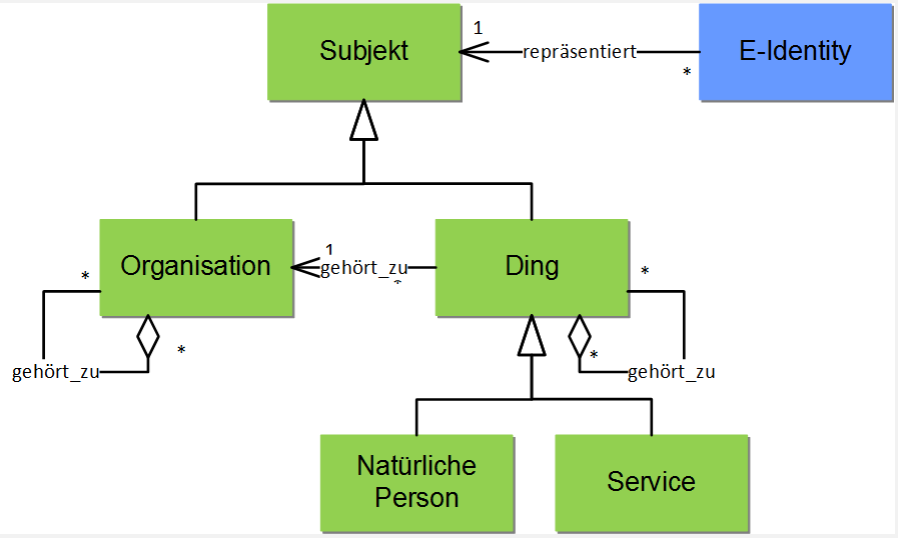
Zur Definitionszeit (siehe Prozesse in Abschnitt 6.2 und Geschäftsservices in Abschnitt 7.2) werden Objekte der realen Welt mit ihren Eigenschaften und Beziehungen in die Informationssysteme (Semantik) abgebildet.

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[2] die in der Abbildung 4 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/Zugriff	Die *Rechte* oder *Zugriffe*, welche das *Subjekt* braucht , um auf die *Ressource* zuzugreifen. Diese können z.B. in Gesetzen oder Verträgen festgelegt sein. Die Rechte oder *Zugriffe* werden aufgrund von *Eigenschaften* des *Subjektes* definiert.
Eigenschaften	*Eigenschaften* sind Charakteristika, Merkmale oder Verhalten eines *Subjekts*.

[2] Die vollständigen Beschreibungen mit Abbildungen und Beispielen sind im eCH-0219 [2] zu finden.

Subjekt	 **Abbildung 5 Subjekt Definition** Ein Subjekt ist 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* in der digitalen Welt repräsentiert. Natürliche Personen können zu einer *Organisation* gehören. Eine *Organisation* ist eine organisatorische Einheit aus mehreren natürlichen Personen. Eine Organisation kann (Unter-)Organisationen enthalten. Eine *juristische Person* ist eine spezielle *Organisation*, die auf einem Vertrag von zwei Organisationen (der juristischen Person und der anerkennenden Behörde) beruht. Einer juristischen Person muss immer mindestens eine natürliche Person zugeordnet sein. Ein *Ding* ist eine existierende oder abstrakte Einheit, die eindeutig identifizierbar ist. Dinge können weitere Dinge enthalten. Ein Ding kann zu einer *Organisation* oder zu einer *natürlichen Person* gehören (nicht zu einem Service). Ein *Service* ist über ein *Netzwerk* erreichbar und darin digital identifizierbar.
Authentifizierungsmittel	Etwas, das ein *Subjekt* besitzt und unter seiner Kontrolle hat (ein kryptographischer Schlüssel, ein Geheimnis, ein biometrisches Merkmal oder ein spezifisches Verhalten). Ein Authentifizierungsmittel kann einen (*single-factor authenticator*) oder auch mehrere unabhängige Authentifizierungsfaktoren (*multi-factor authenticator*) benutzen.

Authentifizierungs-faktor	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 *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.[3]
linkedID	Im organisationsübergreifenden Kontext erlaubt *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*).
Authentifikators	Funktionales Abbild des *Authentifizierungsmittels* der Realwelt. Mit der Funktion eines Authentifikators wird aus einem Eingabewert und einem geheimen Wert ein Ausgabewert erzeugt.

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

Schnittstelle	
Authentifizierungs- und Attributsbestätigung	Eine Bestätigung der erfolgreichen *Authentifikation* eines *Subjektes* (*Authentifizierungsbestätigung*, *Authentication Assertion*) oder eine Bestätigung eines *Attributs* (*Attributbestätigung*, *Attribute Assertion*). Enthält den *Identifikator*.
Identifikator	Eine Zeichenkette, welche ein *E-Identity* oder eine *E-Ressource* innerhalb eines *Namensraumes* eindeutig bezeichnet.[4]
Credential	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 5 Beschreibung der Elemente des Informationsmodels

[4] Der Identifikator einer Ressource ist oft eine URL/URI.

6 Prozesse

Abbildung 6 zeigt eine Übersicht über die Geschäftsprozesse. Sie dient zur Veranschaulichung der Top-Down-Tätigkeiten, welche für eine erfolgreiche Kooperation zwischen den Rollen in einem IAM-System (siehe Definitionen in Kapitel 3) notwendig sind. Die Abbildung 6 übernimmt die Prozesse aus der Abbildung 1 und ergänzt deren Teilprozesse.

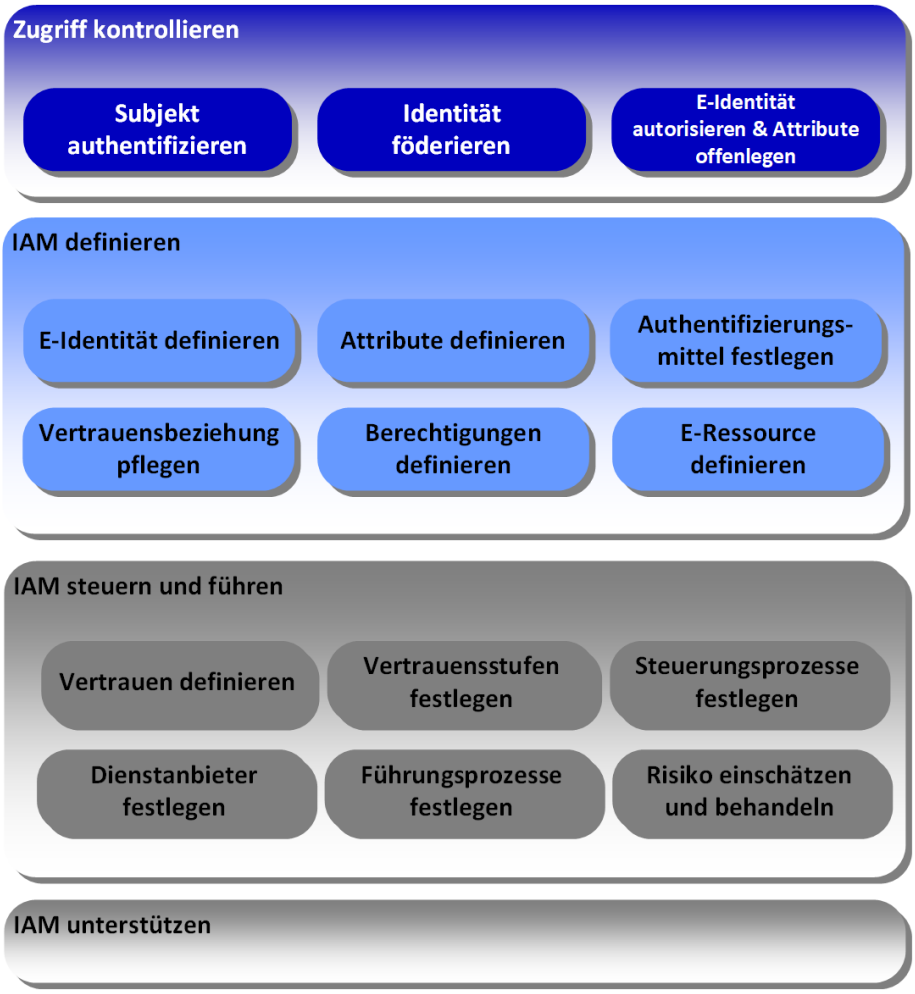


Abbildung 6 IAM-Prozesslandkarte

An diesen Prozessen beteiligen sich die verschiedenen Rollen gemäss Kapitel 3. Die nachstehenden Abschnitte beschreiben die Geschäftsprozesse mit ihren Teilprozessen.

6.1 Zugriff kontrollieren

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 Identiy Provider und Relying Party über ein Netzwerk getrennte Systeme sind, muss die bei der Authentifizierung bestätigte E-Identität des Subjekt zusätzlich noch föderiert werden (Prozess *Identität föderieren*).

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.

Bei auftretenden Fehlern wird der Prozessablauf bei den jeweiligen Überprüfungsschritten abgebrochen, die *Zugriffe* werden alle (auch die ohne Fehler) protokolliert.

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

6.1.1 Subjekt authentifizieren

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

Tätigkeiten:

- Das *Subjekt* verwendet ein ihm zur Verfügung gestelltes und unter seiner Kontrolle befindliches *Authentifizierungsmittel*.
- Das *Authentifizierungsmittel* generiert mit Hilfe des *Authentifikators* einen Ausgabewert aus den Eingaben des Subjekts (Geheimnis und optional anderen Eingabewerten).
- Das *Authentifizierungsmittel* sendet den generierten Ausgabewert an einen IdP zur Überprüfung.
- Der IdP prüft den generierten Ausgabewert mit dem *Credential* der behaupteten E-Identity. Ist die Prüfung positiv, ist die Authentifizierung erfolgreich.

6.1.2 Identität föderieren

Identität föderieren	Variante 1: Übergabe einer Authentifizierungsbestätigung vom IdP an die RP Variante 2: Übergabe einer Authentifizierungs- und/oder Attributbestätigung vom Vermittler an die RP

Beim Prozess *Identität föderieren* wird je nach verwendetem Identitiy Federation Modell (siehe auch Anhang E) zwischen zwei Varianten unterschieden:

Tätigkeiten Variante 1 (IdP an die RP):

- Der IdP überprüft, ob die RP berechtigt ist, eine Authentifizierungsbestätigung anzufordern.
- (optional) Der IdP holt das Einverständnis des Subjekts ein, die Authentifizierungsbestätigung an den aufrufenden Service (RP) zu übermitteln.
- Der IdP erzeugt Authentifizierungsbestätigung mit Zeitstempel, Signatur und optionaler Verschlüsselung.
- Der IdP übergibt die Authentifizierungsbestätigung an die RP.
- Die RP überprüft die Aktualität und Authentizität der Authentifizierungsbestätigung.

- 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).

Tätigkeiten Variante 2 (Vermittler an die RP):

- Der Vermittler überprüft, ob die RP berechtigt ist, eine Authentifizierungs- und Attributbestätigung anzufordern.
- (optional) Attributaggregation: Der Vermittler aggregiert die angeforderte Attribute.
- (optional) Der Vermittler holt das Einverständnis des Subjekts ein, die Authentifizierungs- und/oder Attributbestätigung an den aufrufenden Service (RP) zu übermitteln.
- Der Vermittler erzeugt eine Authentifizierungsbestätigung mit Zeitstempel, Signatur und optionaler Verschlüsselung.
- (optional) Der Vermittler erzeugt eine Attributbestätigung mit Zeitstempel, Signatur und optionaler Verschlüsselung.[5]
- Der Vermittler übergibt die Authentifizierungsbestätigung an die RP.
- (optional) Der Vermittler übergibt die Attributbestätigung an die RP.
- Die RP überprüft die Aktualität und Authentizität der Authentifizierungs- und Attributbestätigungen.
- In Abhängigkeit der verlangten Sicherheitsstufe muss die RP das Subjekt nach einer bestimmten Zeitdauer (unabhängig von ihren eigenen Richtlinien) erneut durch den Vermittler authentifizieren lassen (Re-Authentifizierung).

6.1.3 E-Identity autorisieren und Attribute offenlegen

E-Identity autorisieren & Attribute offenlegen	Prüfen der *Zugriffsberechtigung* einer *authentifizierten E-Identity* auf eine *E-Ressource* und Erteilen des *Zugriffs* auf eine *Ressource* zur Laufzeit. Dabei wird zwischen *Grob-* und *Feinautorisierung* unterschieden. Offenlegen von Attributen des Subjektes.

Tätigkeiten:

- Vorbedingung einer *Autorisierung* ist die erfolgreiche *Authentifizierung* des *Subjekts*.
- Die RP ermittelt die *Zugangsregeln* und *Zugriffsrechte* für den *Zugriff* auf die *E-Ressource*. Daraus werden die benötigten *Attribute* zur *E-Identity* abgeleitet.
- Die RP überprüft, ob die benötigten Attribute vorhanden sind.
- Die RP erlaubt den *Zugang* und den *Zugriff*. Das Subjekt greift anschliessend auf die *E-Ressource* zu.

[5] Die Authentifizierungs- und Attributbestätigungen werden im Normalfall gemeinsam vom Vermittler erzeugt und an die RP übergeben.

- Eine RP kann zusätzlich Attribute des Subjekts anfordern, wenn sie diese zur Erfüllung ihrer Funktion benötigt. (siehe Kapitel 9)

6.2 IAM definieren

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

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, Pflegen und Löschen von *E-Identities*

Tätigkeiten:

- *Subjekt* identifizieren und zugehörige *E-Identity* registrieren.
- *E-Identities* miteinander verlinken.
- *E-Identity* löschen.

Anmerkungen:

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

6.2.2 Attribut definieren

Attribut definieren	Definition, Pflege und Nutzung von *Attributen*.

Tätigkeiten:

- Antrag zur Zuteilung eines *Attributs* an eine dafür autorisierte Stelle schicken.
- Nach entsprechender Beglaubigung einem *Subjekt* entsprechende *Attribute* zuteilen.
- Die erhobenen / vorgelegten *Attribute* zur *E-Identity* registrieren.
- *Attribute* löschen.

Anmerkungen:

Ein *Attribut* 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

Credential definieren	Erstellen, Pflegen und Vergeben von *Authentifizierungsmitteln.*

Tätigkeiten:

- Erstellung, Erhebung und Vergabe von *Authentifizierungsmerkmalen* (z.B. Passwörter, Authentisierungszertifikat).
- Speicherung der öffentlichen Elemente der *Authentifizierungsmittel* (z.B. öffentlicher Schlüssel) zur *E-Identity* im Directory des *Identity Providers.*
- Aushändigung des *Authentifizierungsmittels* (ev. mehrere) an das *Subjekt*.
- Benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln.
- Revozierung von *Authentifizierungsmitteln*.

6.2.4 Vertrauensbeziehungen pflegen

Vertrauensbeziehungen pflegen	Erstellen, Pflegen und Löschen von vertrauenswürdigen *IAM-Dienstanbietern*

Tätigkeiten:

- Pflege der *Metadaten* zu den *IAM-Dienstanbietern.*
- Pflege der Vertrauensstufen für Authentifizierung und Attribute.
- Definieren und Widerrufen der Vertrauensbeziehungen (*Trust*) zwischen Stakeholdern, die im *föderierten* System Aufgaben wahrnehmen, z.B. von *Authentifizierungsbestätigung*, *Attributbestätigung* oder *Zugang* Services.
- Festlegen der Vertrauensanker über die Auswahl der Certificate Authority (CA).

6.2.5 E-Ressource definieren

E-Ressource definieren	Definition, Pflege und Nutzung von *E-Ressourcen*.

Tätigkeiten:

- *Ressource* identifizieren und zugehörige *E-Ressource* (mit *Identifikator*) registrieren
- *Schutzbedarf* der Ressource festlegen.
- *E-Ressource* löschen

Anmerkungen:

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

6.2.6 Berechtigung definieren

Berechtigung definieren	Zuweisen und Löschen von *Zugangsregeln* zur *Grobautorisierung* und *Zugriffsrechten* zur *Feinautorisierung*. Definition von Vertrauensbeziehungen

Tätigkeiten:

- Definieren von *Zugangsregeln* und *Zugriffsrechten* unter Verwendung der verfügbaren *Attribute* von *E-Identities* (gemäss Metadaten und Vertrauensbeziehungen aus *Vertrauen definieren*).
- Zuweisen von *Zugangsregeln* und *Zugriffsrechten* zu einer oder mehreren *E-Ressourcen*.
- Löschen von *Zugangsregeln* / *Zugriffsrechten.*

6.3 IAM steuern und führen

Der Geschäftsprozess *IAM steuern und führen* beschreibt die Aktivitäten für die Definition der notwendigen Vorgaben und Rahmenbedingungen und die Führung für den Betrieb einer IAM Umgebung.

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 etc.

6.3.1 Vertrauen definieren

Vertrauen definieren	Festlegen der Zusammenarbeit und Abläufe sowie der Vertrauensanker

Tätigkeiten:

- Festlegen der Vertrauensanker über die Auswahl der Certificate Authority (CA).
- Identifikation / Festlegung der Zusammenarbeit von *Domänen*: Im E-Government Umfeld erfolgt *IAM* in der Regel über mehrere *Domänen*. Die Organisation und Abläufe zwischen den *Domänen* sind klar zu regeln.

6.3.2 Vertrauensstufen festlegen

Vertrauensstufen festlegen	Festlegen, wie die Qualität der Authentifizierung eines Subjektes bestimmt, überprüft und verglichen werden kann.

Tätigkeiten:

- Qualitätsmodell für die Authentifizierung von Subjekten, dessen Kriterien und dessen Unterteilung definieren (z.B. nach eCH-0170 [4]).
- (Optional) Qualitätsmodell der Attributbestäatigungen, dessen Kriterien und dessen Unterteilung definieren (z.B. nach eCH-0171 [5]).

- Festlegen, wie die Qualität- und Vertrauensstufen zwischen IdP/AA und RP bzw. Vermittler übermittelt werden.

6.3.3 Steuerungsprozesse festlegen

Steuerungsprozesse festlegen	Definition der Nachvollziehbarkeit aller Prozesse. Festlegen von Prozessen und Regeln für die Authentifizierung ergänzte Prozesse (Revozierung, Ersatz, etc.)

Tätigkeiten:

- Festlegung der *IAM*-Policy: Die *IAM*-Policy (inkl. *IAM*-Strategie, *IAM*-Architektur) definiert die Randbedingungen und den Scope für die angestrebte *IAM*-Lösung.
- Erarbeiten und Aktualisieren der relevanten Compliance-Vorgaben: Identifikation der geltenden gesetzlichen, unternehmensinternen und vertraglichen Richtlinien / Regularien. Ebenfalls werden Veränderungen in den Vorgaben verfolgt und allfällige daraus resultierende Massnahmen identifiziert.
- Auditieren und kontrollieren der Umsetzung der Compliance-Vorgaben: Die *IAM*-Landschaft wird entsprechend den Qualitätsanforderungen durch regelmässige Audits geprüft. Ziel der Audits ist die Sicherstellung der Umsetzung der Vorgaben.
- Definition der Nachvollziehbarkeit der gesamten Prozessabläufe (z.B. das Ablegen der relevanten Dokumente) und deren Audit.
- Festlegen der Aufbewahrungsfristen der relevanten Daten für jeden Prozessschritt (siehe auch ISO 29115 [7] Kapitel „Record-keeping/recording)
- Festlegen der Prozesse und Regeln für Revozierung/Deprovisionierung von Authentifizierungsmitteln
- Festlegen der Prozesse und Regeln für den Ersatz von Authentifizierungsmitteln
- Festlegen der Verfügbarkeit (Service Level Agreements) der einzelnen Dienstanbieter.
- (Optional) Festlegen des Lebenszyklus einer Verknüpfung von natürlichen und juristischen Personen (z.B. Aktivierung, Aussetzung, Erneuerung, Widerruf) (siehe auch eIDAS 2015/1502 [6], Abschnitt 2.1.4).
- Maturitätsmodell und Maturitätsstufen festlegen.

Anmerkung:

- Der Standard eCH-0172 [21] definiert IAM Maturitätsstufen für unter anderem die Einstufung für die Prozess-Maturität der Steuerung und wird ergänzt durch ein Hilfsmittel mit konkreten Fragen zur Bestimmung dieser Maturität. Es gibt auch andere Maturitätsmodelle, eher generische Modelle, wie z.B. CMMI for Services v1.3 und die SCAMPI Beurteilung.

6.3.4 Dienstanbieter festlegen

Dienstanbieter festlegen	Festlegen der IAM-Dienstanbieter des IAM-Systems und Aufbau der Vertrauensbeziehungen zwischen diesen

Tätigkeiten:

- Festlegung der Organisation (Stakeholder) sowie ihrer Beziehung untereinander (Zusammenarbeit): Die *IAM*-Organisation beschreibt, wie die verschiedenen involvierten Stakeholder miteinander in Beziehung stehen, wer Entscheidungen trifft, wie die Verantwortlichkeiten geregelt sind, wie *Ressourcen* eingesetzt werden etc. Den entsprechenden Stakeholdern werden die geeigneten Rollen zugewiesen.
- Definieren der Vertrauensbeziehungen zwischen den Stakeholdern

6.3.5 Führungsprozesse festlegen

7.3.5 Führungsprozesse festlegen	

Tätigkeiten:

- Definition der *Rollen* mit Aufgaben, Kompetenzen und Verantwortung. Die Prozesse werden durch die Stakeholder ausgeführt. Diese haben eine (eventuell aber auch mehrere) *Rollen*.
- Reporting aller relevanten Aktivitäten, insbes. zur Compliance
- Auditieren und kontrollieren der Umsetzung der Vorgaben: Die *IAM*-Landschaft wird entsprechend den Qualitätsanforderungen durch regelmässige Audits geprüft. Ziel der Audits ist die Sicherstellung der Umsetzung der Vorgaben.

6.3.6 Risiko einschätzen und behandeln

Risiko einschätzen und behandeln	Definition der Abläufe zur Risikobehandlung (Risikoeinschätzung und -adressierung)

Tätigkeiten:

- Schutzbedarfsanalyse: Die Schutzbedarfsanalyse gewährleistet angepasste Sicherheitsanforderungen (so viel Sicherheit wie nötig, nicht so viel wie möglich).
- Durchführen und Festhalten einer Risikoanalyse.
- Erstellen eines Informations- und Datenschutzkonzepts.
- Kontinuierliche Verbesserung des Sicherheitskonzepts: wird in ISO 27001 definiert. Aufgrund der aktuellen Situation werden periodisch Massnahmen geplant, umgesetzt, überprüft und optimiert. Dieser Verbesserungsprozess ist ein bewährtes und effizientes Vorgehen und heute ein Kernelement von Best Practice.
- [OPTIONAL] Abstützung des Risikomanagements auf ein Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001.

- [OPTIONAL] Abstützung des Risikomanagements auf ein Framework wie COBIT.

6.4 IAM unterstützen

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

Tätigkeiten:

- Annahme und Bearbeitung von Problemfällen in Interaktion zwischen Subjekt, Ressource und allen beteiligten Dienstanbietern.
- Einrichten und Betrieb eines Tracking-Systems zur Bearbeitung und Nachvollziehen von Problemfällen.

7 Geschäftsservices

Nachfolgend werden alle *IAM*-Services, welche von den verschiedenen Rollen (siehe Kapitel 3) 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 des Prozesses *IAM steuern* (vgl. Abschnitt 6.3) 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 *Organisation* (*juristische Person)*, 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. Dies schliesst physische Ressourcen wie Gebäude und Anlagen, deren Benutzung über IT-Systeme gesteuert wird, ein.

Aufgaben (zur Laufzeit):

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

7.2 Services zur Definitionszeit

In Abbildung 7 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*.

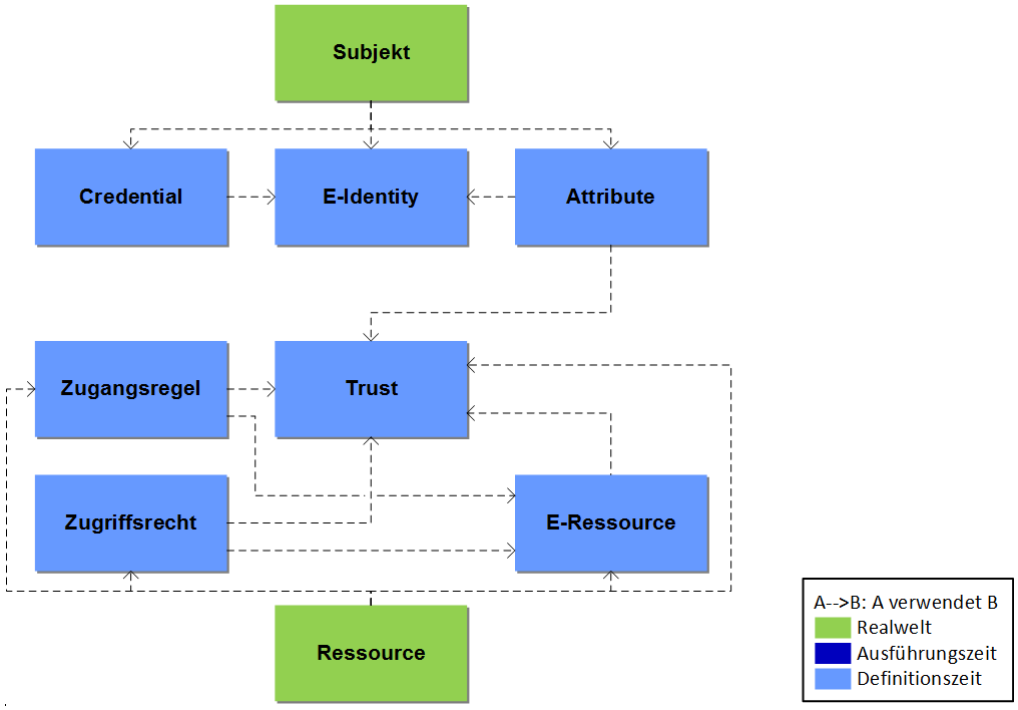


Abbildung 7 Geschäftsservices – Definitionszeit

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* in der Erneuerung ihrer *E-Identities*.
- Kann *E-Identities* widerrufen.
- 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 der 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 zeitaktuell 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*.

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* 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 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 8 dargestellt. Die Abbildung enthält alle Services, die zur Abwicklung der Prozesse *Subjekt authentifizieren* und *E-Identity autorisieren* zur Laufzeit verwendet werden.

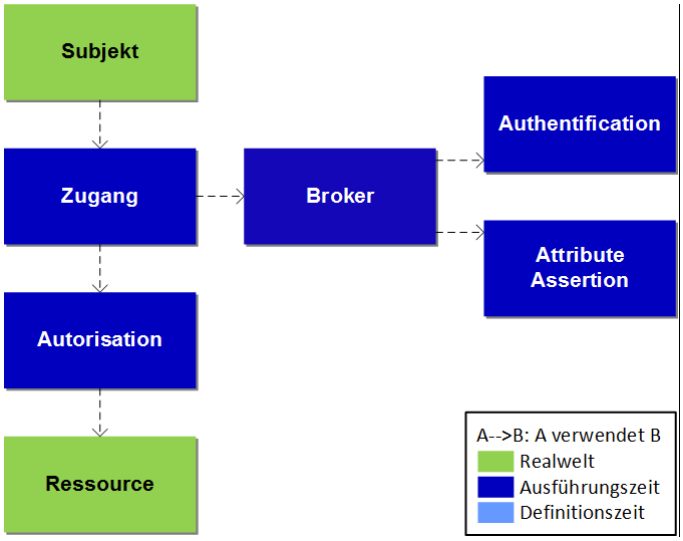


Abbildung 8 Geschäftsservices – Laufzeit

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:[6]

In: Authentifizierungs-Anfrage (*AuthenticationRequest)*,
(*Identifikator)*,
Authentifizierungsfaktoren

[6] 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).

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 [4]) 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 SignOn)

7.3.2 Attribute Assertion Service

Attribute Assertion Service	Eine *Entität*, die *Attributbestätigungen* über eine definierte Schnittstelle ausstellt.

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 [1]), 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 Authentifizierung und Attributbestätigung.

Schnittstelle:

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

Out: *Authentifizierungsbestätigungen,*
(Attributbestätigungen)

Braucht*: Trust Service, Logging 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 aufzukären.

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*

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

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

Aufgaben:

- Informiert das *Subjekt* über benötigte Sicherheitsinformationen (z.B. benötigte Attribute, geforderter Qualität-Level) bezüglich des *Zugriffs*.
- Fordert die *Authentifizierungsbestätigung* und, wenn nötig, *Attributbestätigung* entsprechend der *Zugangsregel* für die *E-Ressource* vom Authentication und Attribute Assertion Service an, oder nutzt einen Broker Service dafür
- 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 9 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.

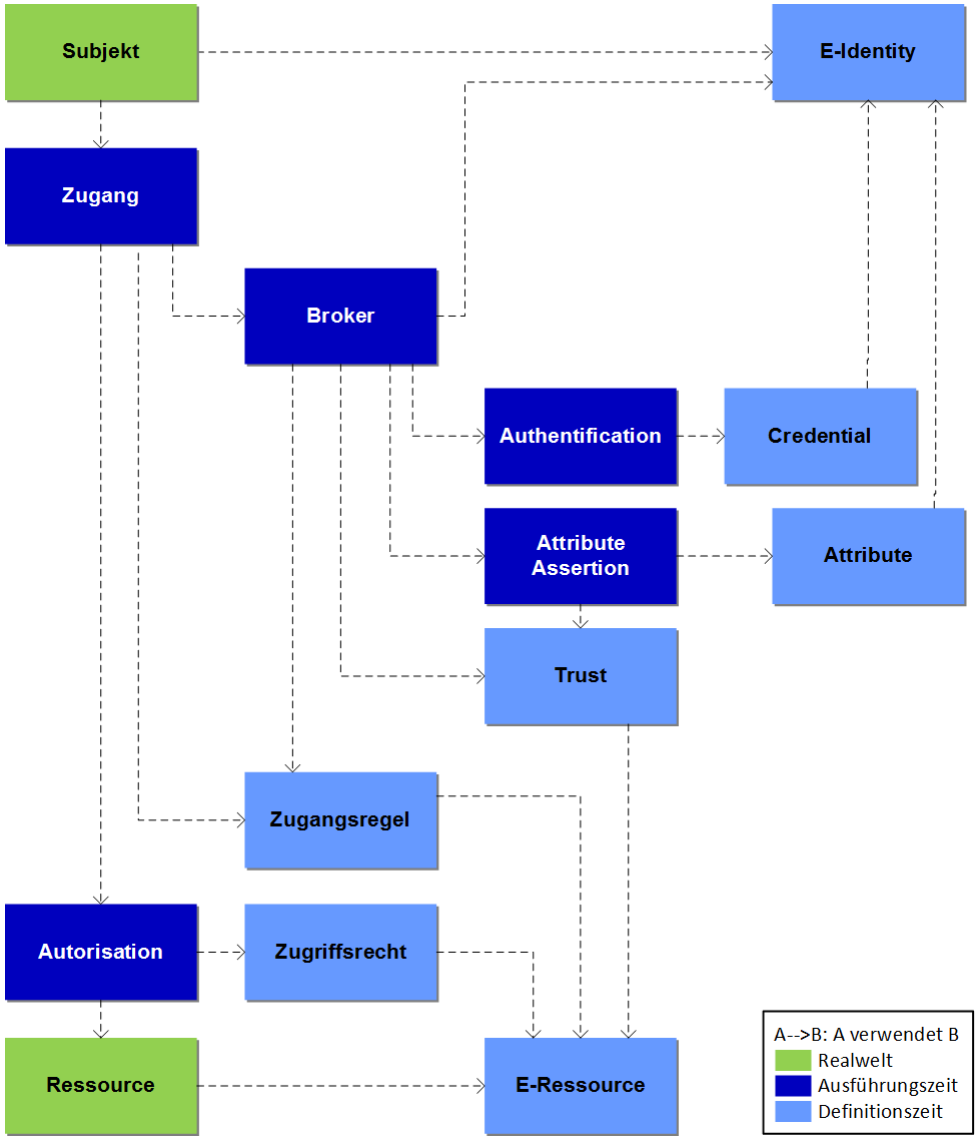


Abbildung 9 Geschäftsservices – Übersicht

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 einfach und in Abbildung 7 und in den Services bereits direkt angesprochen. Diese werden deshalb hier nicht dargestellt.

7.5.1 Subjekt authentifizieren

Abbildung 10 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *Subjekt authentifizieren*.

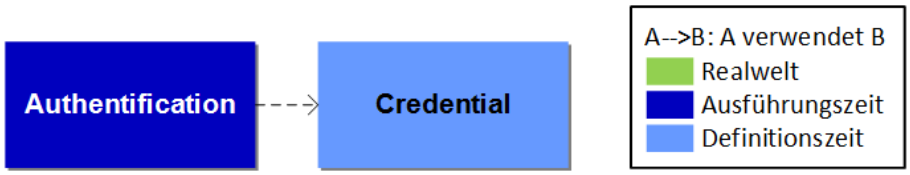


Abbildung 10 Prozessunterstützung *Subjekt authentifizieren*

Subjekt authentifizieren folgt dem nachstehenden Ablauf:

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

7.5.2 Identität föderieren

Abbildung 11 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *Identität föderieren*.

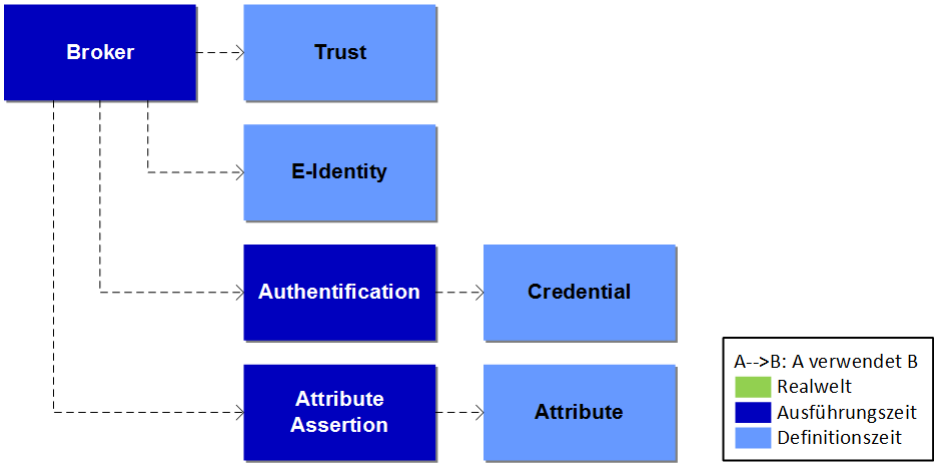


Abbildung 11 Prozessunterstützung *Identität föderieren*

Identität föderieren folgt dem nachstehenden Ablauf:

- Der *Broker Service* prüft, welche *Authentification* und *Attribute Assertion* Service gemäss *Trust Service* die Anforderungen des aufrufenden Service erfüllen.
- Der *Broker Service* delegiert die *Authentifizierung* des *Subjekts* an den gewählten *Authentification* Service (vgl. Abschnitt 7.5.1).

- Nach erfolgreicher Authentifizierung 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.
- 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 Ergebnis der Authentifizierung und die ermittelten Attribute an den aufrufenden Service zu übergeben
- Der *Broker Service* erzeugt Authentifizierungs- und Attributbestätigung und übergibt diese dem aufrufenden Service

7.5.3 E-Identity autorisieren und Attribute offenlegen

Abbildung 12 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *E-Identity autorisieren.*

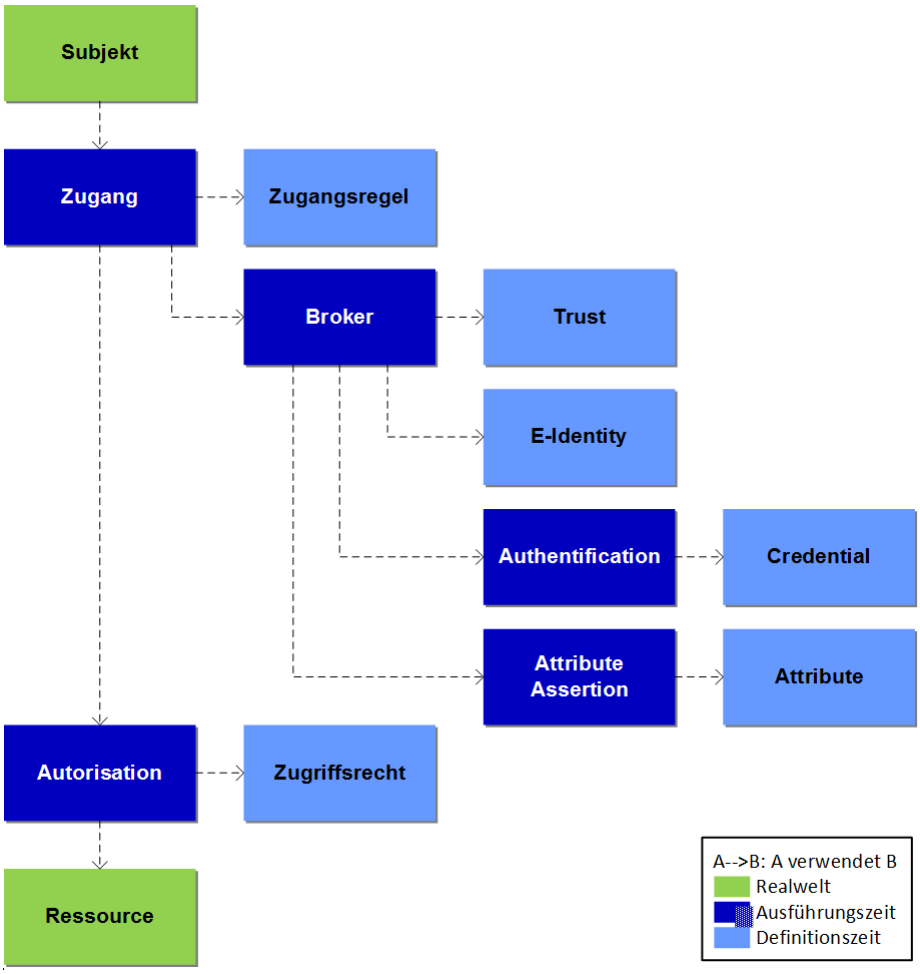


Abbildung 12 Prozessunterstützung *E-Identity autorisieren und Attribute offenlegen*

E-Identity autorisieren und Attribute offenlegen 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. Abschnitt 7.5.2)
- *Autorisation Service* prüft das Zugriffsrecht basierend auf den *Authentifizierungs- und Attribut-Bestätigungen.*
- *Autorisation* Service gewährt den *Zugriff* auf die *Ressource* und übergibt die *Authentifizierungs- und Attribut-Bestätigungen.*

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[7]	Attribut[8]	Zugangsregel	Zugriffsrecht	E-Ressource	Credential	Identifikator einer E-Identity	Ausgabewert des Authentikator	Authentifizierungs-bestätigung	Attributbestätigung	Identifikator einer E-Ressource
Geschäftsservice	E-Identity	B	B[9]					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[10]	LB[10]	
	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 6 Beziehung zwischen Services und Semantik des Informationsmodells

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

7.7 Zuständigkeiten für Geschäftsservices

Tabelle 7 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

fällen.

Tabelle 7 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[11].
- 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 (evt. 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.

[11] 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 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. [12] Eine in einem Authentisierungsvorgang unbeteiligter Externer soll nicht feststellen können ob und wann ein bestimmter Benutzer auf eine RP oder auf eine Ressource zugegriffen hat (z.B. durch zeitliche Korrelation)
R2	Unverkettbarkeit (Unlinkability)	Ein Benutzer kann mehrmals auf eine Ressource zugreifen, ohne dass unberechtigte Dritte diese Ereignisse verbinden können.	Ein Benutzer soll auf unterschiedliche RP's bzw. auf Ressourcen zugreifen können, ohne dass die Identität durch Korrelation der Identitätsdaten durch die beteiligten RP's oder durch Dritte aufgedeckt werden kann.

[12] Umgekehrt kann auch die Anforderung bestehen, dass eine beteiligte RP nicht feststellen können soll, bei welchem IdP/AA sich ein bestimmter Benutzer authentisiert hat. Diese Anforderung ist in der Praxis eher unrealistisch. Eine RP muss i.d. Regel prüfen können, bei welchem IdP/AA sich ein Benutzer authentisiert hat, um das notwendige Vertrauen aufbauen zu können.

ID	Name	Allgemeine Beschreibung	Typische Anwendungsszenarien
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.
R4a	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 [13].
R5	Einwilligung/Freigabe (Consent)	Die Freigabe von Identitätsinformationen an einen anfragenden Dienst kann ohne Einwilligung des Benutzers 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.

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,

[13] 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.

bei welchen Szenarien welche Massnahmen für den Datenschutz zu beachten sind. Dies soll die Vertrauenswürdigkeit der Dienstanbieter stärken.

9.2.1 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.

9.2.2 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.

9.2.3 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.

9.2.4 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.

9.2.5 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.

9.2.6 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.

9.2.7 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] eCH, «eCH-0122: Architektur E-Government Schweiz: Grundlagen, v1.0,» 2014. [Online]. Available: https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0122&documentVersion=1.0.

[2] eCH, «eCH-0219: IAM Glossar, v1.0,» 2017. [Online].

[3] «Protokoll Expertenworkshop “Sicherheitsopportunitäten für den Wirtschaftsstandort Schweiz” vom 8.11.2012 (zu Strategie Informationsgesellschaft)».

[4] eCH, «eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten, v2.0,» 2017. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170&documentVersion=2.0.

[5] eCH, «eCH-0171: Qualitätsmodell der Attributwertbestätigung zur eID,» 2014. [Online]. Available: https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0171&documentVersion=1.0.

[6] eCH, «eCH-0168: SuisseTrustIAM technische Architektur und Prozesse, V1.0,» 2014. [Online]. Available: https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0168&documentVersion=1.0.

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
Spichiger Andreas	Berner Fachhochschule, W
	eCH Fachgruppe IAM

Anhang C – Abkürzungen

AA	Attribute Authority
CP	Credential Provider
IAM	Identity und Access Management
IdP	Identity Provider
RP	Relying Party
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SSO	Single Sign-On
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 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 13) 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 13 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.

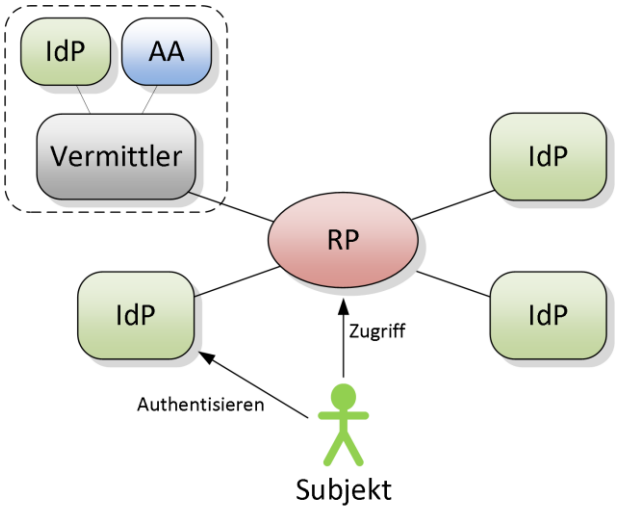


Abbildung 13 RP-zentriertes Modell

E.2 –Vermittler-zentriertes Modell

Das *Vermittler-zentrierte Modell* (vgl. Abbildung 14) 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.

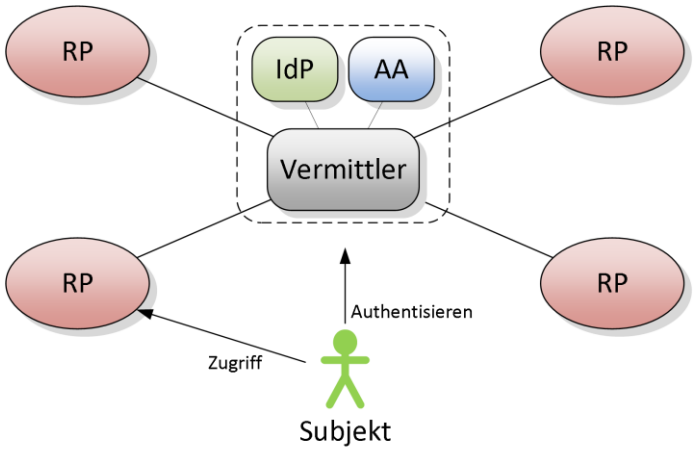


Abbildung 14 Vermittler-zentriertes Modell

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.

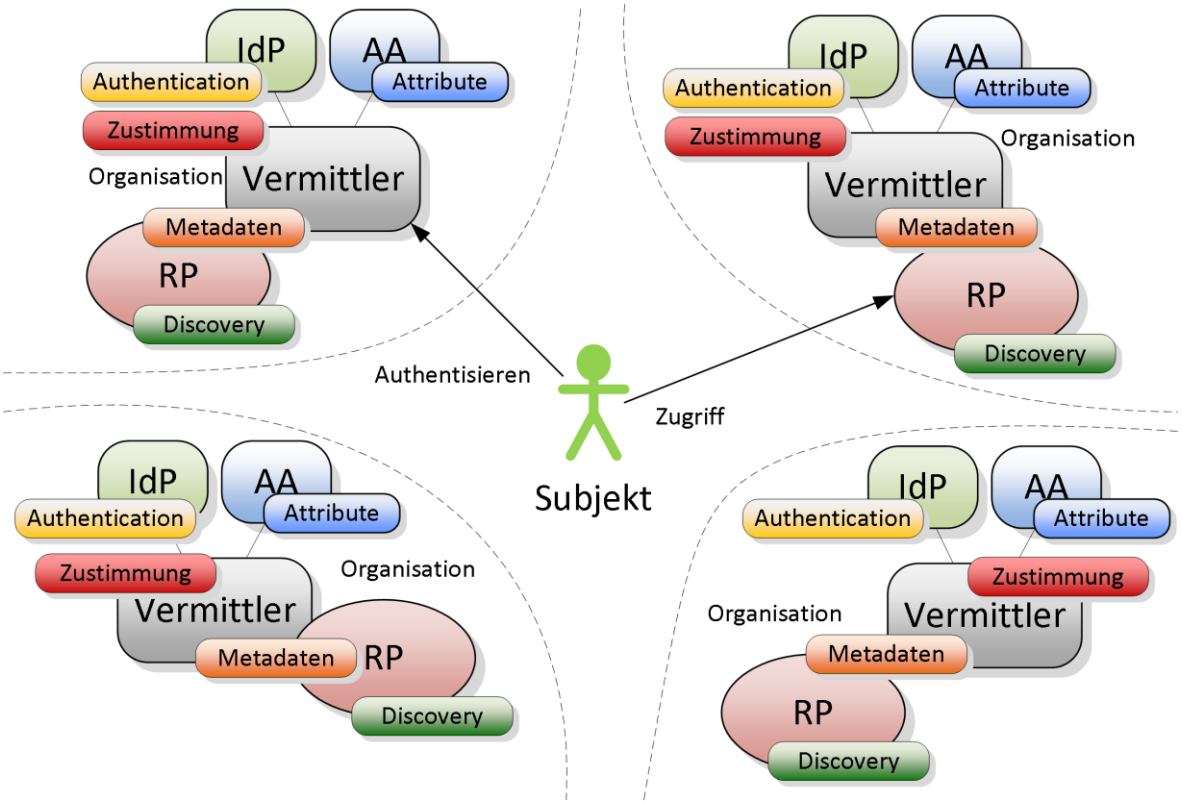


Abbildung 15 Cross Domain Modell

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 16 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).

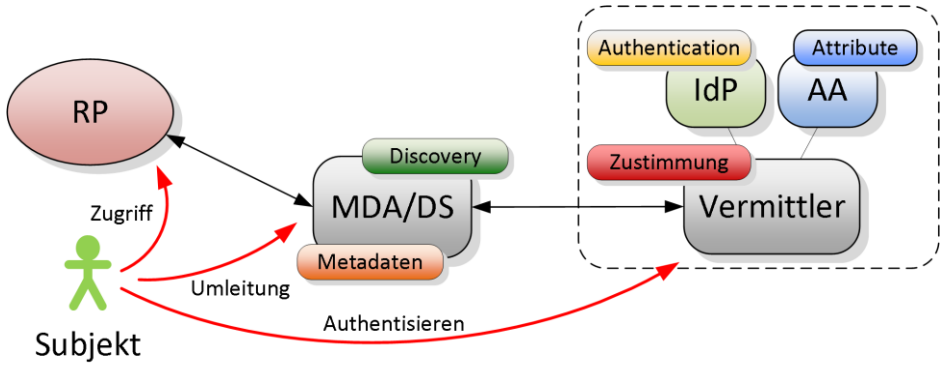


Abbildung 16 Zentralisierte Metadaten und Discovery Service

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[14] Modell basiert auf einem zentralen *Identity Hub*, welchem alle beteiligten Parteien mit ihren Diensten vertrauen. Wie in Abbildung 17 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.

[14] Nabe und Speiche

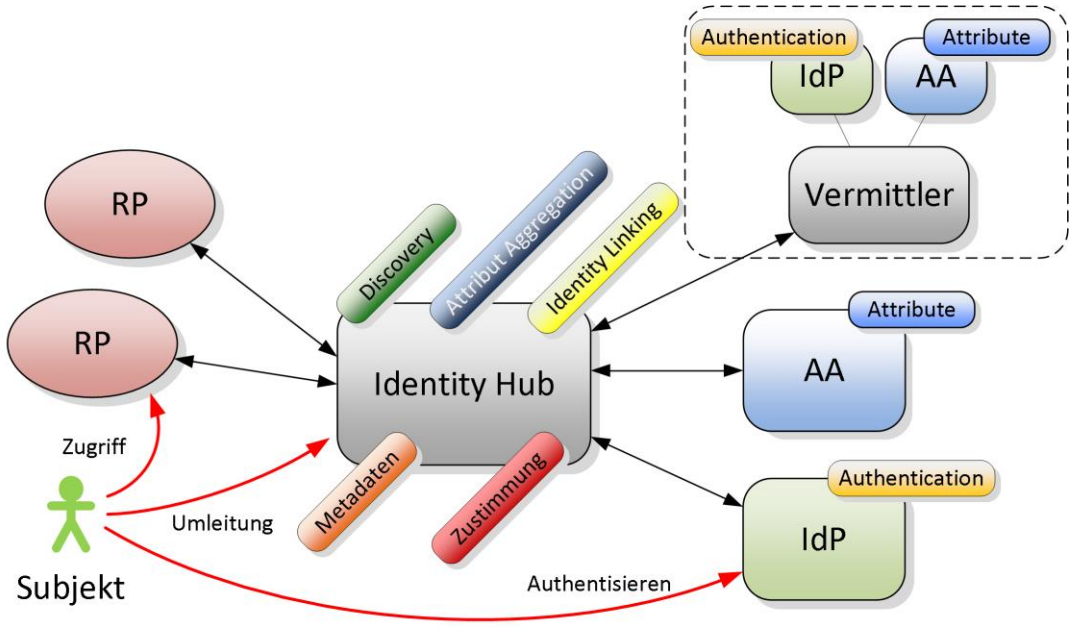


Abbildung 17 Hub-'n'-Spoke Modell

Das in Abbildung 17 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 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.

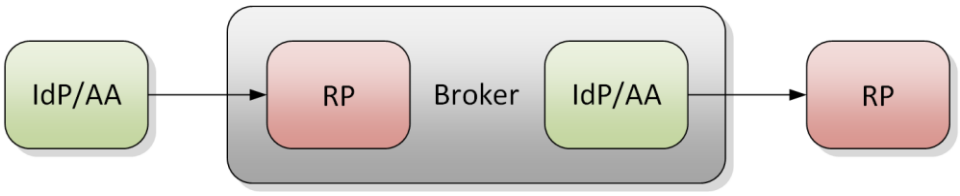


Abbildung 18 Proxied Federation

Anhang F – Änderungen gegenüber Version 2.00 (TODO)

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.*
- *Das Glossar on V2.0 enthielt viele Begriffe aus dem IAM, die nicht im Dokument verwendet wurde. Um in Zukunft eine einheitliche Terminologie beialle IAM-Standards verwenden zu können, wurde diese Glossar in einen eigenen Standard (eCH-0219* [2]*) ausgelagert. Im Dokument selbst werden nur die verwendeten Begriffe definiert (Anhang D – Glossar).*

Einleitung [eCH-0107 V2.0 Kapitel 2]

- *Glossar wurde deutlich erweitert, überarbeitet und in Anhang D ausgelagert.*
- *Die Einleitung wurde komplett überarbeitet und auf föderiertes IAM fokussiert.*

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

- *Neu: Rollen und Zuordnung zu Stakeholdern*

Kapitel 4 Anforderungen [eCH-0107 v2.00 Kapitel 4]

- *Die Architekturvisionen und allgemeinen Designprinzipien wurden neu eingeführt.*
- *Die Anforderungen wurden überarbeitet und durch neue Erkenntnisse ergänzt.*
- *Neu: Struktur und Erweitert mit Anforderung aus eCH-186/174*

Kapitel 5

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

- *Das Informationsmodell wurde erweitert. Dabei wurden die Ergänzungen aus dem eCH-Standard eCH-0170* [4] *übernommen und in das vorhandene Modell übernommen.*
- *Eine weitere Ergänzung betrifft das Subjekt, das neu zusätzlich* ***Dinge*** *umschliesst.*

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

- *Die Prozesse wurden aktualisiert und ergänzt.*

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

- *Neu: Schnittstellen*
- *Die Geschäftsservices wurden wesentlich überarbeitet und auf föderiertes IAM ausgelegt.*

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 in den Anhang E verschoben.