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 v1
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

Das vorliegende Dokument definiert die Prinzipien, die Regeln und den Ordnungsrahmen für die IAM-Systemgestaltung, welche beim Bereitstellen von föderierten IAM-Lösungen im föderalen E-Government Schweiz berücksichtigt werden. Das Gestaltungsprinzip definiert eine modellhafte IAM-Landschaft in organisationsübergreifenden Applikationsszenarien für bestehende und neue Anwendungen. Dabei wird davon ausgegangen, dass Geschäftsservices durch verschiedenste Stakeholder verteilt erbracht resp. genutzt werden können. Der Standard spezifiziert die Anforderungen, die Stakeholder, die Prozesse, die Informationsarchitektur, die Geschäftsservices und mögliche Identity Federation-Modelle. Der Standard kann in allen E-Society-Bereichen angewendet werden.

Inhaltsverzeichnis

1 Status des Dokuments 6

2 Einleitung 6

2.1 Überblick 6

2.1.1 Einführung IAM 6
2.1.2 Föderiertes IAM 8
2.1.3 Anwendungsgebiet 8
2.1.4 Abgrenzung 9
2.1.5 Vorteile 9

2.2 Schwerpunkte 9

2.3 Normativer Charakter der Kapitel 10

3 Stakeholder 11

4 Anforderungen 14

4.1 Architekturvision 14

4.2 Ressourcenbezogene Anforderungen 15

4.3 Subjektbezogene Anforderungen 15

4.4 Allgemeine Designprinzipien 16

5 Informationsarchitektur 16

6 Prozesse 21

6.1 Zugriff kontrollieren 22

6.1.1 Subjekt authentifizieren 22
6.1.2 Identität föderieren (optional) 23
6.1.3 E-Identity autorisieren und Attribute offenlegen 23

6.2 IAM definieren 24

6.2.1 E-Identity definieren 24
6.2.2 Attribut definieren 24
6.2.3 Credential definieren 25
6.2.4 E-Ressource definieren 25
6.2.5 Vertrauen definieren 25
6.2.6 Berechtigung definieren 26

6.3 IAM steuern und führen 26

6.3.1 Governance 26
6.3.2 Risk 27
6.3.3 Compliance 27

7 Geschäftsservices 28

7.1 Realweltobjekte 28

7.1.1 Subjekt 28

7.1.2 Ressource 28
7.2 Services zur Definitionszeit 29
7.2.1 E-Identity Service 29
7.2.2 Credential Service 30
7.2.3 Attribute Service 31
7.2.4 Trust Service 32
7.2.5 E-Ressource Service 32
7.2.6 Zugangsregel Service 33
7.2.7 Zugriffsrecht Service 33
7.3 Services zur Laufzeit 34
7.3.1 Authentication Service 34
7.3.2 Attribute Assertion Service 35
7.3.3 Broker Service 36
7.3.4 Zugang Service 37
7.3.5 Autorisation Service 38
7.3.6 Logging Service 38
7.4 Gesamtmodell 39
7.5 Prozessunterstützung durch Geschäftsservices 40
7.5.1 Subjekt authentifizieren 40
7.5.2 Identität föderieren 40
7.5.3 E-Identity autorisieren und Attribute offenlegen 41
7.6 Zuordnung Service zu Informationselemente 43
7.7 Zuständigkeiten für Geschäftsservices 44
8 IAM für das IoT 45
8.1 Spezielle Eigenschaften von Dingen 45
8.2 Auswirkung auf die IAM Informationsarchitektur 46
8.3 Auswirkung auf die IAM Geschäftsservices 48
9 Haftungsausschluss/Hinweise auf Rechte Dritter 49
10 Urheberrechte 49
Anhang A – Referenzen & Bibliographie 50
Anhang B – Mitarbeit & Überprüfung 51
Anhang C – Abkürzungen 52
Anhang D – Glossar 53
Anhang E – Identity Federation Modelle 61
E.1 – RP-zentriertes Modell 61
E.2 – IdP/AA-zentriertes Modell 61
E.3 – Cross Domain Modell 62

E.4 – Zentralisierte Metadaten und Discovery 62
E.5 – Hub-'n'-Spoke Modell 63
Anhang F – Änderungen gegenüber Version 2.00 65

Abbildungsverzeichnis

Abbildung 1 IAM im Überblick 7
Abbildung 2: Einordnung des eCH-0107 Standards 8
Abbildung 3 Stakeholder und deren Zusammenarbeit 11
Abbildung 4 Zuständigkeiten der Stakeholder 13
Abbildung 5 Informationsmodell 17
Abbildung 6 Subjekt Definition 19
Abbildung 7 IAM-Prozesslandkarte 22
Abbildung 8 Geschäftsservices – Definitionszeit 29
Abbildung 9 Geschäftsservices – Laufzeit 34
Abbildung 10 Geschäftsservices – Übersicht 39
Abbildung 11 Prozessunterstützung Subjekt authentifizieren 40
Abbildung 12 Prozessunterstützung Identität föderieren 40
Abbildung 13 Prozessunterstützung E-Identity autorisieren und Attribute offenlegen 41
Abbildung 14 Definition Subjekt 59
Abbildung 15 RP-zentriertes Modell 61
Abbildung 16 IdP/AA-zentriertes Modell 62
Abbildung 17 Cross Domain Modell 62
Abbildung 18 Zentralisierte Metadaten und Discovery Service 63
Abbildung 19 Hub-'n'-Spoke Modell 63

Tabellenverzeichnis

Tabelle 1 Farbverwendung im Dokument 7
Tabelle 2 Übersicht des normativen Charakters der Kapitel 10
Tabelle 3 Beschreibung der Elemente des Informationsmodels 21
Tabelle 4 Beziehung zwischen Services und Semantik des Informationsmodells 43
Tabelle 5 Beziehung zwischen Geschäftsservices und Stakeholder 44

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, 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.

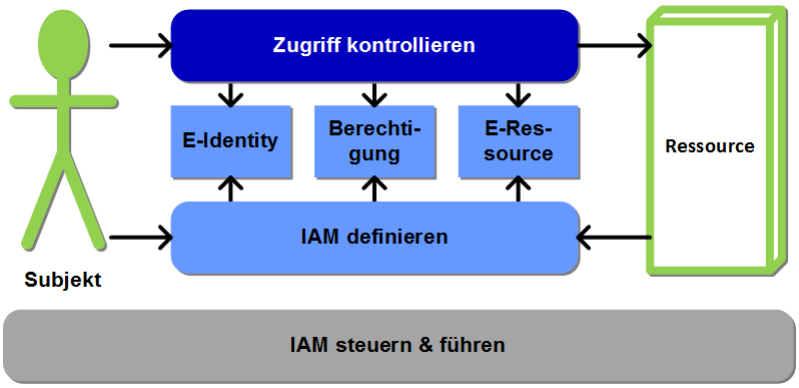


Abbildung 1 IAM im Überblick

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.
dunkel-blau	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.

2.1.2 Föderiertes IAM

Im Unterschied zum organisationsinternen IAM geht das *föderierte IAM* von organisationsübergreifenden *E-Identities* aus. Die *E-Identity* für ein *Subjekt* wird in der *Domäne* A erstellt, kann aber auch Informationen in der *Domäne* B besitzen, die der *E-Identity* der *Domäne* A zugeordnet sind. Weiter ist es möglich, dass Subjekte mit der *E-Identity* aus *Domäne* A auf *Ressourcen* aus der *Domäne* B zugreifen können. Damit ein *föderiertes IAM* etabliert werden kann, müssen sich die verschiedenen *Domänen* vertrauen. Dieses Vertrauen stützt sich auf explizite und implizite Vereinbarungen ab.

2.1.3 Anwendungsgebiet

Die Vision der Vernetzten Verwaltung und die damit verbundenen übergreifenden Prozesse im schweizerischen E-Government bedingen eine behördenübergreifende *Identitäts- und Berechtigungsverwaltung*. Der vorliegende Standard eCH-0107 bildet die Basis der IAM-Standardisierung. Er 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.

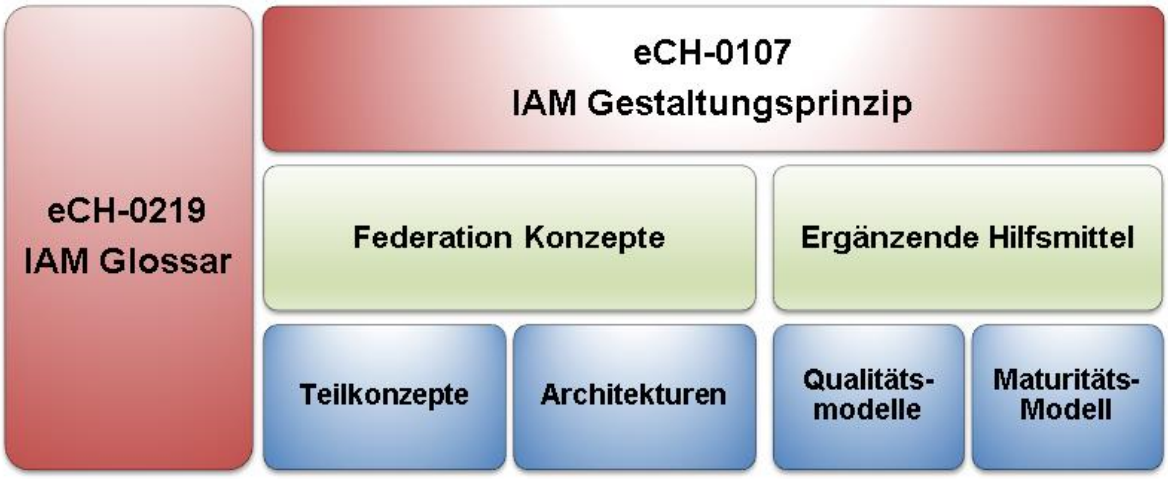


Abbildung 2: Einordnung des eCH-0107 Standards

Unter dem Standard eCH-0107 positionieren sich die Konzepte für föderierte IAM-Lösungen und ergänzende Hilfsmittel. 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.

2.1.4 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 Sicherheitsanforderungen umzusetzen. Entsprechend haben IAM-Lösungen selber die für sie geltenden, häufig hohen Sicherheitsanforderungen zu erfüllen. Diese sind in einschlägigen Sicherheitsstandards beschrieben und werden in diesem Standard nicht nochmals aufgeführt.

2.1.5 Vorteile

Im Umfeld des föderierten *IAM* wurden seit der Version 1 des eCH-0107 Standards wesentliche Fortschritte erzielt, welche nun in der zweiten Version des Standards dokumentiert und definiert werden. Dieser Standard erzielt folgende Vorteile:

- Ein Ordnungsrahmen für und die Anforderungen an föderierte *IAM*-Systeme sind definiert.
- Die Kernelemente eines föderierten *IAM* sind bekannt und stellen die Grundlage dar, um Lösungsideen und -vorschläge zu erarbeiten.
- Eine modellhafte *IAM*-Landschaft (Stakeholder, Prozesse, Informationsmodell, Geschäftsservices) im organisationsübergreifenden Anwendungsszenario ist definiert.
- Mögliche Konzepte für Identity Federations sind dargestellt.
- Begrifflichkeiten im Kontext des föderierten *IAM* sind in einem ausführlichen Glossar für das *IAM*-Umfeld geklärt und erlauben die Diskussion zu diesem Thema mit einem gemeinsamen Vokabular.

2.2 Schwerpunkte

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

Kapitel 3 identifiziert die wichtigsten Stakeholder eines föderierten *IAM*.

In Kapitel 4 werden die Architekturvision und die allgemeinen Anforderungen von Seiten der Realweltobjekte *Subjekt* und *Ressource* aufgelistet.

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.

Damit im föderierten *IAM*-Kontext jeweils von denselben Begrifflichkeiten gesprochen wird, ist im Anhang D ein ausführliches Glossar definiert, welches die wichtigsten Begriffe im *IAM*-Umfeld erklärt.

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
2 Einleitung	Deskriptiv
3 Stakeholder	Normativ
4.1 Architekturvision & 4.4 Allgemeine Designprinzipien	Normativ
4.2 Ressourcenbezogene Anforderungen & 4.3 Subjektbezogene Anforderungen	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
Anhang A – Referenzen & Bibliografie	Deskriptiv
Anhang B – Mitarbeiter & Überprüfung	Deskriptiv
Anhang C – Abkürzungen	Normativ
Anhang D – Glossar	Normativ
Anhang E – Identity Federation Modelle	Dieses Kapitel ist deskriptiv, soll aber zur Einordnung helfen.

Tabelle 2 Übersicht des normativen Charakters der Kapitel

3 Stakeholder

Das Identity und Access Management hat fünf grundlegende Stakeholder, die je nach Kombination und Ausgestaltung unterschiedliche Rollen einnehmen. Die vier 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.

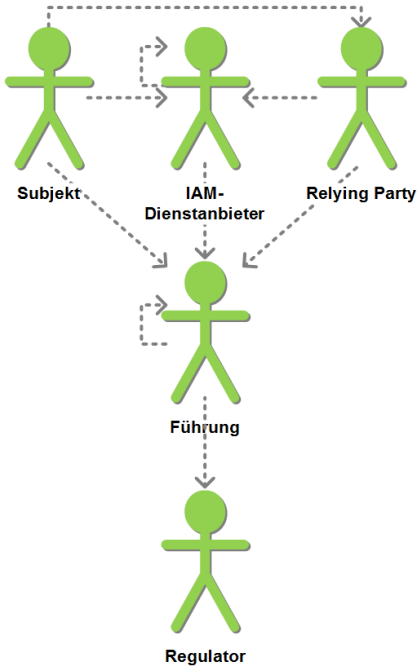


Abbildung 3 Stakeholder und deren Zusammenarbeit

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* definiert die rechtlichen, prozessualen, organisatorischen, semantischen und technischen Rahmenbedingungen, innerhalb derer das IAM abgewickelt werden kann. Er beteiligt alle anderen Stakeholder in geeigneter Weise an der Definition.
IAM-Steuerung und Führung	Die *IAM-Führung* ist verantwortlich für das Managen der IAM Dienstanbietern 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.
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 sind hierbei für unterschiedliche Teile des *IAM*-Gesamtprozesses zuständig. Ihre Zuständigkeiten sind in Abbildung 4 dargestellt. Dabei ist eine Überdeckung eines Prozesses mit mehreren Stakeholdern dahingehend zu interpretieren, dass die Stakeholder zur Erreichung des Prozessziels zusammenarbeiten müssen.

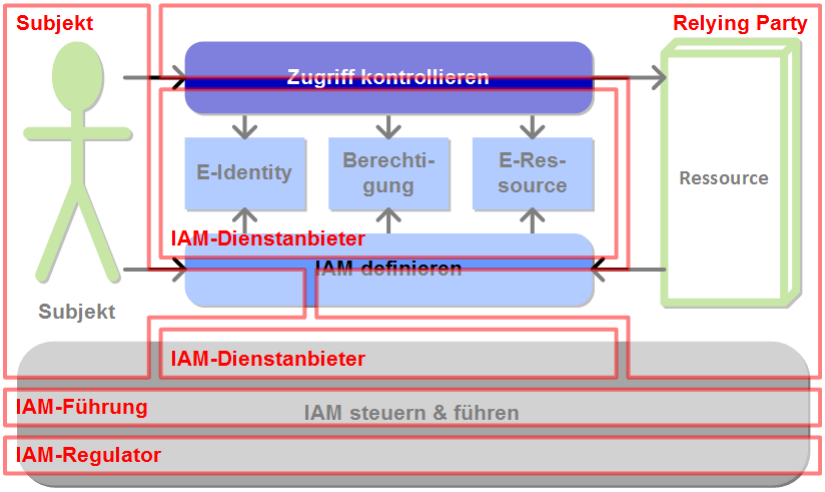


Abbildung 4 Zuständigkeiten der Stakeholder

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.

4.1 Architekturvision

Die Architekturvision beschreibt die allgemeinen Prinzipien für die Gestaltung von föderierten IAM.

- Das *Identity Management* basiert auf einer föderierten, international interoperablen Infrastruktur. [SOWISCH] — Vision-1
  - Das *IAM* ist in andere *IAM* (auch auf internationaler Ebene) einfach integrierbar. — Vision-1.1
  - Das *IAM* kann bestehende *IAM*-Lösungen einfach integrieren. — Vision-1.2

- Informationen und Daten werden föderiert statt repliziert. — Vision-2
- Anstatt Berechtigungseigenschaften zu pflegen, werden vorrangig Personeneigenschaften zur *Berechtigung* verwendet. — Vision-3

- Die *IAM*-Infrastrukturen sind modular und skalierbar aufgebaut. — Vision-4
- Die Geschäftsservices arbeiten über standardisierte Schnittstellen zusammen, welche offene Standards (z.B. ‚Security Assertion Markup Language' (SAML)) benutzen. — Vision-5
- Die je nach Schutzbedürfnissen notwendigen, unterschiedlich starken Authentisierungsverfahren können auf derselben *IAM*-Infrastruktur realisiert werden. — Vision-6
- Die Menge der *Credentials* und *Attribute* ist minimal zu halten und womöglich zu konsolidieren. — Vision-7
- Organisationsübergreifende Effektivität und Effizienz des *IAM* bedingt Vertrauen in die Partner. — Vision-8
- Zum Aufbau von Vertrauensbeziehungen (Trusts) mit anderen *Domänen* und die Nutzung anderswo definierten *Credentials* und *Attributen* werden *föderierte* Konzepte verwendet. — Vision-9
- Soweit vom Trust-Level her möglich, können bestehende *E-Identities* , *Credentials* und *Attribute* von anderen Stellen übernommen werden (Föderation). — Vision-10

4.2 Ressourcenbezogene Anforderungen

Dieser Abschnitt beschreibt die von den *Ressourcen* gestellten, allgemeinen Anforderungen.

- Der Missbrauch von *Ressourcen* ist nicht möglich. Res-1
- Der *Zugriff* auf *Ressourcen* wird nur autorisierten *Subjekten* gestattet. Falls das *Subjekt* keine Rechte für die aufzurufende *Ressource* hat, wird der Aufruf nicht an die *E-Ressource* weitergeleitet. Res-2
- Der Aufwand für die Verwaltung der *E-Ressourcen* ist minimal. Res-3
- Der Aufwand für die Verwaltung der *Berechtigungen* (*Zugangsregeln* und *Zugriffsrechte*) ist minimal. Res-4
- Der Aufwand für die Administration der *E-Identities* (*Credentials* und *Attribute*) ist minimal. Res-5
- Bestätigungen werden durch *Attribute Assertion Services* unterschiedlicher Qualität ausgestellt. [SOWISCH] Res-6
- Für natürliche Personen und *Organisationen* gibt es einen eineindeutigen staatlichen *Identifikator*. [SOWISCH] Res-7
- Die Einhaltung der rechtlichen, organisatorischen und technischen Vorgaben (insbesondere Datenschutz sowie alle organisationsspezifischen Sicherheitsvorgaben) ist zu jeder Zeit gewährleistet. Res-8
  - Die Nachvollziehbarkeit und Nachweisbarkeit, welches *Subjekt* wann auf welche *Ressource* zugegriffen hat, ist gewährleistet. Res-8.1
  - Der Zusammenhang zwischen der *E-Identity* und den dazugehörigen *Credentials* muss zu jedem Zeitpunkt gewährleistet sein. Res-8.2
- Das *Subjekt* muss den Verdacht eines Missbrauchs seiner *E-Identity* melden. [SOWISCH] Res-9

4.3 Subjektbezogene Anforderungen

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

- Das *Subjekt* kann unabhängig vom Standort weltweit auf die *Ressourcen* zugreifen. Sub-1
- Das *Subjekt authentisiert* sich nur dort, wo es notwendig ist. Sub-2
- Falls die *Ressource* nicht wissen muss, wer auf sie zugreift, wird ein pseudonymisierter *Identifikator* übermittelt. Sub-3
- Die Menge der *Attribute*, die zur *Berechtigung* des *Subjekts* notwendig sind, ist minimal. Sub-4
- Es werden *Attribute* von unterschiedlichen *Attribute Services* akzeptiert. Sub-5
- Das *Subjekt* benötigt nur eine geringe Anzahl von *E-Identities* . Sub-6

- Das *Subjekt* kann wählen, wie viele *Credentials* es von welcher Qualität haben will. Sub-7
- Das *Subjekt* kann bei der *Authentisierung* auswählen, welches *Credential* es von der minimal geforderten Qualität der *Authentifizierung* verwendet. Sub-8
- Die Beschaffung von *E-Identities* und *Credentials* ist einfach und günstig. Sub-9
- Die Benutzung von *E-Identities* und *Credentials* ist einfach und unkompliziert. Sub-10
- Ein anderes *Subjekt* kann als Stellvertreter des *Subjekts* handeln. Sub-11
- Niemand kann auf die *Attribute* einer *E-Identity* zugreifen, ausser das *Subjekt* erteilt dazu explizit die Genehmigung oder das Recht ist gesetzlich verankert. Sub-12
- Das *Subjekt* erhält Unterstützung bei Vermeidung und Recovery des Missbrauchs einer *E-Identity*. [SOWISCH] Sub-13
- *IAM-Dienstanbieter* unternehmen das vernünftig Machbare, um den Missbrauch der *E-Identity* des *Subjekts* zu verhindern. [SOWISCH] Sub-14

4.4 Allgemeine Designprinzipien

Die nachstehenden Designprinzipien unterstützen die Umsetzung der oben aufgeführten Vision und Anforderungen.

- Für die *Authentifikation* und den *Zugang* nutzen *Ressourcen* von ihr entkoppelte Dienste. Design-1
- Die *Authentifikation* und *Berechtigung* für den *Zugang* basieren auf standardisierten *Credentials* und *Attributen*. Design-2
- Der *Autorisierung* für einen *Zugriff* auf eine *Ressource* muss (sofern fachlich nötig) die *Authentifikation* des zugreifenden *Subjekts* vorausgehen. Design-3
- Wenn fachlich nicht notwendig, werden keine Informationen zum zugreifenden *Subjekt* an die *Ressource* weitergegeben. Design-4
- Der *Zugang* wird auf Grund der angegebenen *Attribute* gewährt. Design-5

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. **Fehler! Verweisquelle konnte nicht gefunden werden.** zeigt das Informationsmodell zum organisationsübergreifenden IAM.

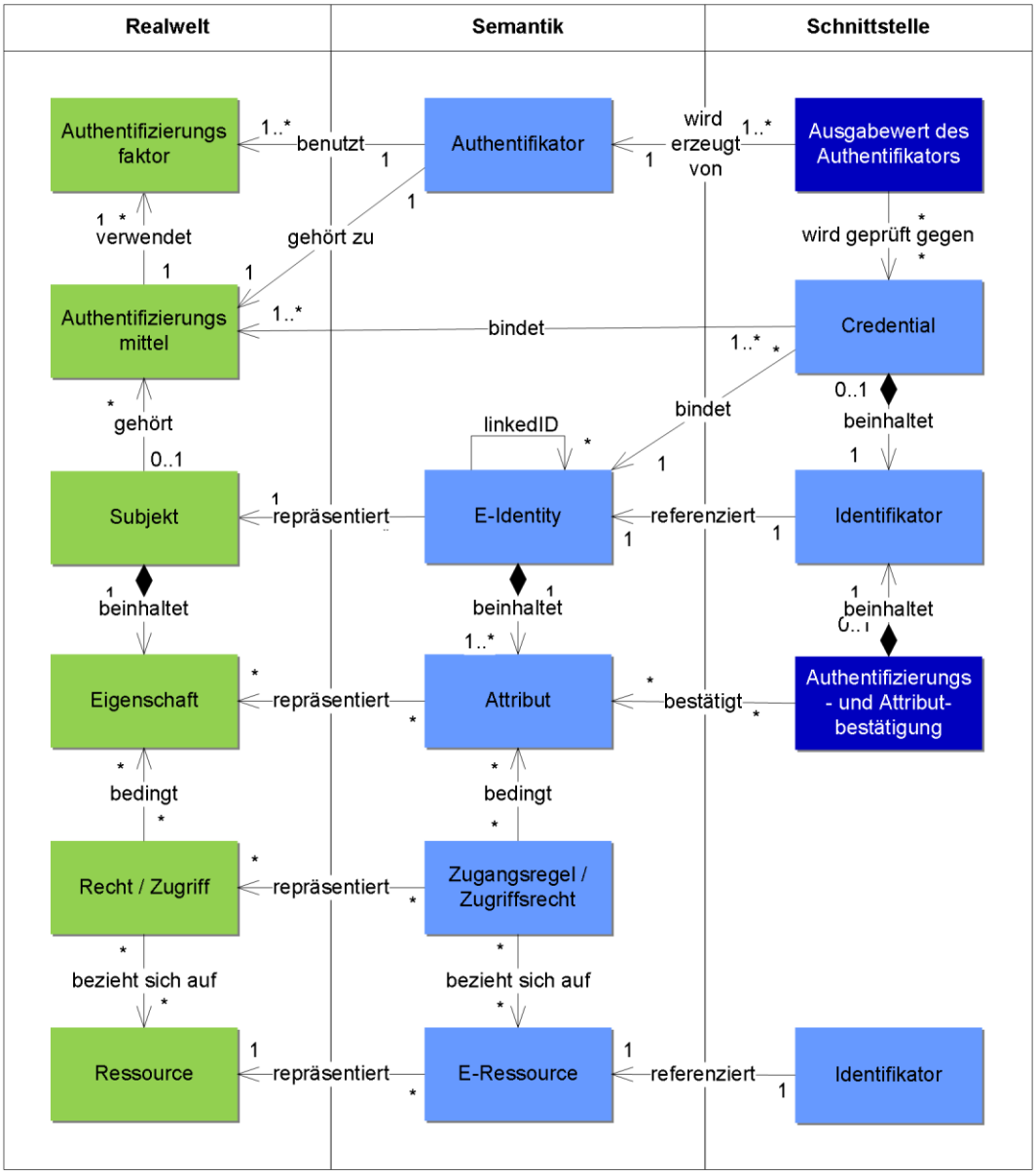


Abbildung 5 Informationsmodell

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 **Fehler! Verweisquelle konnte nicht gefunden werden.** zeigt links (in grün) die Elemente der realen Welt, in der Mitte das semantische Modell (der Informationssysteme), und rechts die Schnittellenobjekte, die zum Informationsaustausch zwischen Informationssystemen verwendet werden. Objekte, die zur Definitionszeit entstehen, sind entspr. der Farbverwendung aus Tabelle 1 hellblau dargestellt, Objekte der Laufzeit in dunkelblau.

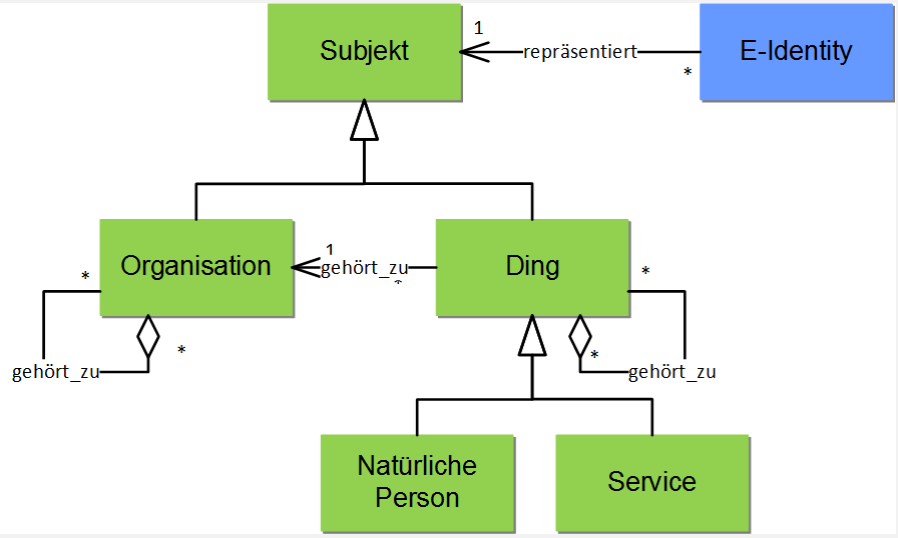
Das semantische Modell in der Mitte macht keine Aussagen über die Verteilung der Information über Informationssysteme.

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

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

Die nachfolgende Tabelle beschreibt die in der **Fehler! Verweisquelle konnte nicht gefunden werden.** 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*.

Subjekt	 **Abbildung 6 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* 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 oder ein biometrisches Merkmal). 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.[1]
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.
Schnittstelle	

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

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.[2]
Credential	Menge von Daten dar, mit der eine *E-Identity* an ein *Authentifizierungsmittel* gebunden wird, welches vom *Subjekt* besitzt 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 3 Beschreibung der Elemente des Informationsmodels

6 Prozesse

Abbildung 7 zeigt eine Übersicht über die Geschäftsprozesse. Sie dient zur Veranschaulichung der Top-Down-Tätigkeiten, welche für eine erfolgreiche Kooperation zwischen den Stakeholdern notwendig sind. Die Abbildung 7 übernimmt die Prozesse aus der Abbildung 1 und ergänzt deren Teilprozesse.

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

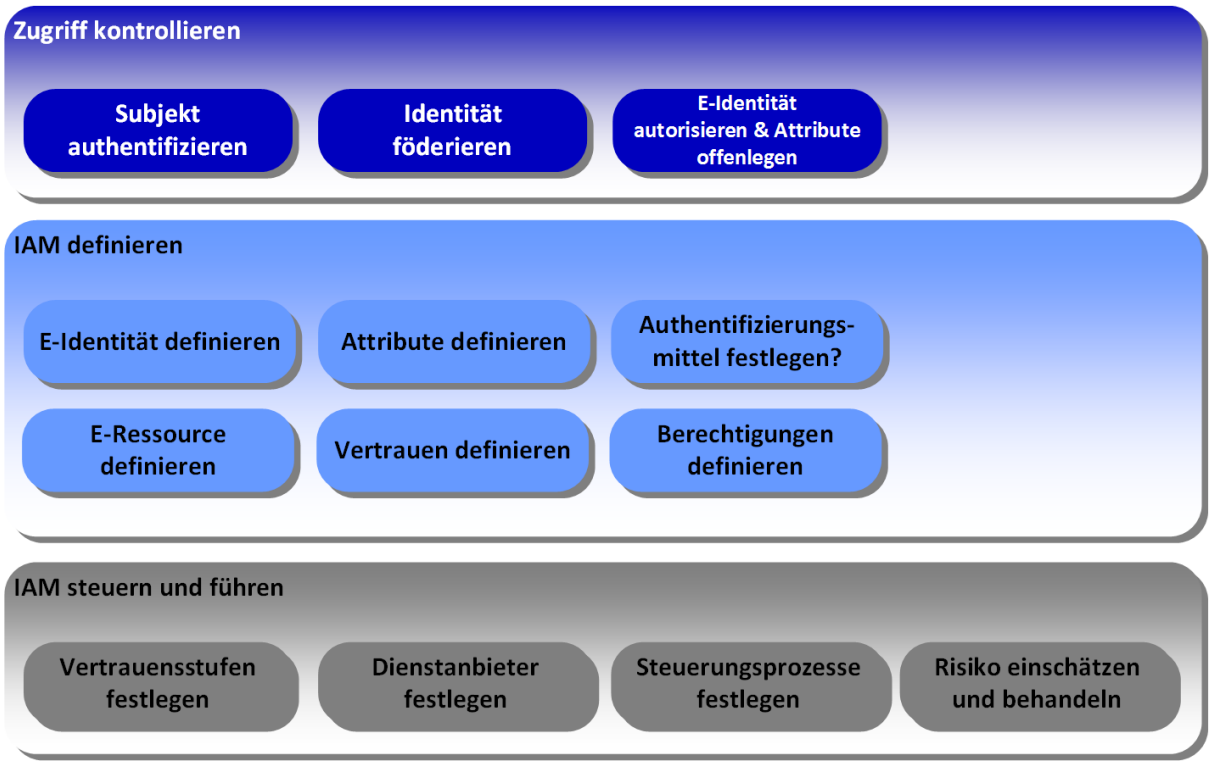


Abbildung 7 IAM-Prozesslandkarte

An diesen Prozessen beteiligen sich die verschiedenen Stakeholder 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 (optional)

Identität föderieren	Übergabe einer Authentifizierungs- und/oder Attributbestätigung vom IdP an die RP

Tätigkeiten:

- Der IdP überprüft, ob die RP berechtigt ist, eine Authentifizierungsbestätigung anzufordern.
- (optional) Attributaggregation: Falls der IdP gleichzeitig eine Attribut-Authorität ist, werden die angefragte Attribute vom IdP geliefert. Falls der IdP keine Attribut-Authorität ist, können die angefragte Attribute von einer oder mehreren Attribut-Authoritäten aggregiert werden.
- (optional) IdP holt das Einverständnis des Subjekts ein, die Authentifizierungs- und/oder Attributbestätigung 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 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 IdP 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 *Zugangsregeln* und *Zugriffsrechte* für den *Zugriff* auf die *E-Ressource* werden ermittelt und daraus die benötigten *Attribute* zur *E-Identity* abgeleitet.
- Die *Attribute* werden (üblicherweise benutzer-zentriert) bestätigt.
- Der *Zugang* und der *Zugriff* werden erlaubt.
- Der *Zugriff* erfolgt.
- Eine RP kann zusätzlich Attribute des Subjekts anfordern, wenn sie diese zur Erfüllung ihrer Funktion benötigt.

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 Credential 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 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*.

6.2.5 Vertrauen definieren

Vertrauen definieren	Erstellen, Pflegen und Löschen von vertrauenswürdigen *IAM-Dienstanbietern*

Tätigkeiten:

- Pflege der *Metadaten* zu den *IAM-Dienstanbietern.*
- Definition der Attribute.
- Festlegen der Vertrauensstufen für Authentifizierung und Attribute.

- Definieren und Widerrufen der Vertrauensbeziehungen (*Trust*) zwischen Stakeholdern, die im *föderierten* System Aufgaben wahrnehmen, z.B. von *Authentifizierungsbestätigung*, *Attributsbestätitgung* oder *Zugang* Services.
- Festlegen der Vertrauensanker über die Auswahl der Certificate Authority (CA).

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

In den Geschäftsprozess *IAM steuern und führen* gehören die Prozesse Governance, Risk und Compliance (GRC), welche zur Steuerung des *IAM* im E-Government dienen.

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 Governance

Governance definiert die *IAM*-Infrastruktur und die *IAM*-Organisation. Governance umfasst:

- Festlegung der *IAM*-Policy: Die *IAM*-Policy (inkl. *IAM*-Strategie, *IAM*-Architektur und *IAM*-Steuerungsprozesse) definiert die Randbedingungen und den Scope für die angestrebte *IAM*-Lösung. Wichtig sind insbesondere die Definition der Nachvollziehbarkeit der gesamten Prozessabläufe (z.B. das Ablegen der relevanten Dokumente) und deren Audit.
- 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.
- 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.

- Definition der *Rollen* mit Aufgaben, Kompetenzen und Verantwortung. Die Prozesse werden durch die Stakeholder ausgeführt. Diese haben eine (eventuell aber auch mehrere) *Rollen*.

6.3.2 Risk

Risk definiert die Abläufe zur Risikobehandlung (Risikoeinschätzung und -adressierung) für IAM-Prozesse. Risk umfasst:

- 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 Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001.
- (optional) Abstützung des Risikomanagements auf ein Framework wie COBIT.

6.3.3 Compliance

Compliance sorgt für die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen. Compliance wird erreicht durch:

- Erarbeiten und Aktualisieren der relevanten Vorgaben: Identifikation der geltenden Richtlinien / Regularien. Ebenfalls werden Veränderungen in den Vorgaben verfolgt und allfällige daraus resultierende Massnahmen identifiziert.
- Reporting aller relevanten Aktivitäten
- 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.

7 Geschäftsservices

Nachfolgend werden alle *IAM*-Services, welche von den verschiedenen Stakeholdern (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.

Aufgaben (zur Laufzeit):

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

7.2 Services zur Definitionszeit

In Abbildung 8 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*.

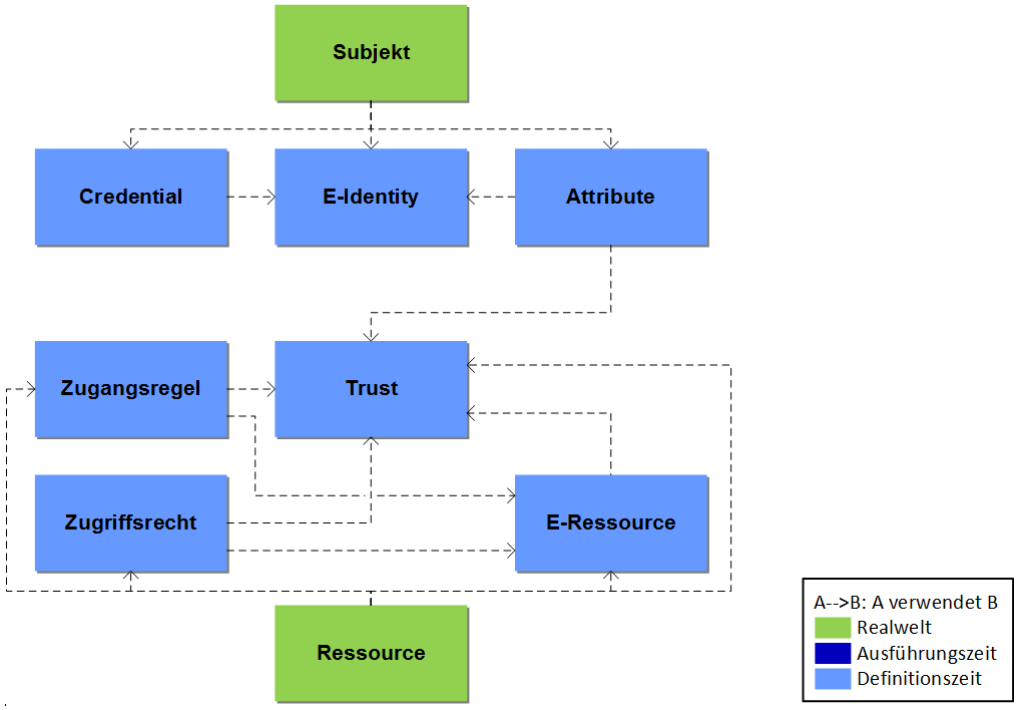


Abbildung 8 Geschäftsservices – Definitionszeit

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

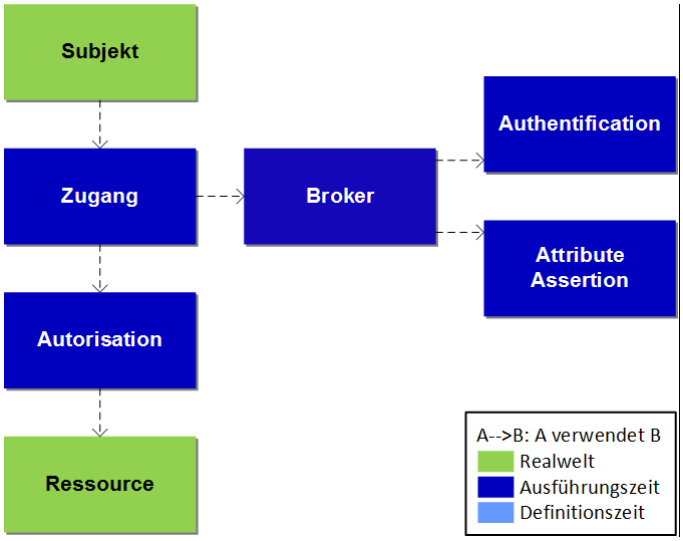


Abbildung 9 Geschäftsservices – Laufzeit

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:[3]

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

[3] 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) 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), 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*
- 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.
- (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 10 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.

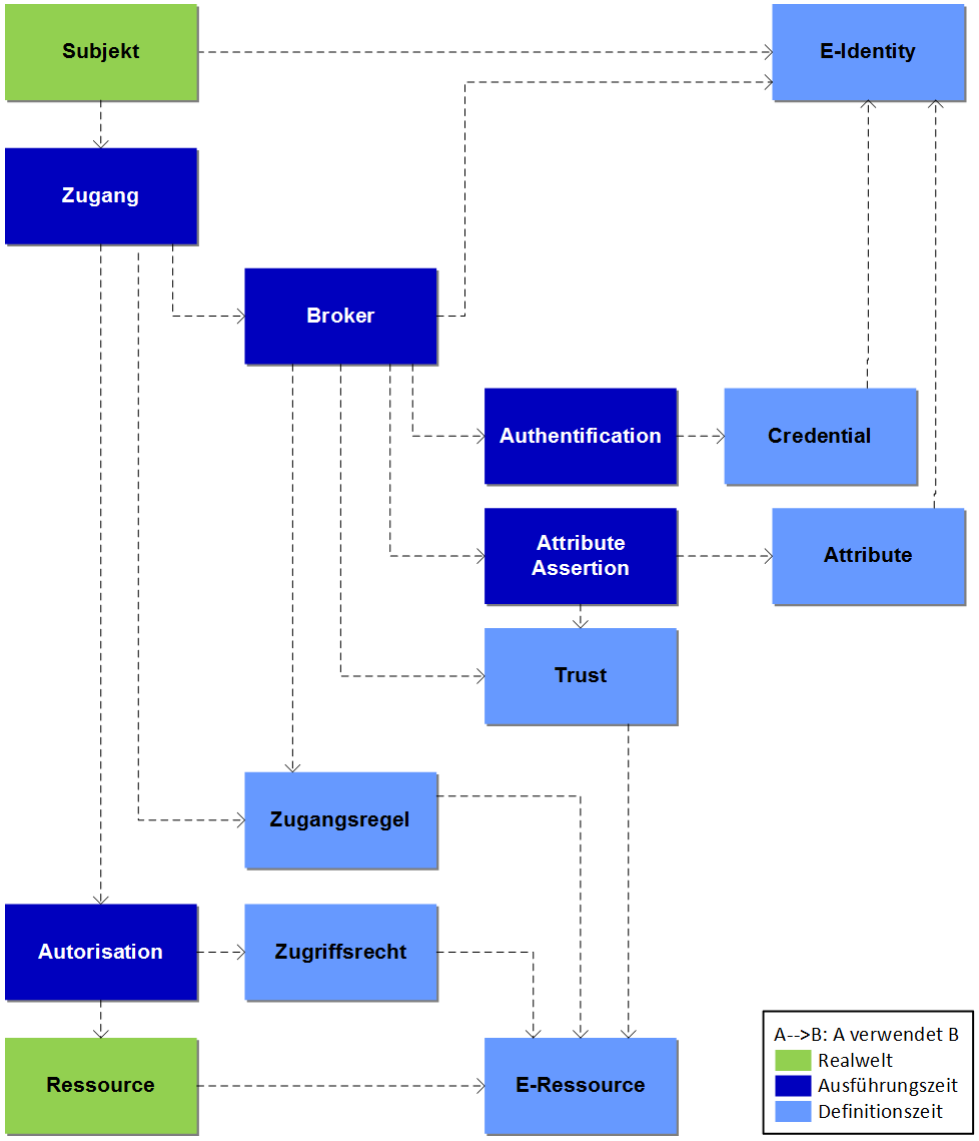


Abbildung 10 Geschäftsservices – Übersicht

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 8 und in den Services bereits direkt angesprochen. Diese werden deshalb hier nicht dargestellt.

7.5.1 Subjekt authentifizieren

Abbildung 11 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *Subjekt authentifizieren*.

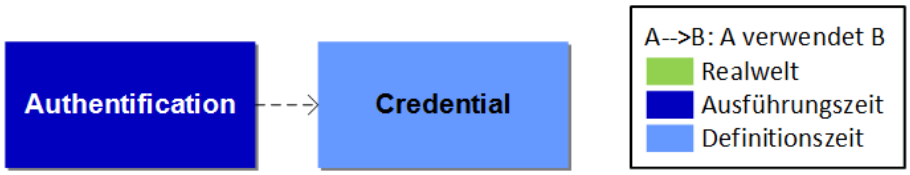


Abbildung 11 Prozessunterstützung *Subjekt authentifizieren*

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

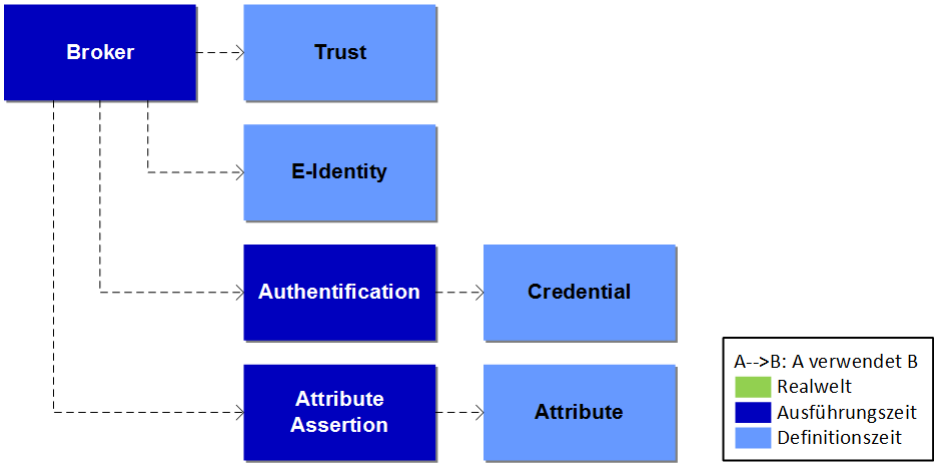


Abbildung 12 Prozessunterstützung *Identität föderieren*

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

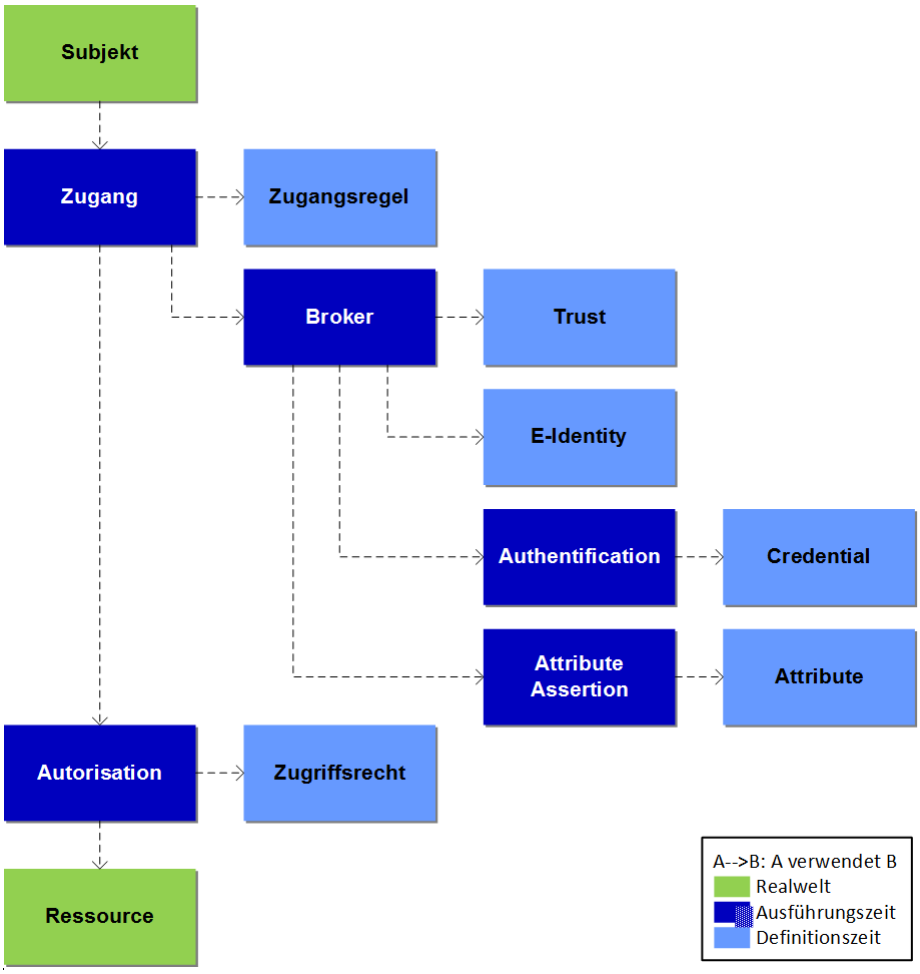


Abbildung 13 Prozessunterstützung *E-Identity autorisieren und Attribute offenlegen*

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[4]	Attribut[5]	Zugangsregel	Zugriffsrecht	E-Ressource	Credential	Identifikator einer E-Identity	Ausgabewert des Authentikator	Authentifizierungs-bestätigung	Attributbestätigung	Identifikator einer E-Ressource
Geschäftsservice	E-Identity	B	B[6]					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[7]	LB[7]	
	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 4 Beziehung zwischen Services und Semantik des Informationsmodells

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

7.7 Zuständigkeiten für Geschäftsservices

Tabelle 5 zeigt auf, welcher Stakeholder idealtypisch welchen IAM-Service zur Definitions- und Laufzeit anbietet. Diese Geschäftsservices sind in Kapitel 7 näher beschrieben. Die hier vorgeschlagene Aufteilung optimiert bezüglich Wiederverwendung der Services in einer *Identity Federation*. Die *Relying Party* gibt deshalb möglichst viel Betriebsverantwortung an *IAM*-Dienstanbieter.

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

Tabelle 5 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[8].
- 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.

[8] 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
Integrieriertes 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 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.

10 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

[CAS]	SECO. Claim Assertion Service Technical Specification. Version 0.98.05, 19.1.2011. http://www.suissecas.org/media/CAS_Specification_0.98.05.pdf
[ISBRefM]	eCH Fachgruppe IAM. Identity & Access Management IAM – Referenzmodell IAM. White Paper. Version 1.1d, 16.3.2011. http://www.isb.admin.ch/themen/architektur/00183/01368/01371/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCEeHt5g2ym162epYbg2c_JjKbNoKSn6A--&t=.pdf
[OASIS]	http://docs.oasis-open.org
[SAML 2.0 TechOverview]	OASIS. Security Assertion Markup Language (SAML) V2.0 Technical Overview. Committee Draft 02, 25.3.2008. http://www.oasis-open.org/committees/download.php/27819/sstcsaml-tech-overview-2.0-cd-02.pdf
[SAML Glossar]	OASIS. Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0. 15.3.2005. https://www.oasis-open.org/committees/download.php/21111/saml-glossary-2.0-os.html
[SOWISCH]	Protokoll Expertenworkshop “Sicherheitsopportunitäten für den Wirtschaftsstandort Schweiz” vom 8.11.2012 (zu Strategie Informationsgesellschaft)
[Stabi3]	eCH Fachgruppe IAM, E-Government Vorhaben B2.06. Stabi3eGov B2.06 IAM Lösungsarchitektur. Bericht. 4.1.2011. http://www.ech.ch/alfresco/guestDownload/attach/workspace/SpacesStore/f91f7628-2050-4889-bd69-f2b27b580e67/E-Gov%20B2.06_IAM-Loesungsarchitektur_V120_04.01.2011_d.pdf
[TOGAF]	http://www.opengroup.org/togaf/
[UML]	http://www.uml.org/

Anhang B – Mitarbeit & Überprüfung

Hassenstein Gerhard	Berner Fachhochschule, TI
Thomas Kessler	Temet
Kunz Marc	Berner Fachhochschule, TI
Laube-Rosenpflanzer Annett	Berner Fachhochschule
Spichiger Andreas	Berner Fachhochschule
	eCH Fachgruppe IAM

Anhang C – Abkürzungen

AA	Attribute Authority
CAS	Attribute Assertion Service
CP	Credential Provider
IAM	Identity und Access Management
IdP	Identity Provider
OASIS	Advancing open standards for the information society
RP	Relying Party
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SSO	Single Sign-On
Stabi3	Stabilisierungspaket
TOGAF	The Open Group Architecture Framework
UML	Unified Modelling Language [UML]
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Anhang D – Glossar

Im Kontext dieses Standards bedeuten:

ABAC	Attribute Based Access Control Bei der attibutbasierten *Zugriffskontrolle* wird den Benutzern auf Grund ihrer *Attribute* dynamisch Zugang/*Zugriff* zu den *Ressourcen* gewährt. vgl. *RBAC*
Access	Siehe *Zugriff*
Access Control	Siehe *Zugriffskontrolle*
Access Service	siehe *Zugang* Service
Access Service Provider	*Entität*, welche den gesamten Vorgang der *Authentisierung* und *Autorisierung* durchführt und die endgültige Entscheidung über den *Zugriff* auf Basis der zur Verfügung gestellten *Credentials* usw. trifft. Der *Access Service*-Provider stellt auch jene Daten zur Verfügung, die für Accounting, Billing und nutzungsbasierte Lizensierung benötigt werden.
Akteur	Ein *Akteur* abstrahiert von realen Benutzern eines Informationssystems. Er steht für eine Rolle, die ein realer Benutzer im Rahmen eines Geschäfts gegenüber dem Informationssystem einnimmt.
Assertion	Siehe *Authentication Assertion* oder *Attribute Assertion*
Attribut / Attribute	Semantisches Abbild einer einem *Subjekt* zugeordneten *Eigenschaft*, die das *Subjekt* näher beschreibt. Der *Identifikator* und die *Credentials* sind ebenfalls *Attribute*. Ein Attribut setzt sich zusammen aus den Meta-Attributen Attributname (z.B. „Schuhgrösse“), Attributtyp (z.B. „Integer“) und Attributwert (z.B. „39“). Im Stellvertretungsfall besitzt die *E-Identity* des Stellvertreters für eine gewisse Zeit eine Menge von *Attribute* der *E-Identity* des vertretenen *Subjekts*.
Attribut-Autorität (AA)	Eine *Attribut-Autorität* ist ein *Register* oder sonstiges *Verzeichnis* mit einem *Attribute Service* zur Pflege von *Attributen* und einem *Attribute Assertion Service* zur Ausstellung von *Attribute Assertions*.
Attributbestätigung	Siehe *Attribute Assertion.*
Attribute Assertion	Bestätigung eines *Attributs* durch eine *Attribute Authority*. Entspricht einer SAML 2.0 Attribute Assertion [SAML 2.0 TechOverview].
Attribute Assertion Service	Siehe *Attribute Authority*.

Attribute Authority	Eine technische *Entität* (Service), die *Attribute Assertions* über eine definierte Schnittstelle ausstellt. [SAMLGlossar]. Synonym: Attribute Assertion Service
Attribute Management	Prozesse zur Definition, Verwaltung und Nutzung von *Attributen*.
Attribute Service	Der *Attribute* Service pflegt zeitaktuell ein oder mehrere *Attribute* für definierte *Subjekte*. Siehe auch *Attribute Management*.
Auditing	a) Überprüfung der *Policy*-Konformität b) Aufzeichnung aller Aktionen und Entscheide zur Gewährleistung der Nachvollziehbarkeit
Authentication Assertion	Eine Bestätigung der erfolgreichen *Authentifikation* eines *Subjektes*. [SAML Glossar]
Authentication Authority	Eine technische *Entität* (Service), die *Authentifikation* als Dienstleistung anbietet und *Authentication Assertions* für *Subjekte* ausstellt. [SAMLGlossar]
Authentication Service	Der *Authentication* Service überprüft mittels der *Credentials*, ob der Zugreifende (*Subjekt*) der ist, der er behauptet zu sein. siehe auch *Authentication Authority*.
Authentifikation	Vorgang der Überprüfung einer behaupteten *E-Identity.* Synonyme: *Authentifizierung*.
Authentifikation-Autorität (AuthnA)	Eine *AuthnA* stellt einen *Authentication* Service zur Verfügung, gegen den sich das *Subjekt* authentifizieren kann. Der *Authentication* Service benutzt *Credentials*, die von einem *Credential* Service ausgestellt werden. Der *Credential* Service kann ein Bestandteil der *AuthnA* sein. Beispiele für *Authentifikation-Autoritäten* sind *IdPs* (nach *SAML*), OpenID Provider und MobilID Provider.
Authentifizierung	Siehe *Authentifikation.*
Authentifizierungs-Anfrage	Eine Authentifizierungs-Anfrage wird vom Subjekt an den Authentication Service gesendet. Dieser initialisiert die Überprüfung der behaupteten E-Identity.
Authentifizierungsbestätigung	Siehe *Authentication Assertion.*
Authentisierung	Nachweis der eigenen *E-Identity* eines *Subjekts*.[9]

[9] Die Begriffe *Authentisierung* und *Authentifikation* werden oft verwendet, als wären sie Synonyme.

Authentifizierungs-merkmal	Das *Authentifizierungsmerkmal* kann auf Wissen (Passwort, PIN), auf Besitz (Zertifikat, privater Schlüssel) oder auf einer *Eigenschaft* (biometrisches Merkmal z.B. Stimme, Irisbild, Fingerabdruck) oder auf einer Kombination dieser Merkmale basieren.
Authorization Provider	*Entität*, die *Autorisierung* als Dienstleistung anbietet.
Authorization Service	Der Service überprüft zur Ausführungszeit die Einhaltung der Rechte für die Nutzung der *E-Ressource* und erlaubt dem *Subjekt* die Nutzung, wenn es die entsprechenden Rechte besitzt.
Autorisierung	a) Administration: Definition der *Zugangsregeln* und *Zugriffsrechte* auf eine *E-Ressource*. b) Zur Laufzeit: Prüfen von Zugriffsberechtigung eines authentifizierten *Subjektes* auf eine *Ressource* und erteilen des *Zugriffs* zur Laufzeit. Dabei wird zwischen *Grob-* und *Feinautorisierung* unterschieden.
Benutzer	Menschliches *Subjekt*.
Berechtigung	Recht eines *Subjekts*, bestimmte *Ressourcen* zu nutzen.
Broker Service	Dieser Service vermittelt zwischen dem *Subjekt*, *Ressourcen* und den Services der Ausführungszeit
Certification Authority (CA)	Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt. Synonym: *Certification Service Providers* (*CSP*)
Certification Service Providers (CSP)	Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt. Synonym: *Certification Authority* (CA)
Claim	Der Begriff *Claim* wurde in diesem Dokument explizit nicht verwendet, da verschiedene, einander z.T. widersprechende Bedeutungen existieren. Es wird empfohlen, den Begriff deshalb zu vermeiden. siehe *Attribute Assertion*
Claim Assertion Service (CAS)	Der *Claim Assertion Service* ist ein spezielle *Attribute Authority*. Seine Aufgabe besteht darin, dem Benutzer zu erlauben, Eigenschaften, welche ihm von einer Organisation oder Register zugeteilt wurden, zu bestätigen. [CAS]
Credential	Nachweis zur Bestätigung einer *E-Identity* eines *Subjekts*. Im IAM-Kontext wird zur Bestätigung einer *E-Identity* eine Benutzerkennung (*Identifikator*) in Verbindung mit einem mit einem (oder mehreren) *Authentifizierungsmerkmal*(en) verwendet. Synonym: Identitätsnachweis
Credential Management	Prozesse zum Erstellen und zur Vergabe von *Credentials.*

Credential Service	Der *Credential* Service gibt *Credentials* aus und verwaltet sie. Die *Credentials* können von unterschiedlichem Typ sein. Ein Credential bezieht sich auf eine *E-Identity* und ist auf ein bestimmtes *Subjekt* ausgestellt.
Credential Service Provider	*Entität*, die als vertrauenswürdiger Herausgeber von elektronischen Zertifikaten oder anderen Sicherheits-Tokens (*Credentials*) agiert.
Digitale Identität / Digital Identity	Siehe *E-Identity*.
Digitales Zertifikat / Digital Certificate	Strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen (auch Zertifikat oder Public-Key-Zertifikat).
Domäne	Administrative / technische Gemeinschaft oder Organisation mit einer gemeinsamen *Policy.*
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 eindeutig einem *Subjekt* zugewiesen werden können. Ein *Subjekt* kann mehrere *E-Identities* haben.
E-Identity Service	Der *E-Identity* Service stellt zu *Subjekten E-Identities* aus und verwaltet sie.
Elektronische Identität / Electronic Identity	Siehe *E-Identity*
Entität / Entity	Ein aktives Element eines IT Systems, z.B. ein automatisierter Prozess oder eine Menge von Prozessen, ein Teilsystem, eine Person oder eine Gruppe von Personen mit definierten Funktionalitäten. [SAML-Glossar]
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. Eine *Ressource* kann mehrere *E-Ressourcen* haben.
E-Ressource Service	Der *E-Ressource* Service stellt zu *Ressourcen E-Ressourcen* aus und verwaltet sie.
Föderiertes Identitätsmanagement / Federated Identity Management (FIdM)	Föderiertes Identitätsmanagement erlaubt die übergreifende Verwendung von *E-Identities* in normalerweise geschlossenen Domänen. FIdM erlaubt den Benutzern einer *Domäne* den einfachen und sicheren Zugang zu den Systemen einer anderen *Domäne*, ohne eine redundante Benutzerverwaltung aufzubauen.
Feinautorisierung	Gewährung bzw. Verweigerung des *Zugriffs* auf einzelne von einer *Ressource* bereitgestellten Funktionen oder Daten.

Föderation / Federation	Zusammenarbeit über Organisations- und Systemgrenzen hinweg, ohne Duplikation oder Replikation der dazu notwendigen Benutzerdaten (*E-Identities*)
Funktion	Eigenschaft, die einem *Subjekt* bestimmte Aufgaben, Kompetenzen und Verantwortung innerhalb einer Organisation zuweist. Ein *Subjekt* kann mehrere Funktionen haben (vgl. Rolle).
Grobautorisierung	Gewährung bzw. Verweigerung des Zugangs zu einer Ressource.
IAM-Dienstanbieter	Der *IAM-Dienstanbieter* ist Betreiber von einem oder mehreren IAM-Geschäftsservices gemäss Kapitel 0.
Identifikator	Eine Zeichenkette, welche ein *E-Identity* oder eine *E-Ressource* innerhalb eines *Namensraumes* eindeutig bezeichnet. Der Identifikator einer Ressource ist oft eine URL/URI.
Identität / Identity	Identität ist die Gesamtheit der ein *Subjekt* kennzeichnenden und als Individuum von allen anderen unterscheidenden Eigentümlichkeiten. Im IAM-Kontext wird hauptsächlich die *E-Identity* eines *Subjekts* verwendet (siehe *E-Identity*).
Identity Provider (IdP)	*Entität*, die *E-Identity* verwaltet und herausgibt. Ein IdP stellt einen *Authentication Service* und meist auch einen *Attribute Assertion Service* zur Verfügung.
Juristische Person	Siehe Organisation
Identitäts- und Zugriffsverwaltung / Identity und Access Management (IAM)	Alle Prozesse und Systeme um Subjekten den Zugriff auf die Ressourcen zu ermöglichen, die diese auf Grund ihrer Funktion in der Organisation benötigen.
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*).
Metadaten	Ein Mittel, um Vertrauen und technische Interoperabilität zwischen *SAML* Komponenten (*Entitäten*) zu ermöglichen. Können auch verwendet werden, um Attributinformationen auszutauschen.
Meta-Domäne	*Domäne*, welche die Zusammenarbeit zwischen zwei oder mehreren *Domänen* regelt.
Namensraum	Anwendungsbereich (z.B. ein Unternehmen, ein Staat, eine Fachgemeinschaft, eine Sprachgemeinschaft), für welchen die Bedeutung einer Zeichenkette (z.B. *Identifikator*) definiert ist.

Organisation	Organisatorische Einheit bestehend aus mehreren *Subjekten* (Juristische Person, Unternehmen, Verein, Amtsstelle, Gruppe von Subjekten, …). vgl. *Subjekt* und Abbildung 14.
Policy	Schriftlich festgehaltene Regelungen und Vorschriften, welche einzuhalten sind.
RBAC	Role Based Access Control Bei der rollenbasierten Zugriffskontrolle werden Benutzern oder Gruppen von Benutzern eine oder mehrere *Rollen* zugeordnet. Eine *Rolle* enthält eine Menge von Berechtigungen (Permissions), die die erlaubten Operationen auf einer *Ressource* beschreiben. vgl. ABAC
Register	Verzeichnisse in der Verwaltungssprache, wie z.B. die Einwohnerregister, Anwaltsregister, Zivilstandsregister, Handelsregister etc. Sie werden in der Regel von offiziellen Stellen (Behörden) geführt.
Registrierung / Registration	Prozess einer Registrierungsstelle, bei dem ein *Subjekt* eine *E-Identity* mit dazugehörigem *Credential* erlangt.
Relying Party (RP)	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*.
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.
Ressourcenverantwortlicher	Verantwortliche Stelle für die von der *Relying Party* verwalteten *Ressourcen* (z.B.: Anwendungsverantwortlicher, Serviceverantwortlicher, Dateninhaber).
Rolle / Role	a) *Subjekt*: Bestimmte Anzahl von Funktionen, die von einem *Subjekt* ausgeführt werden. Einem *Subjekt* können eine oder mehrere *Rollen* zugeteilt werden. b) *E-Identity*: *Attribute*, die die *Rolle*/*Funktionen* des *Subjekts* repräsentieren c) *Entität*: Aufgabe und Zweck einer *Entität* in einer *Föderation*. Einer *Entität* können eine oder mehrere *Stakeholder*rollen (siehe Kapitel 3) zugeteilt werden.

Security Assertion Markup Language (SAML)	SAML (Security Assertion Markup Language) wurde spezifiziert, um herstellerunabhängig Single Sign-On zu ermöglichen. SAML ist ein XML Framework, mit dessen Hilfe *Authentifizierungs-* und *Autorisierungsinformationen* ausgetauscht werden können. SAML wurde von einem internationalen Konsortium und im Rahmen der OASIS standardisiert. [OASIS]
Security Token	Ein Datenpaket, welches verwendet werden kann, um den Zugriff auf eine *Ressource* zu autorisieren.
Service Level Agreement (SLA)	Bezeichnet einen Vertrag zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen.
Subjekt	Eine natürliche Person, *Organisation* oder ein Service, die auf eine *Ressource* zugreift oder zugreifen möchte. Ein *Subjekt* wird durch *E-Identities* repräsentiert.

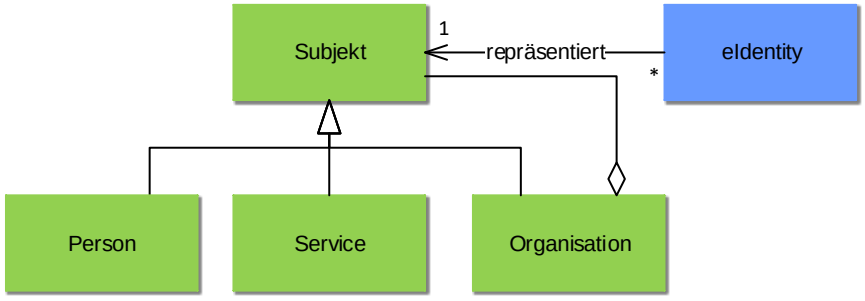


Abbildung 14 Definition Subjekt

Trust Service	Der *Trust* Service pflegt die akzeptierten, vertrauenswürdigen *IAM-Dienstanbieter*.
Trusted Third Party	Vertrauenswürdige Instanz, z.B. zur Verwaltung von öffentlichen Schlüsseln oder Zertifikaten.
Trust-Level	Zwischen den Beteiligten abgemachtes Vertrauensniveau, das Sicherheitsanforderungen für die Prozesse und die technologischen Komponenten festlegt.
Unternehmen	Siehe *Organisation*
User	Siehe *Benutzer*
Vermittlerinfrastruktur	Siehe *Broker* Service
Vertrauen	Formell meist im *SLA* definierte Vertrauensbeziehung zwischen verantwortlichen Stellen. z.B. die formelle Beschreibung der Kriterien, die erfüllt sein müssen, damit sich zwei *Organisationen*, *Entitäten*, *Domänen* etc. gegenseitig vertrauen (engl. Trust).
Verzeichnis	Systematische Sammlung von Informationen mit gemeinsamen Merkmalen.

Zugang Service	Der Service überprüft die Einhaltung der Zugangsregeln und erlaubt dem Subjekt den Zugang, wenn die entsprechenden Regeln erfüllt sind. Synonym: *Access* Service.
Zugangsregel	*Ressourcenverantwortliche* definieren die Zugangsregeln für ihre *E-Ressourcen*. Die *Zugangsregeln* definieren die Bedingungen, unter denen ein *Subjekt* Zugang zu einer *Ressource* erhält (Grobautorisierung), z.B. nach erfolgreicher *Authentifizierung* und Bestätigung bestimmter *Attribute*.
Zugangsregel Service	Der Service verwaltet die Regeln für den Zugang zu einer *Ressource*. Die Regeln sind auf der Basis von *Authentisierung* oder *Attributen* definiert.
Zugriff	Interaktion mit einer *Entität* um eine oder mehrere ihrer *Ressourcen* zu manipulieren und oder zu nutzen. [SAMLGlossar] Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe gespeichert.
Zugriffskontrolle	Überwachung und Steuerung des Zugriffs auf *Ressourcen*. Das Ziel ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen.
Zugriffsrecht	*Ressourcenverantwortliche* definieren die *Zugriffsrechte* für ihre *E-Ressourcen*. Die *Zugriffsrechte* definieren die Bedingungen unter denen ein Subjekt auf die verschiedenen Funktionalitäten einer *Ressource* nutzen darf (*Feinautorisierung*), z.B. nach erfolgreicher *Authentifizierung* und Bestätigung bestimmter *Attribute*.
Zugriffsrecht Service	Der 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.

Anhang E – Identity Federation Modelle

Sobald mehrere RPs und IdP/AAs im Spiel sind, spricht man von komplexen *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 15) 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/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.

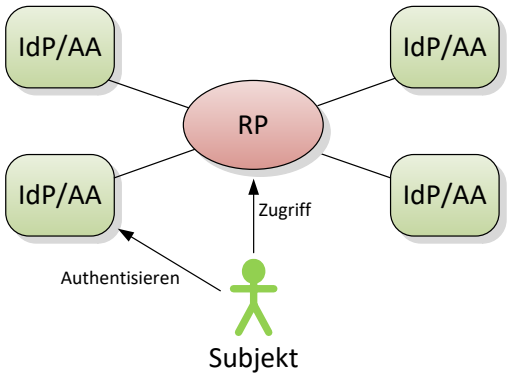


Abbildung 15 RP-zentriertes Modell

E.2 – IdP/AA-zentriertes Modell

Das *IdP/AA-zentrierte Modell* (vgl. Abbildung 16) wird eingesetzt, wenn mehrere *IAM*-Systeme auf eine einzige IdP/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.

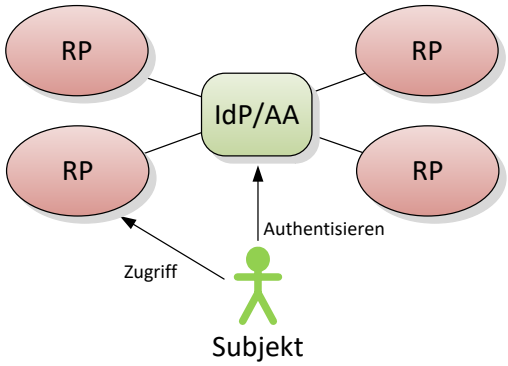


Abbildung 16 IdP/AA-zentriertes Modell

E.3 – Cross Domain Modell

In einem *Cross Domain Modell* kann jede Organisation sowohl *Identity Provider* wie auch *Relying Party* sein. Dies ist ein häufiges Szenario, wenn ein *IdP/AA-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 IdP/AA) wie auch von externen *Subjekten* verwendet werden können.

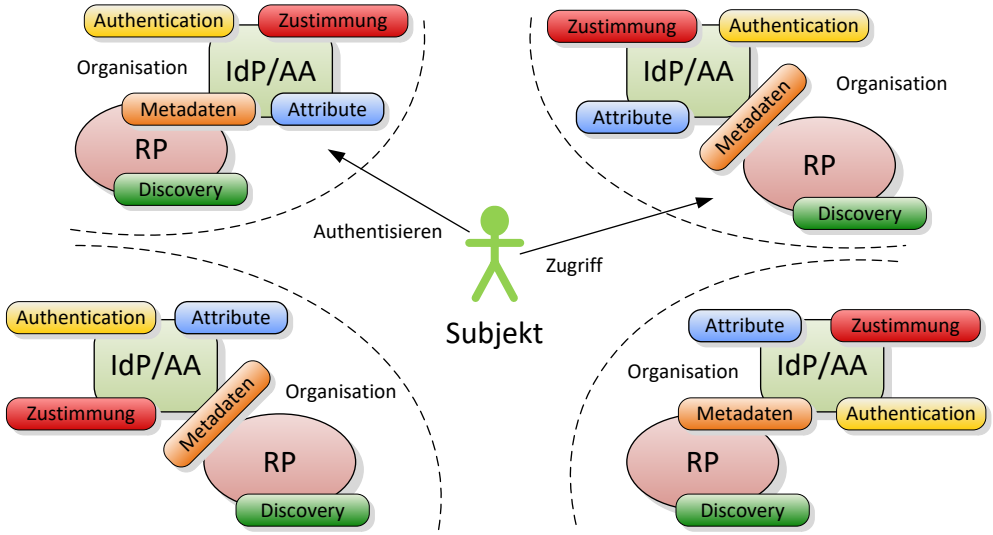


Abbildung 17 Cross Domain Modell

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 18 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).

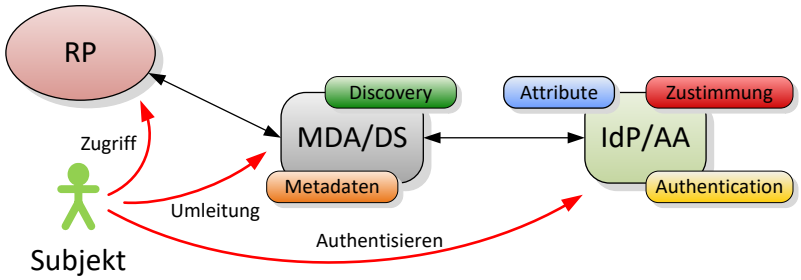


Abbildung 18 Zentralisierte Metadaten und Discovery Service

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[10] Modell basiert auf einem zentralen *Identity Hub*, welchem alle beteiligten Parteien mit ihren Diensten vertrauen. Wie in Abbildung 19 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 IdP/AA-Quellen zusammentragen und stellt diese zu einer aggregierten Antwort an die *Relying Party* zusammen.

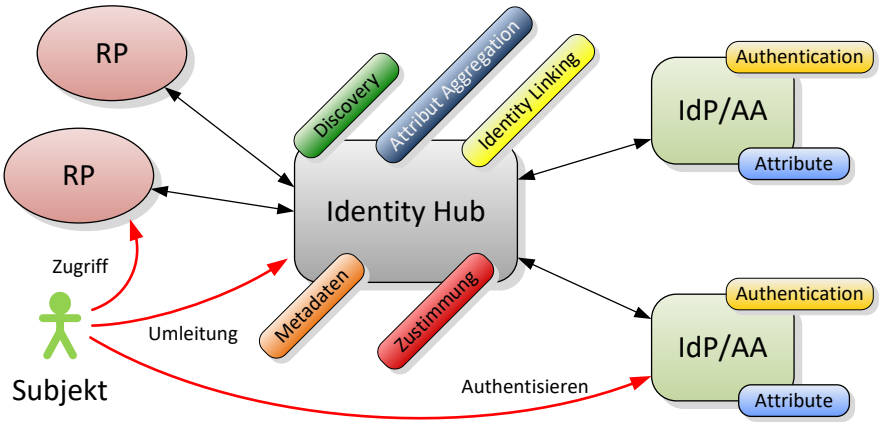


Abbildung 19 Hub-'n'-Spoke Modell

Das in Abbildung 19 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

[10] Nabe und Speiche

grösser ein Organisationsverbund in einer Identity Federation ist, umso mehr muss ein vertragliches Regelwerk die Richtlinien für die Beziehungen der einzelnen Parteien festlegen.

Anhang F – Änderungen gegenüber Version 2.00

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

So wurde eCH-0107 in der Version 2.0 in wesentlichen Teilen neu erarbeitet.

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

Grundsätzliches:

- *Der Aufbau der Kapitel wurde nicht grundsätzlich geändert, sondern die einzelnen Kapitel wurden überarbeitet.*
- *V2.0 beschränkt sich konsequent auf das behördenübergreifende IAM.*
- *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 (Ref ECH Nummer] ausgelagert. Im Dokument selbst werden nur die verwendeten Begriffe definiert (Anhang D – Glossar).*

Kapitel 2

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 Stakeholder [neu]

- *Die grundlegenden Stakeholder-Kategorien und deren Mapping zu den Geschäftsservices wurden neu erarbeitet.*

Kapitel 0

Anforderungen **[eCH-0107 v1.00 Kapitel 2]**

- *Die Architekturvisionen und allgemeinen Designprinzipien wurden neu eingeführt.*
- *Die Anforderungen wurden überarbeitet und durch neue Erkenntnisse ergänzt.*

0

Informationsarchitektur **[eCH-0107 v1.00 teilweise Kapitel 4]**

- *Das Informationsmodell wurde komplett überarbeitet.*
- Das Informationsmodell unterscheidet die Elemente der realen Welt, das semantische Modell und die Schnittstellenobjekte.

6 Prozesse [neu]

- *Die Prozesse wurden neu eingefügt(Basis Stabi 3 eGov).*

Geschäftsservices **[eCH-0107 v1.00 teilweise Kapitel 4]**

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

0

[neu]

- *Die Identity Federation Konzepte wurden neu aufgenommen und dokumentiert.*