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	2.0
Status	Genehmigt; ausser Kraft
Genehmigt am	2013-11-27
Ausgabedatum	2013-12-04
Ersetzt Version	1.00 (Best Practice)
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Beilagen	--
Autoren	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

Abbildungsverzeichnis

Tabellenverzeichnis

1 Status des Dokuments

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

2 Einleitung

2.1 Überblick

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

Internetbasierte Geschäftsprozesse setzen vertrauenswürdige Akteure 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.

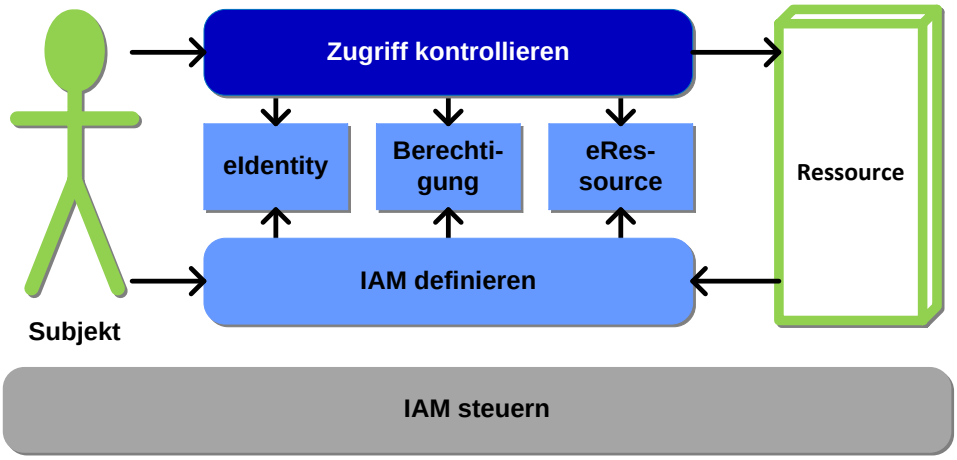

Abbildung 1 IAM im Überblick

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.
dunkelblau	Die dunkelblaue Farbe wird durchgehend für die Laufzeit verwendet. Zur Laufzeit wird der Zugriff basierend auf den definierten Informationselementen kontrolliert (gewährt oder abgelehnt).
hellgrün	Die hellgrüne Farbe wird in diesem Dokument konsequent für Realweltobjekte verwendet.

Tabelle 1 Farbverwendung im Dokument

Subjekt und *Ressource* sind Akteure (und 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 *eIdentity* (hellblau) und der *Ressource* (grün) die *eRessource* (hellblau) zugeordnet. Die *Ressource* legt zur Umsetzung ihrer Ziele im Informationselement Berechtigung (Zugangsregel/Zugriffsrecht) fest, welche *eIdentity* unter welchen Bedingungen auf welche *Ressource* zugreifen darf.

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

2.1.2 Föderiertes IAM

Im Unterschied zum organisationsinternen IAM geht das *föderierte IAM* von organisationsübergreifenden *eIdentities* aus. Die *eIdentity* für ein *Subjekt* wird in der *Domäne* A erstellt, kann aber auch Informationen in der *Domäne* B besitzen, die der *eIdentity* der *Domäne* A zugeordnet sind. Weiter ist es möglich, dass Subjekte mit der *eIdentity* 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.

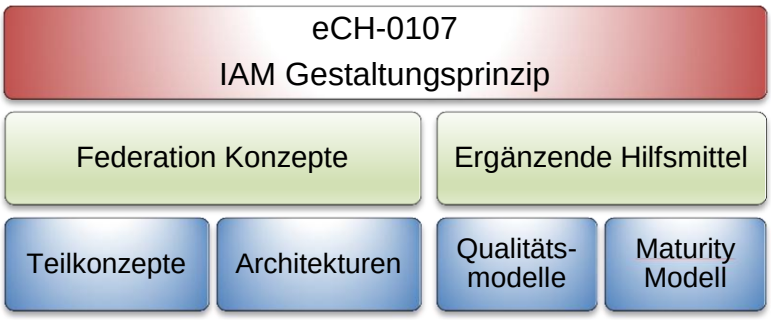

Abbildung 2 Einordung des eCH-0107 Standards

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 Akteure *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.

Kapitel 8 stellt die Varianten, ein föderiertes *IAM* aufzubauen, dar.

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.

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
8 Identity Federation Konzepte	Dieses Kapitel ist deskriptiv, soll aber zur Einordnung helfen.
Anhang A – Referenzen & Bibliografie	Deskriptiv
Anhang B – Mitarbeiter & Überprüfung	Deskriptiv
Anhang C – Abkürzungen	Normativ
Anhang D – Glossar	Normativ

Tabelle 2 Übersicht des normativen Charakters der Kapitel

3 Stakeholder

Das Identity und Access Management hat vier 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.

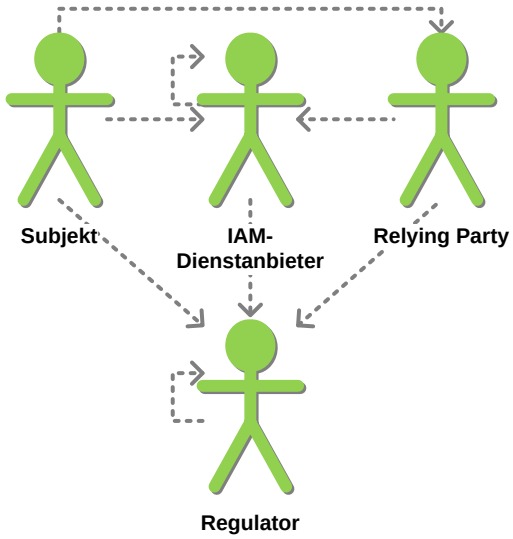

Abbildung 3 Stakeholder und deren Zusammenarbeit

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.
Regulator	Der *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.
Subjekt	Eine natürliche Person, Organisation oder ein Service, welches auf eine *Ressource* einer *Relying Party* zugreifen möchte. Ein *Subjekt* wird durch eine *eIdentity* beschrieben.

Die Stakeholder sind hierbei für unterschiedliche Teile des *IAM*-Gesamtprozesses zuständig. Ihre Zuständigkeiten sind in Abbildung 4 dargestellt. Dabei ist eine Überdeckung eines Pro-

zesses mit mehreren Stakeholdern dahingehend zu interpretieren, dass die Stakeholder zur Erreichung des Prozessziels zusammenarbeiten müssen.

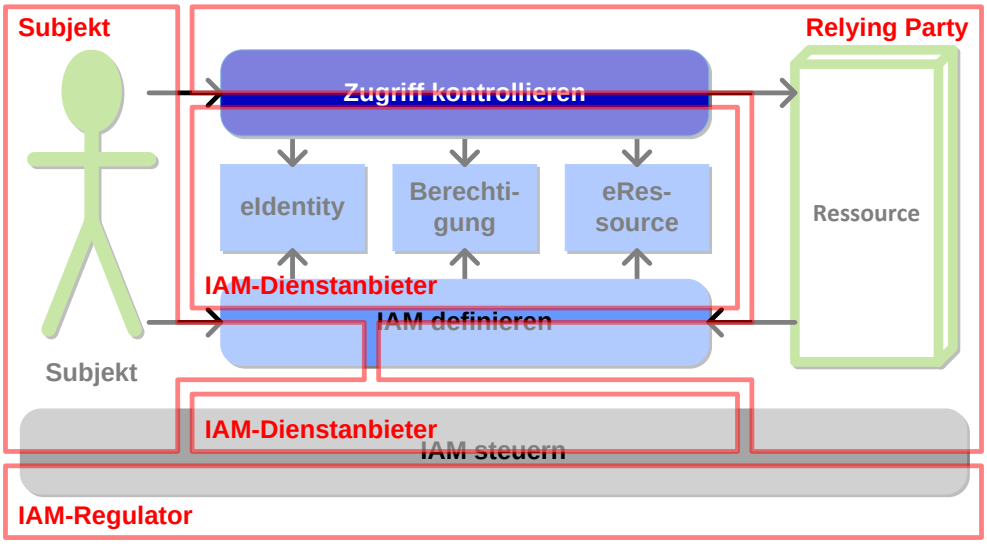

Abbildung 4 Zuständigkeiten der Stakeholder

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 *eIdentities*, *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 *eRessource* weitergeleitet. Res-2
- Der Aufwand für die Verwaltung der *eRessourcen* ist minimal. Res-3
- Der Aufwand für die Verwaltung der *Berechtigungen* (*Zugangsregeln* und *Zugriffsrechte*) ist minimal. Res-4
- Der Aufwand für die Administration der *eIdentities* (*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 *eIdentity* und den dazugehörigen *Credentials* muss zu jedem Zeitpunkt gewährleistet sein. Res-8.2
- Das *Subjekt* muss den Verdacht eines Missbrauchs seiner *eIdentity* 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 *eIdentities*. 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 *eIdentities* und *Credentials* ist einfach und günstig. Sub-9
- Die Benutzung von *eIdentities* 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 *eIdentity* 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 *eIdentity*. [SOWISCH] Sub-13
- *IAM-Dienstanbieter* unternehmen das vernünftig Machbare, um den Missbrauch der *eIdentity* 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. Abbildung 5 zeigt das Informationsmodell zum organisationsübergreifenden IAM.

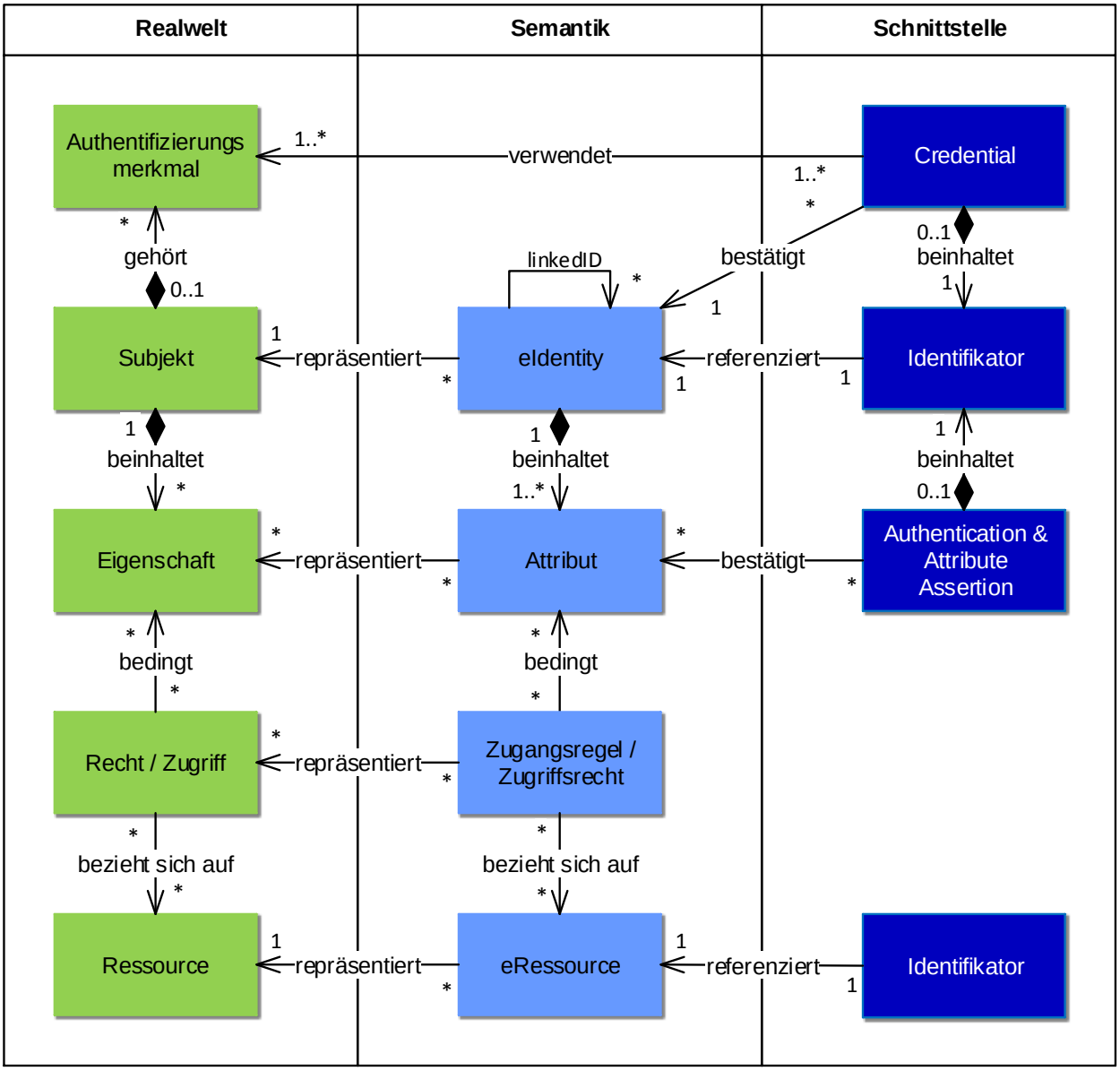

Abbildung 5 Informationsmodell

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 Abbildung 5 zeigt links (in grün) die Elemente der realen Welt, in der Mitte (in hellblau) das semantische Modell (der Informationssysteme), und rechts (in dunkelblau) die Schnittellenobjekte, die zum Informationsaustausch zwischen Informationssystemen verwendet werden.

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 Ausführungszeit (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 Abbildung 5 vorkommenden Elemente.

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.
Eigenschaften	*Eigenschaften* sind Charakteristika, Merkmale oder Verhalten eines *Subjekts*.
Subjekt	Eine natürliche Person, Organisation oder ein Service, die auf eine *Ressource* zugreift oder zugreifen möchte. Ein *Subjekt* wird durch *eIdentities* repräsentiert.
Authentifizierungsmerkmal	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.
Semantik	
eRessource	digitale Repräsentation einer *Ressource*. Eine *eRessource* 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 *eRessourcen*. 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* und die *Credentials* sind ebenfalls *Attribute*.
eIdentity	Repräsentation eines *Subjekts*. Eine *eIdentity* (*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 *eIdentities* haben.[1]
linkedID	Im organisationsübergreifenden Kontext erlaubt *linkedID*, eIdentities aus verschiedenen *Domänen* miteinander in Beziehung zu setzen. *eIdentities* 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*).
Schnittstelle	
Authentication & Attribut Assertion	Eine Bestätigung der erfolgreichen *Authentifikation* eines *Subjektes* (*Authentication Assertion*) oder eine Bestätigung eines *Attributs* (*Attribute Assertion*). Enthält den *Identifikator*.
Identifikator	Eine Zeichenkette, welche ein *eIdentity* oder eine *eRessource* innerhalb eines *Namensraumes* eindeutig bezeichnet.[2]
Credential	Nachweis zur Bestätigung der *eIdentity* eines *Subjekts*. Im *IAM*-Kontext wird zur Bestätigung einer *eIdentity* eine Benutzerkennung (*Identifikator*) in Verbindung mit einem (oder mehreren) *Authentifizierungsmerkmal(en)* verwendet.

Tabelle 3 Beschreibung der Elemente des Informationsmodels

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

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

6 Prozesse

Abbildung 6 zeigt eine Übersicht über die Geschäftsprozesse. Sie dient zur Veranschaulichung der Top Down-Tätigkeiten, welche für eine erfolgreiche Kooperation zwischen den Stakeholdern notwendig sind. Die Abbildung 6 übernimmt die Prozesse aus der Abbildung 1 und ergänzt deren Teilprozesse.

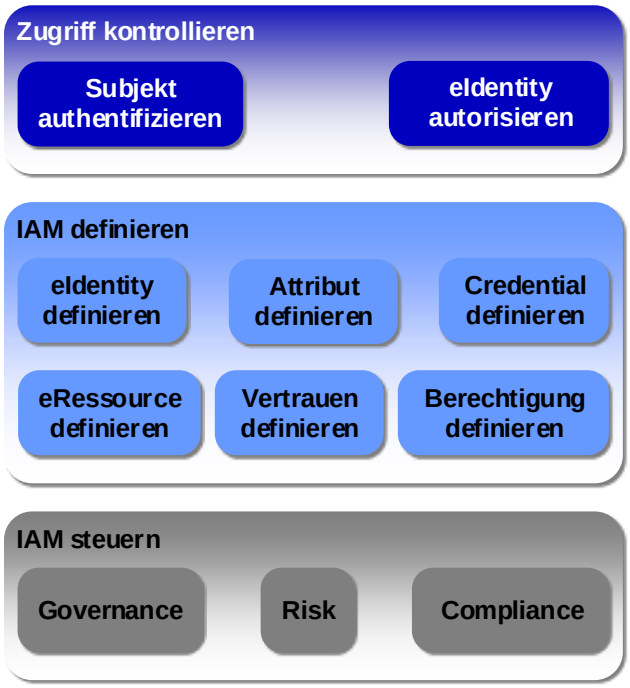

Abbildung 6 IAM-Prozesslandkarte

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

6.1 Zugriff kontrollieren

Zugriff kontrollieren umfasst die Prozesse der Ausführungszeit. 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. 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 Überprüfung einer behaupteten *eIdentity* eines *Subjekts.*

Tätigkeiten:

- Das Subjekt wird mit Hilfe von *Credentials* authentifiziert.

6.1.2 eIdentity autorisieren

eIdentitity autorisieren	Prüfen der *Zugriffsberechtigung* einer *authentifizierten eIdentity* auf eine *eRessource* und Erteilen des *Zugriffs* auf eine *Ressource* zur Ausführungszeit. Dabei wird zwischen *Grob-* und *Feinautorisierung* unterschieden.

Tätigkeiten:

- Vorbedingung einer *Autorisierung* ist die erfolgreiche *Authentifizierung* des *Subjekts*.
- Die *Zugangsregeln* und *Zugriffsrechte* für den *Zugriff* auf die *eRessource* werden ermittelt und daraus die benötigten *Attribute* zur *eIdentity* abgeleitet.
- Die *Attribute* werden (üblicherweise benutzer-zentriert) bestätigt.
- Der *Zugang* und der *Zugriff* werden erlaubt.
- Der *Zugriff* erfolgt.

6.2 IAM definieren

Während der Definitionszeit werden alle notwendigen Bedingungen geschaffen, damit zur Ausführungszeit 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 eIdentity definieren

eIdentity definieren	Umfasst die Prozesse zum Registrieren, Pflegen und Löschen von *eIdentities*

Tätigkeiten:

- *Subjekt* identifizieren und zugehörige *eIdentity* registrieren.
- *eIdentities* miteinander verlinken.
- *eIdentity* löschen.

Anmerkungen:

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

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 *eIdentity* registrieren.
- *Attribut* 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 *Credentials.*

Tätigkeiten:

- Erstellung, Erhebung und Vergabe von *Authentifizierungsmerkmalen* (z.B. Authentisierungszertifikats-*Credentials*).
- Speicherung der öffentlichen Elemente der *Authentifizierungsmerkmale* (z.B. öffentlicher Schlüssel) zur *eIdentity* im Directory des *Identity Providers.*
- Aushändigung des *Authentifizierungsmerkmals* (ev. mehrere) an das *Subjekt*.
- Revozierung von *Credentials*.

6.2.4 eRessource definieren

eRessource definieren	Definition, Pflege und Nutzung von *eRessourcen*.

Tätigkeiten:

- *Ressource* identifizieren und zugehörige *eRessource* (mit *Identifikator*) registrieren
- *eRessource* löschen

Anmerkungen:

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

6.2.5 Vertrauen definieren

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

Tätigkeiten:

- Pflege der *Metadaten* zu den *IAM-Dienstanbietern*
- Definieren und Widerrufen der Vertrauensbeziehungen (*Trust*) zwischen Stakeholdern, die im *föderierten* System Aufgaben wahrnehmen, z.B. von *Authentication*, *Attribute Assertion* oder *Zugang* Services.

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 *eIdentities* (gemäss Metadaten und Vertrauensbeziehungen aus *Vertrauen definieren*).
- Zuweisen von *Zugangsregeln* und *Zugriffsrechten* zu einer oder mehreren *eRessourcen*.
- Löschen von *Zugangsregeln* / *Zugriffsrechten*

6.3 IAM steuern

In den Geschäftsprozess *IAM steuern* 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 Ausführungszeit, 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 Ausführungszeit (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 Akteuren *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 (Akteure) und ihre Aufgaben werden nachfolgend genauer beschrieben. Sie sind in allen Modellen immer hellgrün dargestellt.

7.1.1 Subjekt

Subjekt	Eine natürliche Person, Organisation oder ein Service, die auf eine *Ressource* zugreift oder zugreifen möchte. Ein *Subjekt* wird durch *eIdentities* beschrieben.

Aufgaben (zur Ausführungszeit):

- *Authentisiert* sich.
- 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 Ausführungszeit):

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

7.2 Services zur Definitionszeit

In Abbildung 7 sind die Services zur Definitionszeit (in den Modellen hellblau), die zur Verwaltung der verschiedenen Objekte benötigt werden, dargestellt. Die erste Gruppe bezieht sich auf das Subjekt. Die zweite Gruppe definiert Objekte in Abhängigkeit der *Ressource*.

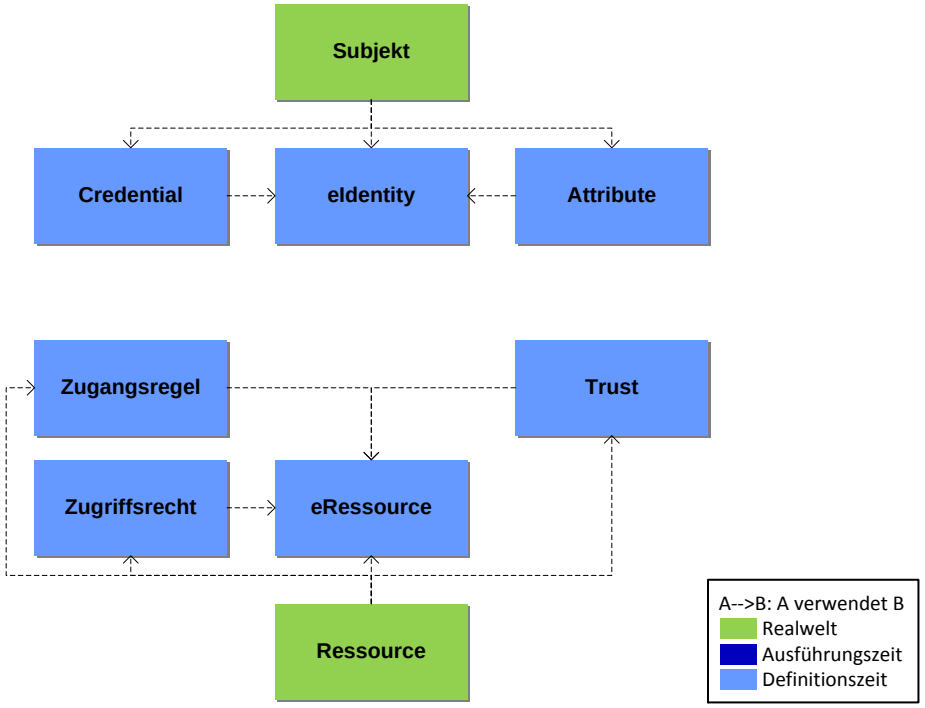

Abbildung 7 Geschäftsservices – Definitionszeit

7.2.1 eIdentity Service

eIdentity Service	Der *eIdentity Service* stellt zu *Subjekten eIdentities* aus und verwaltet sie.

Aufgaben:

- Ermöglicht die Registrierung von *Subjekten*
- Stellt Funktionen zur Ausgabe, Pflege und Verwaltung von *eIdentities* bereit.
- Stellt die physische *Identifizierung* des *Subjekts* anhand definierter Regeln abhängig von der angestrebten Qualität sicher (Vertrauenskette zwischen *eIdentity* und *Subjekt*).
- Kennt andere *eIdentity Services* und ermöglicht die Pflege der *linkedID* zu anderen *eIdentities* des *Subjekts*.
- Stellt in geeigneter Weise die Qualität und Aktualität der *eIdentity* sicher
- Begrenzt die Lebensdauer von *eIdentities* und unterstützt die *Subjekte* in der Erneuerung ihrer *eIdentities*.

- Kann *eIdentities* widerrufen.
- Gewährt vertrauenswürdigen *Credential* und *Attribute* Services elektronischen Zugang zu den *eIdentities*.
- Gewährt vertrauenswürdigen *Authentication* Services elektronischen Zugang zu den *eIdentities*.

7.2.2 Credential Service

Credential Service	Der *Credential* Service gibt *Credentials* aus und verwaltet sie. Die *Credentials* können von unterschiedlichem Typ sein. Ein Credential bezieht sich auf eine *eIdentity* und ist auf ein bestimmtes *Subjekt* ausgestellt.

Aufgaben:

- Registriert *Credentials* unter allfälliger Verwendung von *Authentifizierungsmerkmalen* des *Subjekts*
- Stellt Funktionen zur Ausgabe und Verwaltung der *Credentials* zur Verfügung.
- Verwendet für kryptografische Schlüssel ein Schlüsselmanagement (nicht Teil der IAM-Geschäftsservices).
- Ermöglicht die Überprüfung der Gültigkeit der verwalteten *Credentials* und der Zugehörigkeit zu einer *eIdentity* bzw. dem zugehörigen *Subjekt*.
- Begrenzt die Lebensdauer der ausgegebenen *Credentials* und unterstützt die *Subjekte* in der Erneuerung ihrer *Credentials*.
- Kann *Credentials* widerrufen.

7.2.3 Attribute Service

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

Aufgaben:

- Stellt Funktionen zur Pflege und Verwaltung der Informationen bereit, welche nötig sind, um bestimmen zu können, ob ein *Subjekt* ein 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 *eIdentity* des Subjekts.
- 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 *eIdentity Service* abfragen können (z.B. Verifikation der *eIdentity*).

Anmerkungen:

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

7.2.4 Trust Service

Trust Service	Der *Trust* Service pflegt die akzeptierten, vertrauenswürdigen *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 Certification Service Provider (CSP)
- Registriert die Services der *IAM-Dienstanbieter* und deren Qualität (z.B. autoritative Datenquellen)
- Definiert die Metadaten und die Semantik der *Attribute* der *eIdentities* und der *eRessourcen* für den *Broker* Service und die anderen Metadaten-abhängigen Geschäftsservices.
- Kennt andere *Trust* Services und kann ihre Informationen nutzen

7.2.5 eRessource Service

eRessource Service	Der *eRessource* Service stellt zu *Ressourcen eRessourcen* aus und verwaltet sie.

Aufgaben:

- Stellt Funktionen zur Definition und Verwaltung von *eRessourcen* bereit.
- Eine *Ressource* kann durch mehrere *eRessourcen* repräsentiert sein.
- Ordnet jeder *eRessource* genau einen eindeutigen *Identifikator* zu.

7.2.6 Zugangsregel Service

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

Aufgaben:

- Stellt Funktionen zur Verwaltung der *Zugangsregeln* bereit, die den Zugang zu den *eRessourcen* regeln (*Grobautorisierung*). Die *Zugangsregeln* enthalten Angaben zur *Authentisierung* und zu *Attributen* (inklusive deren Qualität), die ein *Subjekt* entsprechend dem Schutzbedarf erfüllen muss.

7.2.7 Zugriffsrecht Service

Zugriffsrecht Service	Der *Zugriffsrecht* Service verwaltet die Rechte für die Nutzung einer *eRessource*. Die Rechte sind auf der Basis von *Authentisierung*, *Attributen* oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen) definiert.

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 der *Ressource* zugreifen darf (*Feinautorisierung*).

7.3 Services zur Ausführungszeit

Die Geschäftsservices zur Laufzeit (in den Modellen dunkelblau) sind in Abbildung 8 dargestellt. Die Abbildung enthält alle Services, die zur Abwicklung der Prozesse *Subjekt authentifizieren* und *eIdentity autorisieren* zur Ausführungszeit verwendet werden.

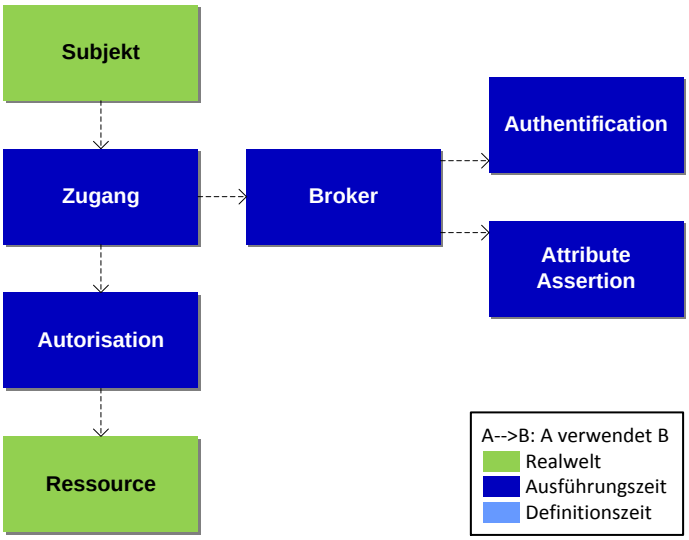

Abbildung 8 Geschäftsservices – Ausführungszeit

7.3.1 Authentication Service

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

Schnittstelle:

In: *Identifikator*, *Authentifizierungsmerkmale*

Out: *Authentifizierungsbestätigung* (Angabe, ob die Überprüfung des *Subjekts* positiv ausgefallen ist oder nicht)

Aufgaben:

- Überprüft, ob die gelieferten *Authentifizierungsmerkmale* zu *Credentials* der *eIdentity* des gelieferten *Identifikator* gehören.
- Bestätigt im positiven Fall die Authentizität des aufrufenden *Subjekts* mit einer *Authentifizierungsbestätigung* der entsprechenden Qualität
- Holt das Einverständnis des *Subjekts* ein, die *Authentifizierungsbestätigung* an den aufrufenden Service zu übermitteln (Zustimmung; erfolgt allenfalls zusammen mit der Zustimmung zur Übermittlung der *Attributbestätigungen*).

7.3.2 Attribute Assertion Service

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

Schnittstelle:

In: Attribute-Request, *Identifikator*

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

Aufgaben:

- Generiert berechnete und abgeleitete Attributwerte aus *Attributen* (z.B. over18).
- Bestätigt elektronisch mit entsprechender Qualität, ob ein bestimmtes *Attribut* einem *Subjekt* zugewiesen ist oder nicht.
- Holt das Einverständnis des *Subjekts* 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.

Schnittstelle:

In: *Identifikator*, [Credentials], Art und Qualität der *Authentifikation*, Art und Qualität der *Attribute*

Out: *Authentifizierungsbestätigungen, Attributbestätigungen*

Aufgaben:

- *Trusted Third Party*, die Services und *Metadaten* vermittelt (Discovery)
- Kontaktiert die gemäss Trust vertrauenswürdigen *Authentication Services* zur *Authentifikation* des *Subjekts*.
- [OPTIONAL] Kontaktiert ausgehend von der durch den *Identifikator* referenzierten eIdentity 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.
- [OPTIONAL] Kontaktiert ausgehend von der durch den *Identifikator* referenzierten eIdentity 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 *Authentication & Attribute Assertions* zusammen. 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 *Authentication & Attribute Assertions* 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.

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: *Subjekt* (*Identifikator*, *Credential*), *Identifikator* einer *Ressource*

Out: *Authentifizierungsbestätigungen, Attributbestätigungen*

Aufgaben:

- Ruft einen *Broker*-Service und fordert die *Authentifizierungsbestätigung* und *Attributbestätigung* entsprechend der *Zugangsregel* für die *eRessource* an.
- 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 *Authentication Assertions* und die *Attribute Assertions* an den *Autorisation* Service weiter.
- Informiert das *Subjekt* über benötigte Sicherheitsinformationen (z.B. benötigte Attribute, geforderter Qualität-Level) bezüglich des *Zugriffs*.
- [OPTIONAL] Erzeugt und verwaltet, wenn gefordert, Zugangsinformationen. Diese enthalten alle notwendigen Daten, welche für die vollständige Nachvollziehbarkeit benötigt werden.
- [OPTIONAL] Bietet rechtlich verifizierte und verifizierbare Audit- und Monitoring-Funktionen zur vollständigen Nachvollziehbarkeit.

7.3.5 Autorisation Service

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

Schnittstelle:

In: *Authentifizierungsbestätigungen*, *Attributbestätigungen*, *Identifikator* einer *eRessource*

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

Aufgaben:

- Überprüft, ob die übergebenen Bestätigungen (*Assertions*) 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.
- [OPTIONAL] Erzeugt und verwaltet, wenn gefordert, Zugriffsinformationen. Diese enthalten alle notwendigen Daten, welche für die vollständige Nachvollziehbarkeit benötigt werden.
- [OPTIONAL] Bietet rechtlich verifizierte und verifizierbare Audit- und Monitoring-Funktionen zur vollständigen Nachvollziehbarkeit.
- [OPTIONAL] Arbeitet mit dem Lizenzmanagement zusammen, z.B. um den Zugriff zu verweigern, wenn die maximale Anzahl von gleichzeitigen Benutzern erreicht ist.

7.4 Gesamtmodell

In Abbildung 9 werden alle IAM-Geschäftsservices zusammen dargestellt. Man erkennt, dass die Laufzeitservices zur Erfüllung ihrer Funktionalitäten auf die Daten der Services der Definitionszeit zugreifen.

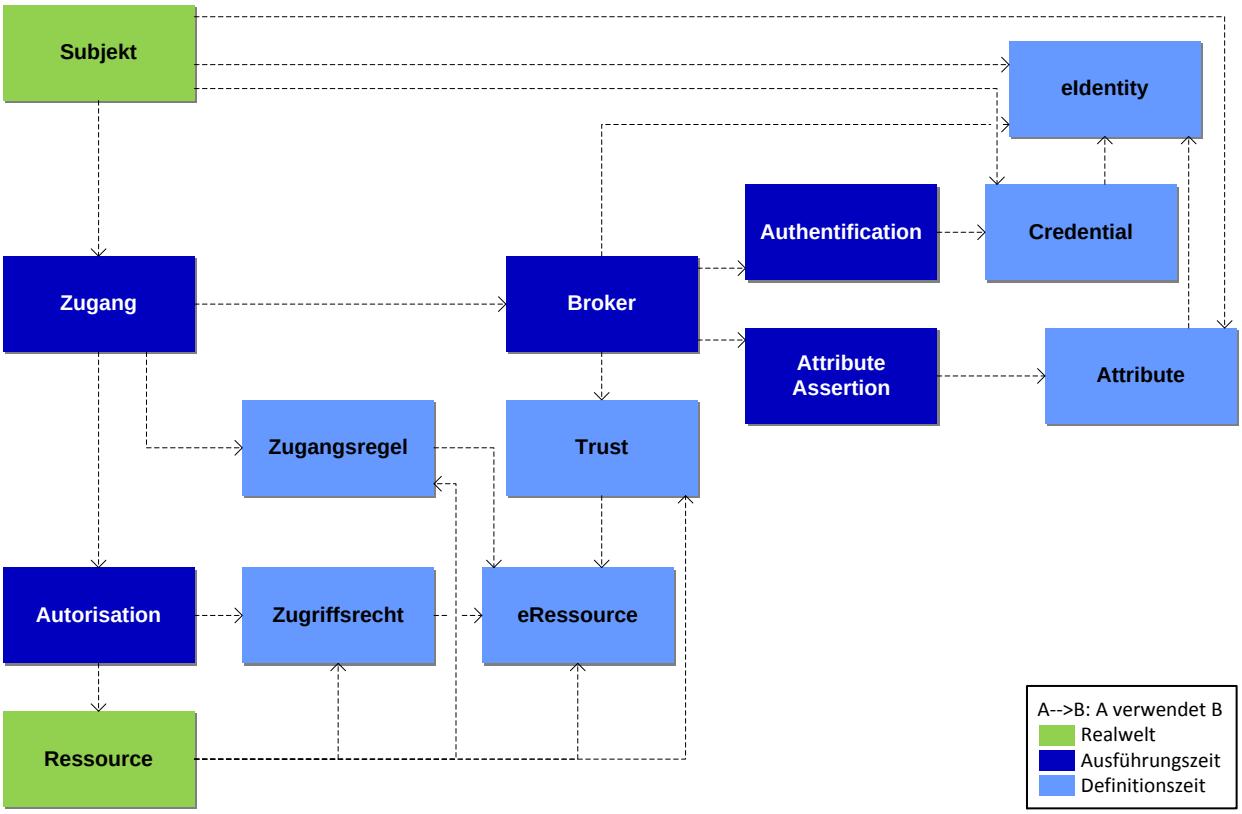

Abbildung 9 Geschäftsservices – Übersicht

7.5 Prozessunterstützung durch Geschäftsservices

In diesem Abschnitt wird an den Laufzeitprozessen dargestellt, wie die Services zusammenarbeiten. Die Zusammenarbeit der Services zur Erbringung der Definitionsprozesse ist einfach und in den Services bereits direkt angesprochen. Diese werden deshalb hier nicht dargestellt.

7.5.1 Subjekt authentifizieren

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

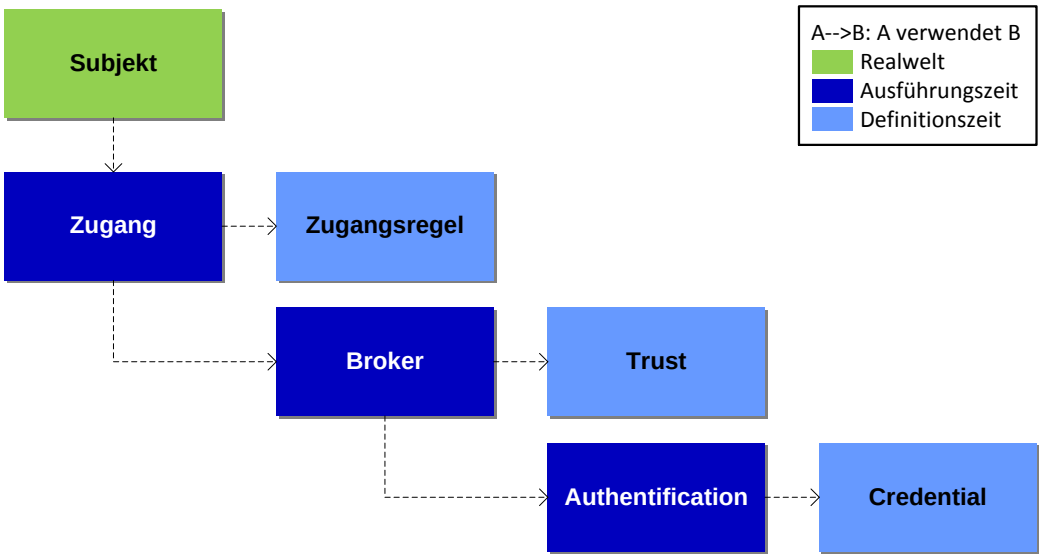

Abbildung 10 Prozessunterstützung *Subjekt authentifizieren*

Subjekt authentifizieren folgt dem nachstehenden Ablauf:

- Subjekt möchte unter Angabe des *Identifikators* einer *Ressource* auf die Ressource zugreifen.
- *Zugang* Service prüft die *Zugangsregeln* für die durch den Identifikator referenzierte eRessource und verlangt vom *Broker Service*, das *Subjekt* entsprechend den Anforderungen zu authentifizieren.
- Der *Broker* Service prüft, welche *Authentication Service* gemäss *Trust* Service die Anforderungen vom *Zugang* Service erfüllen. Er bietet dem *Subjekt* die entsprechende Auswahl an.
- Das *Subjekt* authentisiert sich gegenüber einem dieser *Authentication* Service. Dieser prüft das *Credential* des *Subjekts*.

7.5.2 eIdentity autorisieren

Abbildung 11 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *eIdentity autorisieren.*

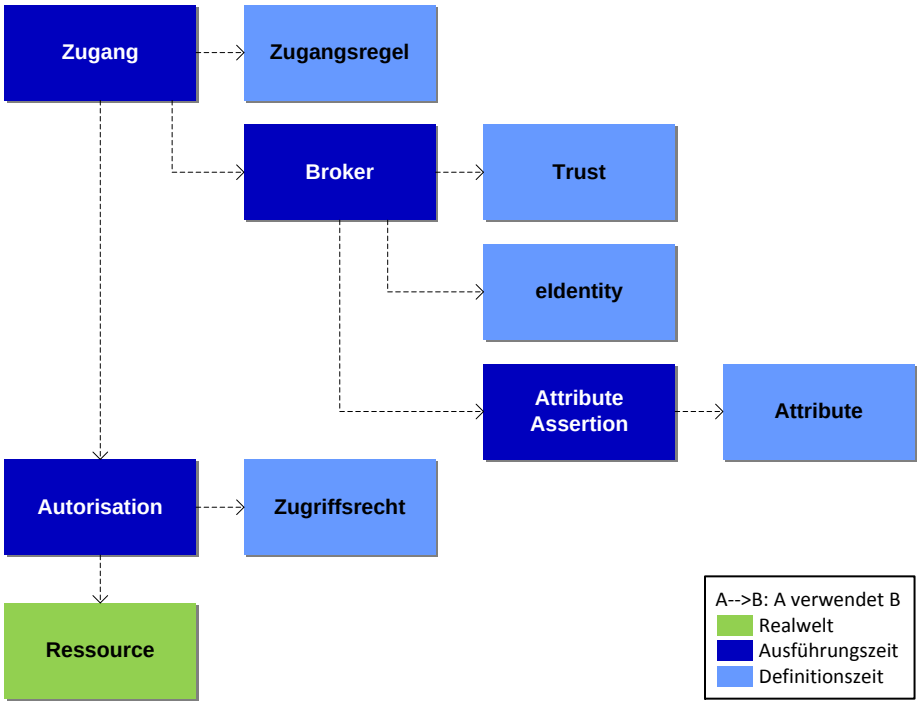

Abbildung 11 Prozessunterstützung *eIdentity autorisieren*

eIdentity autorisieren folgt dem nachstehenden Ablauf:

- Vorbedingung einer *Autorisierung* ist die erfolgreiche *Authentifizierung* des *Subjekts* (vgl. Abschnitt 7.5.1).
- *Zugang* Service prüft die Zugangsregeln für diese eRessource und verlangt vom Broker, entsprechend den Anforderungen Attribute zur *eIdentity* zu bestätigen.
- Der *Broker* Service prüft, welche *Attribute Assertion* Service gemäss *Trust* Service die Anforderungen vom *Zugang* Service erfüllen. Diese *Attribute Assertion* Service-Auswahl wird auf die reduziert, die gemäss den verlinkten *eIdentities* (linkedID) der *eIdentity* Service Informationen zur *eIdentity* führen.
- Der *Broker* Service frägt die entsprechenden *Attribute Assertion* Service, die entsprechenden *Attribute* zu bestätigen.
- *Autorisation* Service prüft das Zugriffsrecht basierend auf den *Authentication & Attribut Assertions*.
- *Autorisation* Service gewährt den *Zugriff* auf die *Ressource*.

Anmerkung: In den Abschnitten 7.5.1 und 7.5.2 wendet sich Zugang je einmal an den Broker. Diese Anfragen können auch in einer Anfrage kombiniert werden.

7.6 Zuordnung Service zu Informationselemente

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

		Informationselement									
		eIdentity[3]	Attribut[4]	Zugangsregel	Zugriffsrecht	eRessource	Credential	Identifikator einer eIdentity	Authentication Statem.	Attribute Statement	Identifikator einer Ressource
Geschäftsservice	eIdentity	B	B[5]					B			
	Credential	L	B[6]				B	L			
	Attribute	L	B					L			
	Trust	M	M			M					
	eRessource					B					B
	Zugangsregel	M	M	B		L					
	Zugriffsrecht	M	M	L	B	L					
	Authentication	L					L	L	B		
	Attribut Assertion		L					L		B	
	Broker	L						L	LB[7]	LB[7]	L
	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

[3] inkl. Beziehung linkedID
[4] inkl. Beziehung zu eIdentity
[5] B für Identifikator (ist auch ein Attribut)
[6] B für Credentials (sind auch Attribute)
[7] B, wenn Broker selber kombinierte *Authentication and Attribute Assertions* ausstellt

7.7 Zuständigkeiten für Geschäftsservices

Tabelle 5 zeigt auf, welcher Stakeholder idealtypisch welchen Service anbietet. Die Geschäftsservices werden in Kapitel 7 näher beschrieben. Die hier vorgeschlagene Aufteilung optimiert bezüglich Wiederverwendung der Services. Die *Relying Party* gibt deshalb möglichst viel Betriebsverantwortung an *IAM*-Dienstanbieter.

		Stakeholder			
		Subjekt	IAM-Dienstanbieter	Relying Party	Regulator
Geschäftsservices	eIdentity		X		
	Credential		X		
	Attribute		X		
	Trust		X		
	eRessource			X	
	Zugangsregel		X		
	Zugriffsrecht			X	
	Authentication		X		
	Attribute Assertion		X		
	Broker		X		
	Zugang		X		
	Autorisation			X	

Tabelle 5 Beziehung zwischen Geschäftsservices und Stakeholder

8 Identity Federation Konzepte

E-Government erfordert eine elektronische Zusammenarbeit über Organisationsgrenzen hinweg. Das Problem dabei ist, dass sowohl die *Ressourcen*, wie auch die *Subjekte* sich, wie in Abbildung 12 dargestellt, in unterschiedlichen administrativen Domänen befinden.[8]

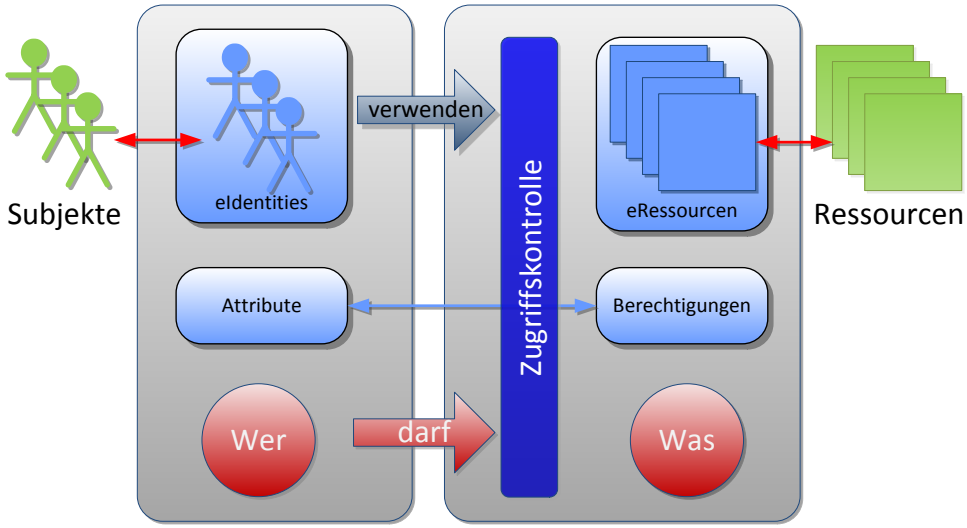

Abbildung 12 Wer darf was?

E-Government stellt demnach eine organisations- und domänenübergreifende Berechtigungslandschaft dar. Der Zugriff von ‚Aussen' auf eine geschützte *Ressource* einer *Domäne* wird durch geeignete Mittel ermöglicht. Das *Subjekt* wird dabei *authentifiziert* und auf der Basis der *Berechtigungen autorisiert*, auf die *Ressource* zuzugreifen. Es gibt einige Lösungsansätze, wie diesem Problem begegnet werden kann.

1. Betroffene *Domänen* tauschen die Informationen ihrer *eIdentities* aus, so dass diese jeweils in den anderen *Domänen* bekannt sind.
2. *Domänen* bauen untereinander oder zu einer dritten Partei eine Vertrauensbeziehung auf.

Insbesondere, wenn eine grössere Anzahl *Domänen* beteiligt sind, skaliert der erste Lösungsansatz schlecht. Ausserdem müssen die *eIdentities* laufend abgeglichen werden, was zu einem grossen Aufwand führen kann. Der zweite Ansatz ist deutlich flexibler. Es gibt einige Modelle dazu, wie solche Vertrauensbeziehungen zwischen administrativen *Domänen* aufgebaut werden können (bilateral, indirekt hierarchisch oder föderiert). Hier wird der Fokus auf die *Identity Federation* gelegt.

[8] Die in diesem Kapitel enthaltenen Grafiken beinhalten Farben für Objekte, welche keinen Bezug auf die vorgängig in diesem Dokument verwendete Bedeutung von Farben nimmt.

8.1 Vertrauen und Föderieren

Eine *Föderation* beinhaltet eine Delegierung der Zuständigkeiten und der Verantwortung zwischen den einzelnen Parteien. Dies setzt ein entsprechendes Vertrauen voraus. Im Falle einer *Föderation* von *eIdentities* zwischen mehreren *Domänen*, ist heute die Hauptanwendung die Single-Sign-On-Funktionalität. Diese Vereinfachung der *Authentifizierung* eines *Subjekts* ist aber nicht das Einzige, was in einer *Identity Federation* delegiert werden kann. Je nach Ausprägung können auch *Autorisierung* und sogar das ganze *Identity Management* ausgelagert werden.

Eine *Identity Federation* mit SSO-Funktionalität muss also über standardisierte Verfahren verfügen, wie die Parteien untereinander Informationen austauschen, so dass diese gegenseitig verstanden und auf Echtheit und Integrität geprüft werden können.

8.2 Identity Federation Grundbausteine

Eine *Identity Federation* führt neue Begriffe und Komponenten als Grundbausteine ein. In den folgenden Abschnitten wird der Begriff IdP/AA verwendet, welcher den Geschäftsservices *Authentication Service*, *Attribute Assertion Service*, *Credential Service*, *eIdentity Service* und *Attribute Service* in Kapitel 7 entspricht.

Wenn ein *Subjekt* auf eine bestimmte *Ressource* einer *Relying Party* (RP) zugreifen will (vgl. (1) in Abbildung 13), so wählt das Subjekt seinen Heimat-*Authentifizierungsdienst* (*Identity Provider*) aus. Die *Relying Party* leitet das *Subjekt* an diesen weiter (2). Der *Identity Provider* (IdP) unterhält lokale *eIdentities*, beispielsweise in Form eines Verzeichnisses der Subjekte. Der *Identity Provider authentifiziert* das *Subjekt* und kann das Ergebnis in einer standardisierten Form gegenüber der anfragenden Stelle (*Relying Party*) bestätigen. Der *Identity Provider* kann auch als *Attribute Authority* (AA) agieren, indem er zur Authentifizierungsbestätigung weitere Informationen des *Subjekts* in Form von Attributbestätigungen mitliefert. Bevor diese Attributbestätigungen ausgeliefert werden können, gibt das *Subjekt* dazu seine Zustimmung (3).

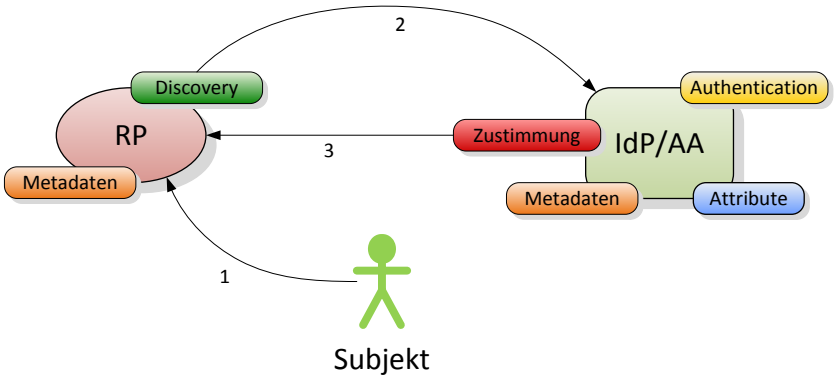

Abbildung 13 Bausteine einer Identity Federation

Die *Relying Party* verifiziert die Antwort und gewährt dem Subjekt auf Grund des Resultats Zugriff auf die *Ressource* oder weist ihn ab. Die Autorisierung erfolgt lokal auf Seite der *Relying Party*. Damit die jeweiligen Services ihre Eigenschaften kennen und sich gegenseitig vertrauen können, benötigt das System genau definierte Informationen aller beteiligten Komponenten. Diese Information wird in Form von *Metadaten* gegenseitig ausgetauscht.

8.3 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.

8.3.1 RP-zentriertes Modell

Das *RP-zentrierte Modell* (vgl. Abbildung 14) 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 *eIdentities* nicht selbst verwalten muss. Ihr reicht die *Authentifizierungs-* und *Attributbestätigung*, um das *Subjekt* für den *Zugriff* auf die *Ressource* zu berechtigen.

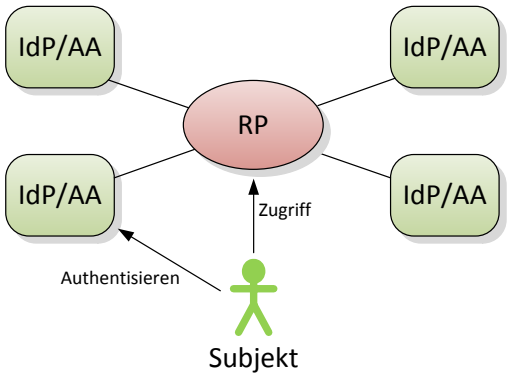

Abbildung 14 RP-zentriertes Modell

8.3.2 IdP/AA-zentriertes Modell

Das *IdP/AA-zentrierte Modell* (vgl. Abbildung 15) 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.

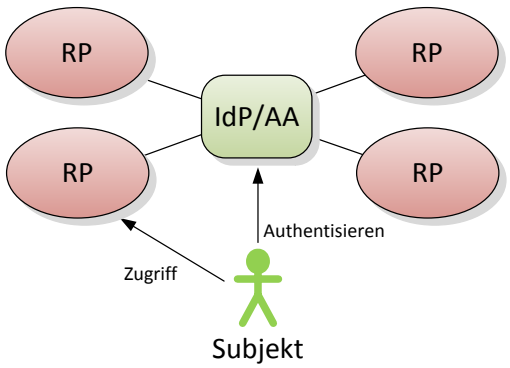

Abbildung 15 IdP/AA-zentriertes Modell

8.3.3 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 *eIdentities* 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.

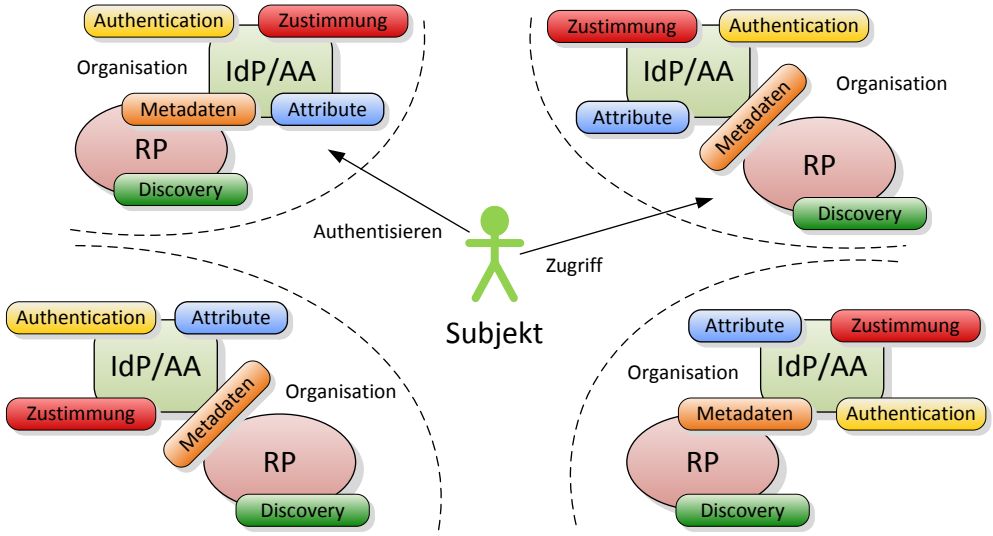

Abbildung 16 Cross Domain Modell

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 8.3.4).

8.3.4 Zentralisierte Metadaten und Discovery

Die Auslagerung der beiden Dienste Metadaten und Discovery, wie in Abbildung 17 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).

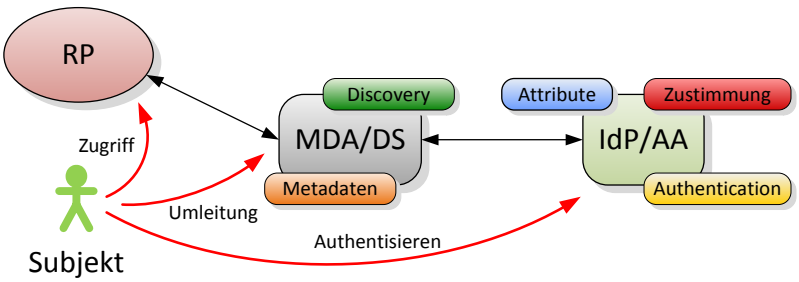

Abbildung 17 Zentralisierte Metadaten und Discovery Service

Es können aber noch weitere Dienste zentralisiert werden, wie das *Hub-'n'-Spoke Modell* in Abschnitt 8.3.5 aufzeigt.

8.3.5 Hub-'n'-Spoke Modell

Das Hub-'n'-Spoke[9] Modell basiert auf einem zentralen *Identity Hub*, welchem alle beteiligten Parteien mit ihren Diensten vertrauen. Wie in Abbildung 18 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 *eIdentities* 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.

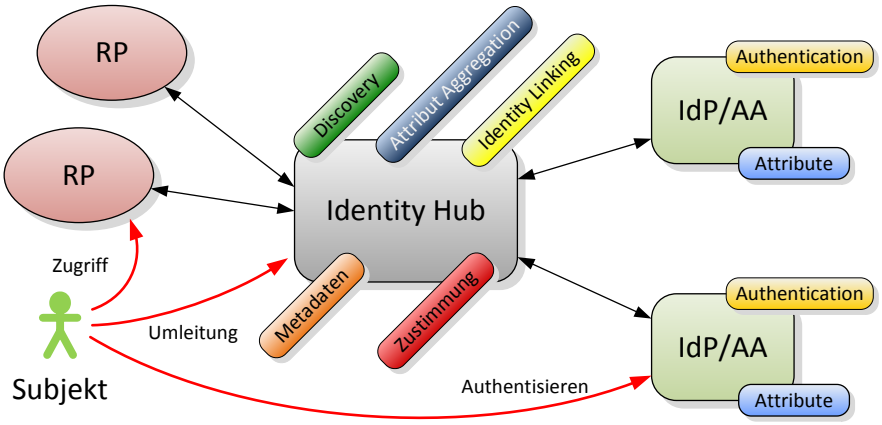

Abbildung 18 Hub-'n'-Spoke Modell

Das in Abbildung 18 dargestellte *Hub-'n'-Spoke Modell* zeigt eine Möglichkeit der Zentralisierung von Diensten auf. Es sind hier ganz verschiedene Ausprägungen der Zentralisierung möglich, wie es auch Mischformen der hier vorgestellten *Identity Federation* Modelle gibt.

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

[9] Nabe und Speiche

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

Bernold Ronny	Berner Fachhochschule
Besiryan René	accessec
Buff Raffael	Abraxas
Burger Hans	Adnovum
Eberle Marcel	Kanton SG
Fischer Markus	
Häni Hans	Berner Fachhochschule
Hassenstein Gerhard	Berner Fachhochschule
Hempel Torsten	IC Consult
Kuhn Fabienne	Berner Fachhochschule
Laube-Rosenpflanzer Annett	Berner Fachhochschule
Leiser Daniel	ATOS AG
Minth Lars	ISB
Muhm Christofer	IC Consult
Müller Willy	ISB
Rohr Sebastian	Accessec
Spichiger Andreas	Berner Fachhochschule
Topfel Martin	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 Papiers 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 *eIdentity* des Stellvertreters für eine gewisse Zeit eine Menge von *Attribute* der *eIdentity* 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 *eIdentity.* 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-bestätigung	Siehe *Authentication Assertion.*
Authentisierung	Nachweis der eigenen *eIdentity* eines *Subjekts*.[10]
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.

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

Authorization Provider	*Entität*, die *Autorisierung* als Dienstleistung anbietet.
Authorization Service	Der Service überprüft zur Ausführungszeit die Einhaltung der Rechte für die Nutzung der *eRessource* und erlaubt dem *Subjekt* die Nutzung, wenn es die entsprechenden Rechte besitzt.
Autorisierung	a) Administration: Definition der *Zugangsregeln* und *Zugriffsrechte* auf eine *eRessource*. 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 *eIdentity* eines *Subjekts*. Im IAM-Kontext wird zur Bestätigung einer *eIdentity* 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 *eIdentity* 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 *eIdentity*.
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.*
eIdentity	Repräsentation eines *Subjekts*. Eine *eIdentity* (*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 *eIdentities* haben.
eIdentity Service	Der *eIdentity* Service stellt zu *Subjekten eIdentities* aus und verwaltet sie.
Elektronische Identität / Electronic Identity	Siehe *eIdentity*
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. [SAMLGlossar]
eRessource	Digitale Repräsentation einer *Ressource*. Eine *eRessource* hat einen *Identifikator* (eindeutiger Name, oft URL/URI), welche innerhalb eines *Namensraumes* eindeutig einer *Ressource* zugewiesen werden kann. Eine *Ressource* kann mehrere *eRessourcen* haben.
eRessource Service	Der *eRessource* Service stellt zu *Ressourcen eRessourcen* aus und verwaltet sie.
Föderiertes Identitätsmanagement / Federated Identity Management (FIdM)	Föderiertes Identitätsmanagement erlaubt die übergreifende Verwendung von *eIdentities* 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 (*eIdentities*)

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 7.
Identifikator	Eine Zeichenkette, welche ein *eIdentity* oder eine *eRessource* 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 *eIdentity* eines *Subjekts* verwendet (siehe *eIdentity*).
Identity Provider (IdP)	*Entität*, die *eIdentity* 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*, eIdentities aus verschiedenen Domänen miteinander in Beziehung zu setzen. eIdentities 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 19.

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 *eIdentity* 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.
Ressourcen-verantwortlicher	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) *eIdentity*: *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 *eIdentities* repräsentiert.

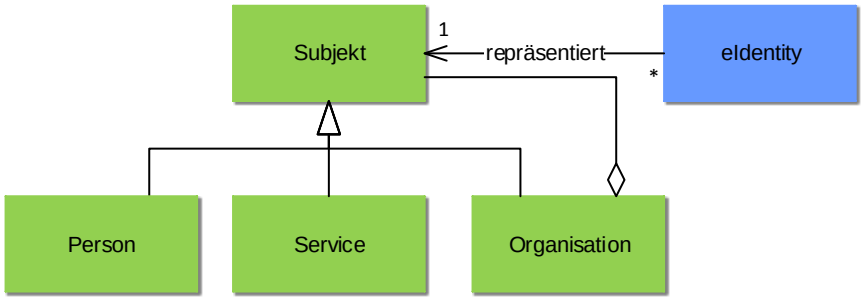

Abbildung 19 Definition Subjekt

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*
Vermittler-infrastruktur	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 *eRessourcen*. 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 *eRessourcen*. 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 *eRessource*. Die Rechte sind auf der Basis von *Authentisierung*, *Attributen* oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen) definiert.

Anhang E – Änderungen gegenüber Version 1.00

Der vorliegende Standard basiert auf dem Gestaltungsprinzip eCH-0107 v1.00. 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 1.00 verwiesen.

Grundsätzliches:

- *V1.00 ist eine Best Practice, V2.0 ist neu ein Standard.*
- *Der Aufbau der Kapitel wurde grundsätzlich geändert und soll dem Leser so einen einfacheren Einstieg in das organisationsübergreifende IAM gewährleisten.*
- *Die Arbeiten aus dem Projekt Stabi 3 eGov und deren Lösungsarchitektur wurden integriert und umgesetzt.*
- *V2.0 beschränkt sich konsequent auf das behördenübergreifende IAM.*

Kapitel 2 Einleitung [eCH-0107 v1.00 Kapitel 1]

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

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

5 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).*

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

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

8 Identity Federation Konzepte [neu]

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