

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

Name	Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)
Standard-Nummer	eCH-0107
Kategorie	Standard (neu)
Reifegrad	definiert; experimentell; implementiert; verbreitet
Version	3.0
Status	Genehmigt; ausser Kraft
Genehmigt am	
Ausgabedatum	2013-12-04
Ersetzt Version	2.0
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Beilagen	--
Autoren	<p>Annett Laube-Rosenpflanzner, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Marc Kunz, BFH TI, marc.kunz@bfh.ch Thomas Kessler, Temet, thomas.kessler@temet.ch Torsten Gruoner, ISB, torsten.gruoner@isb.admin.ch Marc Heerkens, ISB, marc.heerkens@isb.admin.ch eCH Fachgruppe IAM</p> <p>V2.0: Ronny Bernold, BFH FBW, ronny.bernold@bfh.ch Gerhard Hassenstein, BFH TI, gerhard.hassenstein@bfh.ch Annett Laube-Rosenpflanzner, 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</p> <p>V1.0: Willy Müller, ISB, willy.mueller@isb.admin.ch Hans Häni, AFT TG SEAC-Projektgruppe IAM</p>
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	8
2	Einleitung	8
2.1	Überblick	8
2.1.1	Einführung IAM.....	8
2.1.2	Anwendungsgebiet	10
2.1.3	Föderiertes IAM.....	10
2.1.4	Abgrenzung	11
2.1.5	Vorteile	11
2.2	Schwerpunkte.....	12
2.3	Normativer Charakter der Kapitel.....	12
3	Rollen und Stakeholder.....	14
3.1	Rollen in IAM	14
3.2	Stakeholder im IAM	17
4	Anforderungen	21
4.1	Grundprinzipien eines föderierten IAM-Systems	21
4.2	Anforderungen an das föderierte IAM-System	22
4.3	Anforderungen der Stakeholder	23
4.3.1	Anforderungen des Leistungsbezügers	24
4.3.2	Anforderungen der Leistungserbringer	25
4.3.3	Anforderungen der Dienstanbieter.....	26
4.3.4	Anforderungen der Führung	27
4.3.5	Anforderungen des Regulators.....	28
5	Informationsarchitektur	29
6	Prozesse	34
6.1	Zugriff kontrollieren (Laufzeit)	35
6.1.1	Subjekt authentifizieren	36
6.1.2	E-Identity bestätigen.....	36
6.1.3	Zugang erlauben	37
6.1.4	Zugriff erlauben und Attribute offenlegen.....	37
6.2	IAM definieren (Definitionszeit)	38
6.2.1	E-Identity pflegen	38
6.2.2	Attribut pflegen	38
6.2.3	Authentifizierungsmittel pflegen	39
6.2.4	E-Ressource pflegen	39
6.2.5	Berechtigungen pflegen.....	40
6.3	IAM unterstützen.....	40
6.4	IAM führen (Etablierung).....	40

6.4.1	Dienstanbieter managen	40
6.4.2	Relying Parties verwalten	41
6.4.3	Attributstruktur managen	42
6.4.4	IAM-Servicekatalog verwalten	42
6.4.5	Risikoanalyse durchführen und Risiko überwachen.....	43
6.4.6	IAM-Führung managen.....	43
6.5	IAM steuern (Regulierung).....	43
6.5.1	IAM-Policy verwalten	44
6.5.2	Qualitätsmodel(le) pflegen.....	44
6.5.3	IAM-Führung beraten	45
6.5.4	Risikoanalyse durchführen	45
6.5.5	IAM Steuerung managen.....	46
7	Geschäftsservices.....	47
7.1	Realweltobjekte	47
7.1.1	Subjekt	47
7.1.2	Ressource	48
7.2	Services zur Definitionszeit.....	48
7.2.1	E-Identity Service	48
7.2.2	Credential Service	49
7.2.3	Attribute Service	50
7.2.4	Trust Service	51
7.2.5	E-Ressource Service.....	51
7.2.6	Zugangsregel Service.....	52
7.2.7	Zugriffsrecht Service.....	52
7.3	Services zur Laufzeit	53
7.3.1	Authentication Service.....	53
7.3.2	Attribute Assertion Service	54
7.3.3	Broker Service.....	55
7.3.4	Zugang Service	56
7.3.5	Autorisation Service.....	57
7.3.6	Logging Service.....	57
7.4	Gesamtmodell	58
7.5	Prozessunterstützung durch Geschäftsservices	59
7.5.1	Subjekt authentifizieren	59
7.5.2	Identität fördern.....	59
7.5.3	E-Identity autorisieren und Attribute offenlegen	60
7.6	Zuordnung Service zu Informationselemente.....	62
7.7	Zuständigkeiten für Geschäftsservices	63
8	IAM für das IoT	64
8.1	Spezielle Eigenschaften von Dingen.....	64

8.2	Auswirkung auf die IAM Informationsarchitektur	65
8.3	Auswirkung auf die IAM Geschäftsservices	67
9	Privacy	68
9.1	Anforderungen an Sicherheit und zum Schutz der Privatsphäre	68
9.2	Verwaltung und Verarbeitung von Daten von Subjekten	69
9.2.1	Minimierung der Datensammlung und des Datenbestands	70
9.2.2	Verhindern von Profiling	70
9.2.3	Kenntnisnahme und Einwilligung	70
9.2.4	Nutzungsbeschränkung	70
9.2.5	Regress	70
9.2.6	Datenschutz- und Risikoanalyse	70
9.2.7	Datenschutzmassnahmen	70
10	Haftungsausschluss/Hinweise auf Rechte Dritter	71
11	Urheberrechte	71
	Anhang A – Referenzen & Bibliographie	72
	Anhang B – Mitarbeit & Überprüfung	73
	Anhang C – Abkürzungen	74
	Anhang D – Glossar	75
	Anhang E – Identity Federation Modelle	76
E.1	– RP-zentriertes Modell	76
E.2	– Vermittler-zentriertes Modell	76
E.3	– Cross Domain Modell	77
E.4	– Zentralisierte Metadaten und Discovery	78
E.5	– Hub-'n'-Spoke Modell	78
E.6	– Proxied Federation	79
	Anhang F – Änderungen gegenüber Version 2.00	81

Abbildungsverzeichnis

Abbildung 1 IAM im Überblick	9
Abbildung 2: Einordnung des eCH-0107 Standards	10
Abbildung 3 Zusammenarbeit von Rollen in einem föderierten IAM-System.....	17
Abbildung 4 Abbildung von Stakeholdern auf Rollen	18
Abbildung 5: Sicht des Leistungsbezügers	18
Abbildung 6 Sicht des Leistungserbringers.....	19
Abbildung 7 Sicht der Führung des gesamten IAM-Systems	20
Abbildung 8 Sicht des Regulars.....	20
Abbildung 9 Informationsmodell	29
Abbildung 10 Subjekt Definition.....	31
Abbildung 11 IAM-Prozesslandkarte	34
Abbildung 12 Zustandsdiagramm <i>Zugriff kontrollieren</i>	35
Abbildung 13 Geschäftsservices – Definitionszeit	48
Abbildung 14 Geschäftsservices – Laufzeit	53
Abbildung 15 Geschäftsservices – Übersicht.....	58
Abbildung 16 Prozessunterstützung <i>Subjekt authentifizieren</i>	59
Abbildung 17 Prozessunterstützung <i>Identität föderieren</i>	59
Abbildung 18 Prozessunterstützung <i>E-Identity autorisieren und Attribute offenlegen</i>	60
Abbildung 19 RP-zentriertes Modell	76
Abbildung 20 Vermittler-zentriertes Modell	77
Abbildung 21 Cross Domain Modell	77
Abbildung 22 Zentralisierte Metadaten und Discovery Service	78
Abbildung 23 Hub-'n'-Spoke Modell.....	79
Abbildung 24 Proxied Federation	80

Tabellenverzeichnis

Tabelle 1 Farbverwendung im Dokument	9
Tabelle 2 Übersicht des normativen Charakters der Kapitel	13
Tabelle 3 Anforderungen der Stakeholder an die Rollen	24
Tabelle 4 Beschreibung der Elemente des Informationsmodells	33
Tabelle 5 Beziehung zwischen Services und Semantik des Informationsmodells	62
Tabelle 6 Beziehung zwischen Geschäftsservices und Stakeholder	63

1 Status des Dokuments

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

2 Einleitung

2.1 Überblick

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

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

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

2.1.1 Einführung IAM

Die Kernelemente eines *IAM* sind für das Verständnis des Standards essentiell und werden daher in diesem Abschnitt kurz erläutert.

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

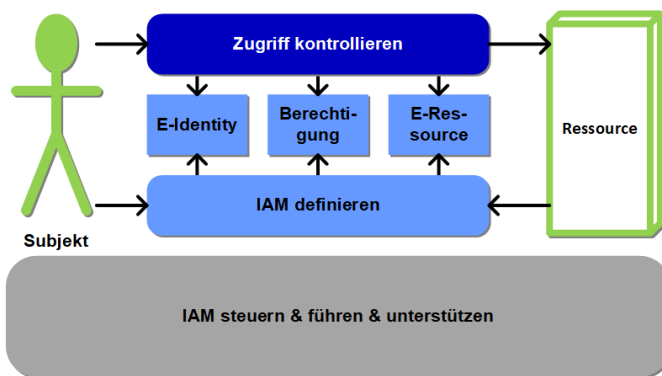


Abbildung 1 IAM im Überblick

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

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

Tabelle 1 Farbverwendung im Dokument

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

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

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

2.1.2 Anwendungsgebiet

Die Vision der Vernetzten Verwaltung und die damit verbundenen übergreifenden Prozesse im schweizerischen E-Government bedingen eine über Organisationsgrenzen hinweggreifende *Identitäts- und Berechtigungsverwaltung*. Der vorliegende Standard eCH-0107 bildet die Basis der IAM-Standardisierung. Dabei werden die Definitionen und Begriffe aus dem eCH-0122 [1], der die Architektur des E-Government Schweiz definiert, zu Grunde gelegt.

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

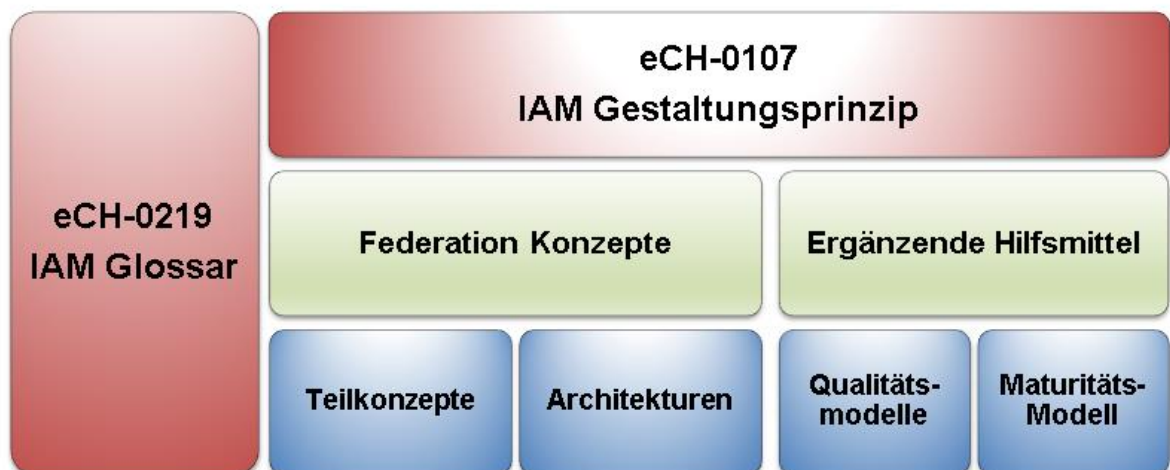


Abbildung 2: Einordnung des eCH-0107 Standards

Unter dem Standard eCH-0107 positionieren sich die Konzepte für föderierte IAM-Lösungen und ergänzende Hilfsmittel. Im IAM Glossar (eCH-0219 [2]) sind Begriffe definiert, die für alle eCH-Standards im Bereich IAM gültig sind. Die Konzepte sind konkrete Beschreibungen, wie ein IAM-Lösungsvorschlag aussieht, und beinhalten Teilkonzepte und Architekturen, die für die Umsetzung berücksichtigt werden müssen. Daneben werden den Konzepten Hilfsmittel zur Seite gestellt, die ergänzende Informationen zur Verfügung stellen und die für mehr als ein Konzept relevant sind. Die dargestellten Qualitäts- und Maturitätsmodelle sind Beispiele für Hilfsmittel und sind nicht abschliessend.

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

2.1.3 Föderiertes IAM

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

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

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

Beim föderierten IAM, im Gegensatz zum replizierenden IAM (siehe [2]), im E-Government stellen Behörden Ressourcen den Subjekten ihren internen (andere Behörden der Schweiz) oder externen Partnern (Personen, Unternehmen, Organisationen oder Behörden anderer Staaten) zur Verfügung, mit denen definierte Leistungen aus dem Bereich ihrer Zuständigkeit online verfügbar gemacht werden. Diese Ressourcen sollen für Subjekte der eigenen Domäne(n) und für Subjekte mit E-Identities anderer Domänen zugreifbar sein. Eine Behörde kann somit Relying Party aber auch u.U. gleichzeitig IAM-Dienstanbieter sein.

2.1.4 Abgrenzung

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

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

2.1.5 Vorteile

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

Dieser Standard erzielt folgende Vorteile:

- Ein 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, Rollen, Prozesse, Informationsmodell, Geschäftsservices) im organisationsübergreifenden Anwendungsszenario ist definiert.
- Mögliche Konzepte für Identity Federations sind dargestellt.
- Die Auswirkungen auf das *IAM* bei Ausdehnung des Wirkungsbereiches auf das Internet of Things werden diskutiert.
- Neu hinzugekommen sind verschärfte Anforderungen zum Schutz der Privatsphäre des Subjektes.
- 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 sieben Kapitel, die nachfolgend kurz beschreiben werden.

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

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

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

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

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

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

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

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

2.3 Normativer Charakter der Kapitel

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

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

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

Tabelle 2 Übersicht des normativen Charakters der Kapitel

3 Rollen und Stakeholder

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

3.1 Rollen in IAM

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

Relying Party	<p>Die <i>Relying Party</i> vertritt die Interessen der <i>Ressource</i> im IAM-System. Sie nutzt IAM-Geschäftsservices und verarbeitet Informationen von <i>IAM-Dienstleistern</i> für den Schutz ihrer <i>Ressourcen</i>. Sie braucht zur Beurteilung der <i>Berechtigung</i> eines Ressourcenzugriffs nähere Informationen (berechtigungsrelevante Eigenschaften) zu einem <i>Subjekt</i>, dessen <i>E-Identity</i> und den Kontext des Zugriffs (Lokation, Zeitpunkt, Sicherheitsniveau etc.)</p> <p>Primärer Stakeholder: Leistungserbringer</p>
---------------	---

IAM-Dienstanbieter	<p>Der <i>IAM-Dienstanbieter</i> ist verantwortlich für den Betrieb¹ von einem oder mehreren IAM-Geschäftsservices gemäss Kapitel 7. Es können die folgenden Spezialisierungen unterschieden werden, die aber oft gemeinsam implementiert werden.</p> <p>Die <i>Registrierungsstelle (RA)</i> erfasst und prüft die E-Identities der Subjekte.</p> <p>Der <i>Credential Service Provider (CSP)</i> vergibt und verwaltet Authentifizierungsmittel für E-Identities.</p> <p>Der <i>Identity Provider (IdP)</i> überprüft zur Laufzeit die E-Identities der Subjekte.</p> <p>Die <i>Attribut-Autorität (AA)</i> verwaltet die Attribute der Subjekte und gibt Attributbestätigungen aus.</p> <p>Ein <i>Vermittler</i> bietet gemeinsame Dienste, wie Metadatenverwaltung, IdP-Discovery, Identity Linking oder Transformation des Authentifizierungs- und Attributbestätigung, für alle andere IAM-Dienstanbieter und Relying Parties in einer Identity Federation an.</p> <p>Primärer Stakeholder: Dienstanbieter</p>
--------------------	---

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

IAM-Regulator	<p>Der <i>IAM-Regulator</i> (oder die <i>IAM-Steuerung</i>) definiert die rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen, innerhalb derer das IAM abgewickelt werden muss. Er berücksichtigt dabei die Interessen aller Stakeholder und beteiligt alle anderen Rollen in geeigneter Weise an der Definition.</p> <p>IAM-Regulatoren existieren in verschiedenen Formen und können sowohl innerhalb einer einzigen Organisation, aber auch organisationsübergreifend agieren.</p> <p>Die <i>IAM-Steuerung</i> definiert die IAM-Policy für ein organisationsinternes oder -externes IAM-System bzw. von IAM-Geschäftsservices.</p> <p>Der <i>Gesetzgeber</i> definiert die rechtlichen Rahmenbedingungen.</p> <p>Das <i>Standardisierungsgremium</i> erstellt Normen und Richtlinien für die prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen.</p> <p>Primärer Stakeholder: Regulator</p>
IAM-Führung	<p>Die <i>IAM-Führung</i> ist verantwortlich für das Managen eines IAM-Systems oder von Teilen davon (IAM-Dienstanbieter oder Relying Party).</p> <p>Die <i>IAM-Führung des Gesamtsystems</i> managt die teilnehmenden IAM-Dienstanbieter und Relying Parties analog ITIL [ref] oder IT4IT [ref] 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 Relying Parties geschehen.</p> <p>Primärer Stakeholder: Führung</p>
IAM-Support	<p>Der <i>IAM-Support</i> ist verantwortlich für alle Aktivitäten zum Auffinden und Lösen von Problemen.</p> <p>Primärer Stakeholder: Dienstanbieter</p>
Subjekt	<p>Eine <i>natürliche Person</i>, eine <i>Organisation (juristische Person)</i>, ein <i>Service</i> oder ein <i>Ding</i>, das auf eine <i>Ressource</i> zugreift oder zugreifen möchte. Ein Subjekt wird durch <i>E-Identities</i> repräsentiert.</p> <p>Primärer Stakeholder: Leistungsbezüger</p>

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

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

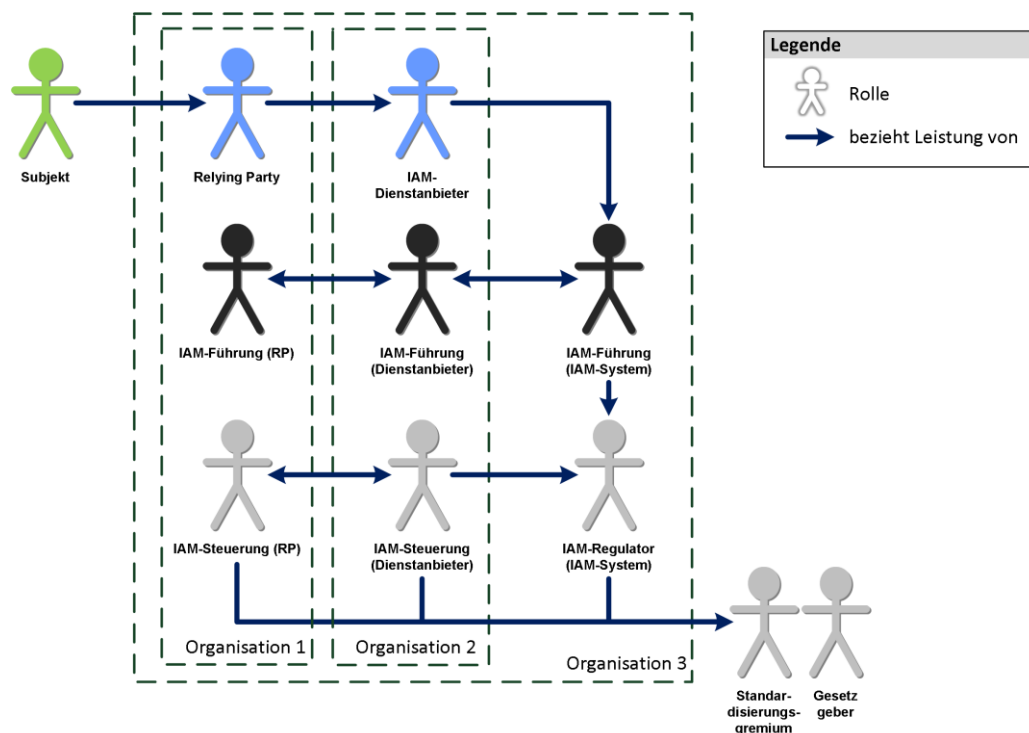


Abbildung 3 Zusammenarbeit von Rollen in einem föderierten IAM-System

3.2 Stakeholder im IAM

Die Stakeholder sind Personen, Gruppen von Personen oder Organisationen, die gemeinsame Interessen im IAM haben. Stakeholder haben Anforderungen (siehe Kapitel 4) an die verschiedenen Rollen in einem IAM-System.

Die Rollen in einem IAM-System (siehe Kapitel 3.1) werden durch die Stakeholder motiviert. In Abbildung 4 ist aufgezeigt, welcher Stakeholder welche Rollen einnehmen kann, dabei wird zwischen Hauptrollen, Nebenrollen² und optionalen Rollen unterschieden.

² Bei einer Selbstregistrierung übernimmt das Subjekt die Rolle der RA und ggf. der AA, die Überprüfung der Identität des Subjektes und seiner Attribute entfällt.

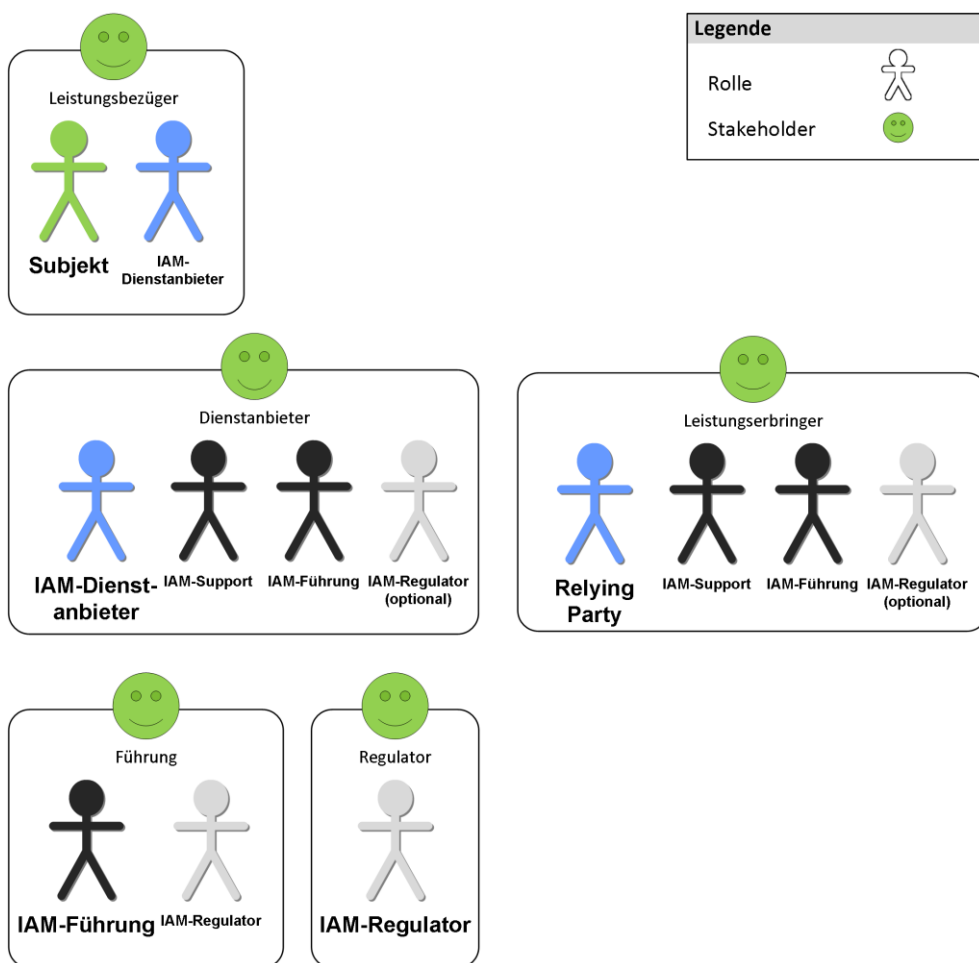


Abbildung 4 Abbildung von Stakeholdern auf Rollen

Leistungsbezüger (LB)

Der Leistungsbezüger möchte jederzeit, kostengünstig und einfach eine fachliche Leistung³ online in Anspruch nehmen. Er fordert Unterstützung bei Problemen (z.B. Identitätsdiebstahl) und erwartet Konformität mit gesetzlichen Regelungen.

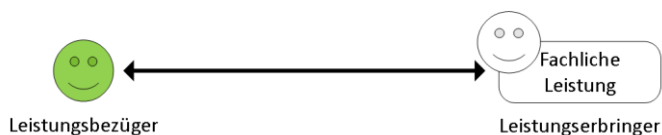


Abbildung 5: Sicht des Leistungsbezügers

Abbildung 6 zeigt die Sicht des Leistungsbezügers auf das Gesamtsystem. Der Leistungsbezüger möchte vorrangig eine fachliche Leistung eines Leistungserbringers in Anspruch neh-

³ Die hier erwähnte fachliche Leistung ist z.B. die Bestellung einer Funklizenz oder einer Parkkarte, nicht eine IAM-Leistung von einem Dienstanbieter.

men. Das verwendete IAM-System ist für ihn zweitrangig und nur Mittel zum Zweck sein Ziel zu erreichen.

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

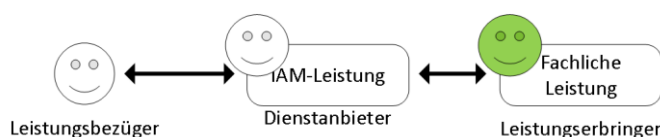


Abbildung 6 Sicht des Leistungserbringers

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

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

Führung	Die Führung möchte problemlos ein IAM-System, das allen Stakeholdern gerecht wird, und die daran beteiligten IAM-Dienstanbieter und Relying Parties managen sowie den zuverlässigen Betrieb des IAM-Systems garantieren.
----------------	--

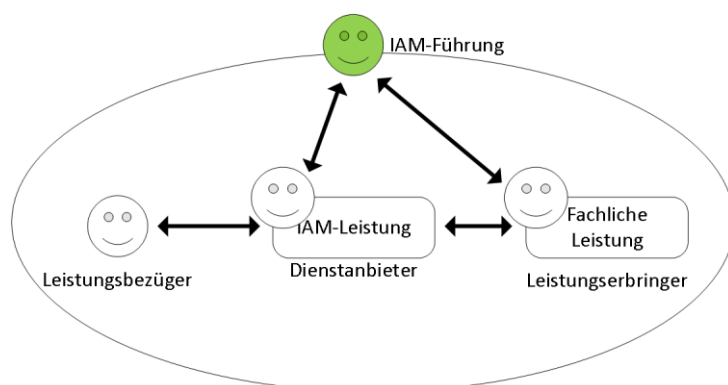


Abbildung 7 Sicht der Führung des gesamten IAM-Systems

Abbildung 7 zeigt die Sicht der Führung des gesamten IAM-Systems. Die Führung möchte das IAM-System und die daran beteiligten Leistungserbringer und Dienstleister effizient managen, um die Implementierung zu erleichtern und den zuverlässigen Betrieb zu garantieren. Die Führung vertritt dabei die Anforderungen aller Stakeholder im IAM-System, auch die des Subjektes.

Regulator	Der Regulator möchte die Interoperabilität, Robustheit und Sicherheit des IAM-Gesamtsystems sicherstellen.
-----------	--

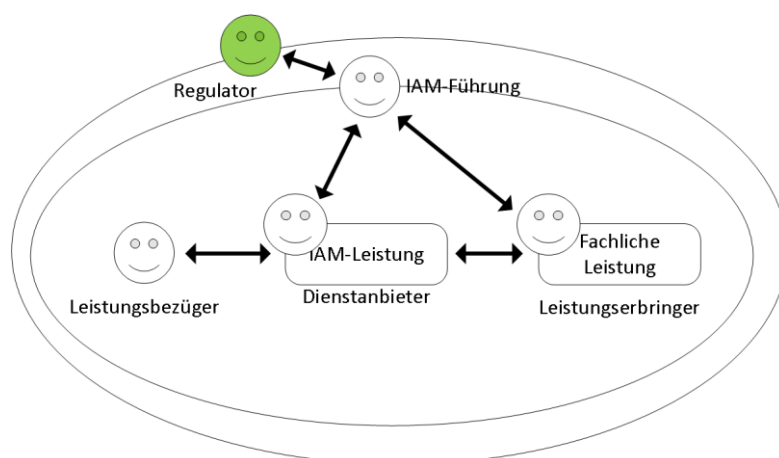


Abbildung 8 Sicht des Regulators

Abbildung 8 zeigt die Sicht des Regulators. Die Regulator möchte durch die Schaffung entsprechender Rahmenbedingungen (Gesetze, Standards, Fördermassnahmen, etc.) den Einsatz von förderierten IAM-Systemen organisationsübergreifend fördern und gleichzeitig eine hohe Qualität nicht funktionaler Qualitätsmerkmale, wie z.B. Interoperabilität, Zuverlässigkeit und Sicherheit, erreichen.

4 Anforderungen

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

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

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

4.1 Grundprinzipien eines föderierten IAM-Systems

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

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

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

4.2 Anforderungen an das föderierte IAM-System

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

Bezeichnung	Typ	Beschreibung	Begründung / Prinzip
IAM-1	T/A	Das IAM SOLLTE auf einer international interoperablen Architektur basieren. [3]	Interoperabilität, Prinzip-10
IAM-1.1	T/A	Das IAM MUSS in andere IAM (auch auf internationaler Ebene) einfach integrierbar sein.	Interoperabilität, Prinzip-10
IAM-1.2	T/A	Das IAM MUSS die Fähigkeit haben bestehende IAM-Lösungen einfach integrieren.	Interoperabilität, Prinzip-10
IAM-2	A/D	Die <i>Authentifikation</i> und <i>Berechtigung</i> für den Zugang SOLLTEN auf standardisierten Authentifizierungsmitteln und <i>Attributen</i> basieren.	Interoperabilität Prinzip-10
IAM-3	T/A	Die IAM-Systeme MÜSSEN modular und SOLLTEN skalierbar aufgebaut sein.	Kosten, Wiederverwendbarkeit, Wartbarkeit

Bezeichnung	Typ	Beschreibung	Begründung / Prinzip
			Prinzip-10
IAM-4	A	Die technischen Services MÜSSEN über standardisierte Schnittstellen zusammenarbeiten, welche offene Standards gemäss ihrer Spezifikation (z.B. SAML, OIDC)) benutzen.	Interoperabilität Prinzip-10
IAM-5	T	Die je nach Schutzbedürfnissen notwendigen, unterschiedlich starken Authentisierungs- und Autorisierungsverfahren KÖNNEN auf derselben IAM-Infrastruktur realisiert werden.	Interoperabilität, Kosten, Wiederverwendbarkeit Prinzip-10
IAM-6	D	Die Menge der E-Identities, Authentifizierungsmittel und Attribute SOLLTE minimal gehalten und womöglich konsolidiert werden.	Kosten, Benutzerfreundlichkeit Prinzip-9
IAM-7	A	Der Transport der Daten MUSS zwischen den IAM-Diensteanbietern und RPs auf Protokollebene abgesichert sein (z.B. TLS).	Sicherheit, Schutz der Privatsphäre Prinzip-8
IAM-8	A	Die technischen Services, welche Authentifizierungs- und Attributbestätigungen erstellen oder konsumieren, MÜSSEN ihre Zeit mit einem zugelassenen Zeitserver synchronisieren.	Interoperabilität, Sicherheit, Robustheit
IAM-9	B/A	Die von den Geschäftsservices erstellten Authentifizierungs- und Attributbestätigungen MÜSSEN auf ihre Authentizität und Integrität überprüft werden können (z.B. mithilfe der Signatur oder durch Rückfragen).	Sicherheit, Trust Prinzip-6
IAM-10	A/B	Es MUSS gewährleistet sein, dass jederzeit nachvollzogen und nachgewiesen werden kann, welches <i>Subjekt</i> wann auf welche <i>Ressource</i> zugegriffen hat.	Nachvollziehbarkeit, Prinzip-8
IAM-11	B/A/T	Es MUSS sichergestellt werden (z.B. durch Verschlüsselung der Daten), dass Authentifizierungs- und Attributbestätigungen nur von berechtigten Instanzen gelesen werden können.	Schutz der Privatsphäre, Prinzip-8

4.3 Anforderungen der Stakeholder

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

Rollen						
Stakeholder	Subjekt	Relying Party	IAM-Dienst-anbieter	IAM-Führung	IAM-Support	IAM-Regulator

Leistungsbezüger		A	A		A	A
Leistungserbringer	A		A	A	A	A
Dienstanbieter	(A)		A	A		A
Führung		A	A	A	A	A
Regulator				A		A

Tabelle 3 Anforderungen der Stakeholder an die Rollen

4.3.1 Anforderungen des Leistungsbezügers

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

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
LB-1	A/D	Wenn das Subjekt auf schützenswerte Ressource zugreift, MUSS sich das Subjekt authentisieren.	Authentifizierung als Grundlage der Autorisierung, Datenschutz	Prinzip-4
LB-1.1	B/A/T	Das Subjekt MUSS sich minimal mit der geforderten Vertrauensstufe authentisieren. Es DARF sich mit einer höheren Vertrauensstufe authentisieren.	Kosten, Benutzerfreundlichkeit, Schutz der Privatsphäre	Prinzip-7, Prinzip-5
LB-2	D	Ein eindeutiger Identifikator gegenüber der Ressource MUSS nur dann vom Subjekt verwendet werden, wenn die Nutzung der Ressource das fordert.	Schutz der Privatsphäre	Prinzip-7
LB-2.1	D	Einen zufälligen Identifikator (z.B. eine Transient ID) gegenüber der Ressource SOLLTE vom Subjekt bei der Nutzung verwendet werden.	Schutz der Privatsphäre (Unlinkability)	Prinzip-7
LB-3	D	Es MÜSSEN nur die Attribute vom Subjekt bei der Authentifikation übermittelt werden, die zur Berechtigung der Ressource notwendig sind.	Need-to-Know-Prinzip, Schutz der Privatsphäre	Prinzip-7
LB-3.1	D	Weitere Attribute KÖNNEN vom Subjekt übermittelt werden, wenn die Ressource diese für die Funktionserfüllung benötigt.	Schutz der Privatsphäre	Prinzip-7
LB-4	B/A	Die IAM-Dienstanbieter (IdP, AA), welche die E-Identities und Attribute verwaltet, KÖNNEN vom Subjekt gewählt werden.	Selbstbestimmung, Wahlfreiheit	Prinzip-2

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
LB-5	D	Die Anzahl der benötigten E-Identities, die das Subjekt haben muss, SOLLTE möglichst geringgehalten werden.	Kosten, Benutzerfreundlichkeit, Kontextabdeckung	IAM-6
LB-6	B	Die Anzahl von Authentifizierungsmittel verschiedener Qualitäten, KANN vom Subjekt selbst bestimmt werden.	Selbstbestimmung, Wahlfreiheit	
LB-7	B	Das Authentifizierungsmittel (während der Authentisierung), welches die minimal geforderte Qualität erfüllt, KANN vom Subjekt selbst bestimmt werden.	Selbstbestimmung, Wahlfreiheit	Prinzip-2
LB-8	B	Die Beschaffung von E-Identities und Authentifizierungsmitteln SOLLTE einfach und günstig sein.	Kosten	
LB-9	A	Die Benutzung von E-Identities und Authentifizierungsmitteln SOLLTE einfach und unkompliziert sein.	Benutzerfreundlichkeit	
LB-10	B	Ein anderes Subjekt SOLL die Fähigkeit haben kontextbezogen und zeitlich begrenzt als Stellvertreter zu handeln.	Delegation von Berechtigungen	
LB-11	B/A	Der Weitergabe von Attributen MUSS das Subjekt zustimmen können, ausser das Recht zur Weitergabe ist gesetzlich verankert oder anderswo geregelt.	Schutz der Privatsphäre	Prinzip-8
LB-12	B/A	Das Subjekt WILL Unterstützung bei Vermeidung und Recovery des Missbrauchs einer E-Identity erhalten. [3]	Benutzerfreundlichkeit, Sicherheit	
LB-13	B/A/T	<i>IAM-Dienstleister MÜSSEN</i> das vernünftig Machbare unternehmen, um den Missbrauch der <i>E-Identity</i> des <i>Subjekts</i> zu verhindern. [3]	Schutz der Privatsphäre, Sicherheit	LE-9, Führ-3
LB-14	A	Der IAM-Support MUSS das Subjekt beim Lösen von Problemen, die eine erfolgreiche Nutzung der Ressource verhindern, unterstützen.	Benutzerfreundlichkeit	Führ-6
LB-15	A	Die vom Subjekt freigegebenen Attribute SOLLTEN nur von den berechtigten Instanzen gelesen werden können.	Schutz der Privatsphäre	Prinzip-8, IAM-11
LB-16	B	Die Nutzung der Ressource ist jederzeit möglich.	Verfügbarkeit	

4.3.2 Anforderungen der Leistungserbringer

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

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
LE-1	B/A/T	Der Missbrauch von <i>Ressourcen</i> SOLLTE ausgeschlossen sein.	Sicherheit	
LE-2	A	Der <i>Zugriff</i> auf schützenswerte <i>Ressourcen</i> MUSS auf autorisierte <i>Subjekte</i> eingeschränkt sein.	Sicherheit (Access Control)	Prinzip-4
LE-2.1	A	Falls das <i>Subjekt</i> keine Rechte für die aufzurufende schützenswerte <i>Ressource</i> hat, MUSS der Aufruf an die <i>E-Ressource</i> verworfen werden und/oder entsprechend umgeleitet werden.	Sicherheit, Benutzerfreundlichkeit	
LE-3	B/A	Der Aufwand für die Verwaltung der <i>E-Ressourcen</i> SOLLTE minimal sein.	Kosten	
LE-4	B/A	Der Aufwand für die Verwaltung der <i>Berechtigungen</i> (<i>Zugangsregeln</i> und <i>Zugriffsrechte</i>) SOLLTE minimal sein.	Kosten	
LE-5	D	Die Menge der unterstützten <i>E-Identities</i> und <i>Attribute</i> MUSS minimal gehalten und SOLLTE womöglich konsolidiert werden.	Kosten	IAM-6, LB-5
LE-6	B	<i>E-Identities</i> und <i>Attribute</i> MÜSSEN bei Veränderungen zeitnah gepflegt werden.	Aktualität	
LE-7	A	Authentifizierungs- und Attributbestätigungen KÖNNEN durch <i>IAM-Dienstanbieter</i> unterschiedlicher Qualität ausgestellt werden. [3]	Interoperabilität	Prinzip-2
LE-8	B	Für <i>Subjekte</i> SOLLTE ein eindeutiger <i>Identifikator</i> verwendet werden. Im Idealfall kann es sich um einen staatlichen Identifikator handeln. [3]	Wiedererkennung des Subjekts	
LE-9	B	Das <i>Subjekt</i> und die <i>IAM-Dienstanbieter</i> MÜSSEN den Verdacht eines Missbrauchs einer <i>E-Identity</i> melden. [3]	Sicherheit	
LE-10	B/A/T	<i>IAM-Dienstanbieter</i> MÜSSEN das vernünftig Machbare unternehmen, um den Missbrauch der <i>E-Identity</i> des <i>Subjekts</i> zu verhindern. [3]	Schutz der Privatsphäre, Sicherheit	LB-13

4.3.3 Anforderungen der Dienstanbieter

Dieser Abschnitt beschreibt die Anforderungen der Dienstanbieter.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
Dienst-1	B/A	Der Aufwand für die Administration der <i>E-Identities</i> (Authentifizierungsmittel und <i>Attribute</i>) SOLLTE minimal im Verhältnis zur angestrebten Qualität sein.	Kosten	LB-8
Dienst-2	D	Der Zusammenhang zwischen der <i>E-Identity</i> und den dazugehörigen <i>Authentifizierungsmitteln</i> MUSS zu jedem Zeitpunkt gewährleistet sein.	Nachvollziehbarkeit	IAM-10
Dienst-3	B	E-Identities und Attribute MÜSSEN bei Veränderungen zeitnah gepflegt werden.	Aktualität	

4.3.4 Anforderungen der Führung

Dieser Abschnitt beschreibt die Anforderungen der Führung.

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
Führ-1	B/A	Die IAM-Dienstanbieter und Relying Parties SOLLTEN sich auf eine standardisierte Menge von Authentifizierungsmitteln und Attributen einigen.	Interoperabilität, Benutzerfreundlichkeit, Führbarkeit	IAM-2, IAM-6
Führ-2	T	Die IAM-Dienstanbieter und Relying Parties MÜSSEN standardisierte Schnittstellen verwenden.	Interoperabilität	IAM-4
Führ-3	B/A	Die verschiedenen IAM-Dienstanbieter und die Relying Parties MÜSSEN zusammenarbeiten, um das Subjekt bei Vermeidung und Recovery des Missbrauchs seiner E-Identity zu unterstützen.	Benutzerfreundlichkeit, Sicherheit	LB-12, LB-13, LE-11
Führ-4	B/D	Die verschiedenen IAM-Dienstanbieter und die Relying Parties MÜSSEN zusammenarbeiten, so dass jederzeit nachvollziehen werden kann, welches <i>Subjekt</i> wann auf welche <i>Ressource</i> zugegriffen hat.	Nachvollziehbarkeit	IAM-10
Führ-5	B	Der IAM-Regulator MUSS die erforderlichen rechtlichen, prozessualen, organisatorischen/architektonischen und technischen Rahmenbedingungen für	Rechtskonformität, Sicherheit, Robustheit	Prinzip-8

Bezeichnung	Typ	Beschreibung	Begründung	Referenz
		das betroffene IAM-System definieren.		
Führ-5.1	B	Die verschiedenen IAM-Dienstleister und die Relying Parties SOLLTEN die vom IAM-Regulator definierten Rahmenbedingungen einhalten.	Rechtskonformität, Sicherheit, Robustheit	Prinzip-8
Führ-6	A	Der IAM-Support MUSS das Subjekt effizient, kundenfreundlich, günstig und nachvollziehbar beim Lösen von Problemen, die eine erfolgreiche Nutzung der Ressource verhindern, unterstützen.	Benutzerfreundlichkeit, Kosten	LB-14

4.3.5 Anforderungen des Regulators

Dieser Abschnitt beschreibt die Anforderungen der IAM-Regulatoren.

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

5 Informationsarchitektur

Nachstehendes Modell stellt die wichtigen Begriffe des *IAM* und ihre Beziehungen in einer Übersicht als UML-Klassendiagramm dar. Weil die Elemente des *IAM*-Informationsmodells an sehr vielen Orten (nicht nur im *IAM*) verwendet werden, ist es hier wichtig, differenzierte Begriffe zu verwenden, damit Syntax und Semantik für alle Beteiligten eindeutig und unmissverständlich definiert sind. Abbildung 9 zeigt das Informationsmodell zum organisationsübergreifenden IAM.

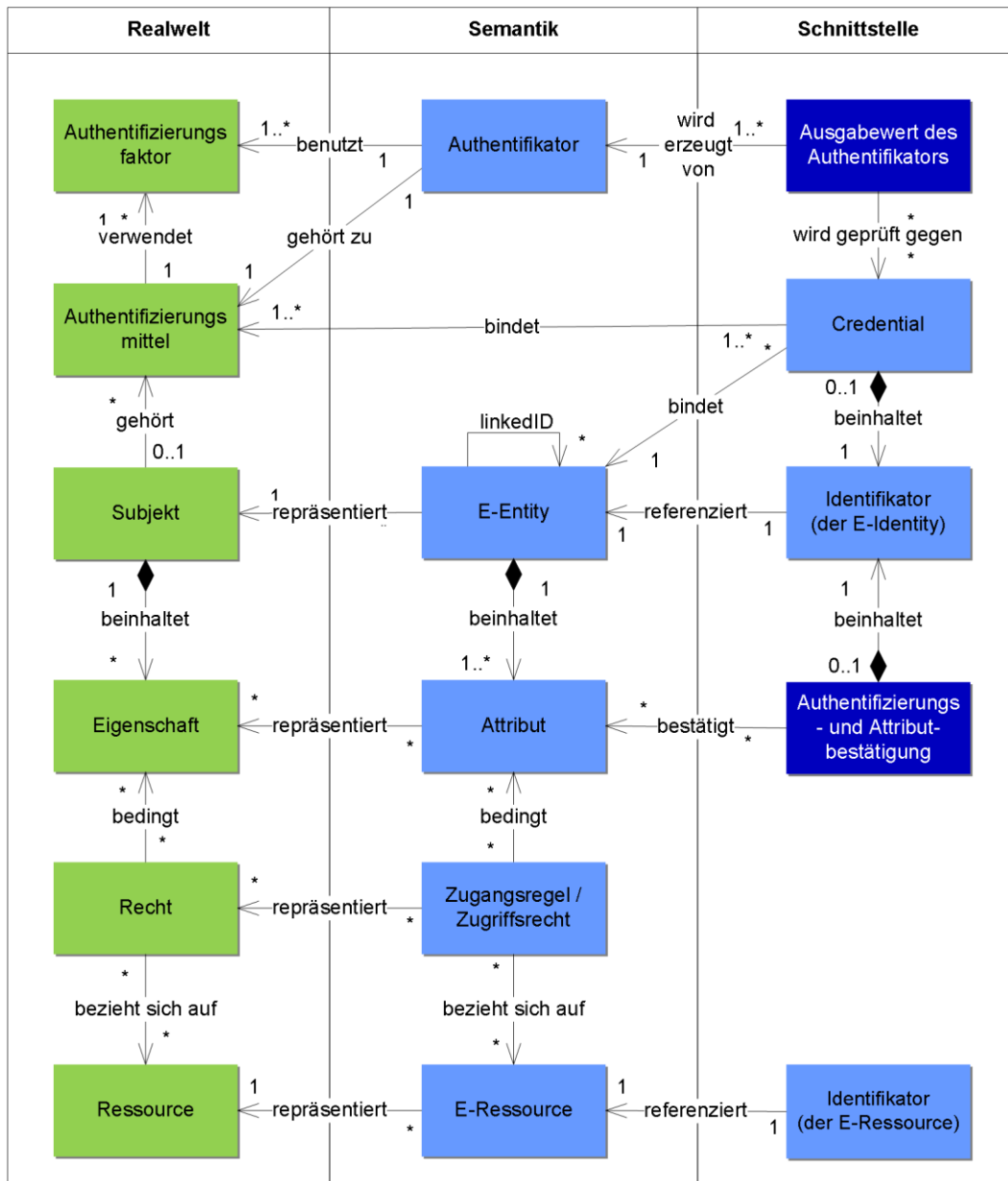


Abbildung 9 Informationsmodell

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

len Welt wesentlich sind, werden hier für unterschiedliche Elemente auch unterschiedliche Bezeichner verwendet. Das Informationsmodell in Abbildung 9 zeigt links (in grün) die Elemente der realen Welt, in der Mitte das semantische Modell (der Informationssysteme), und rechts die Schnittstellenobjekte, 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 kurz⁴ die in der Abbildung 9 vorkommenden Elemente und ihre Beziehungen.

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

⁴ Die vollständigen Beschreibungen mit Abbildungen und Beispielen sind im eCH-0219 [2] zu finden.

Subjekt

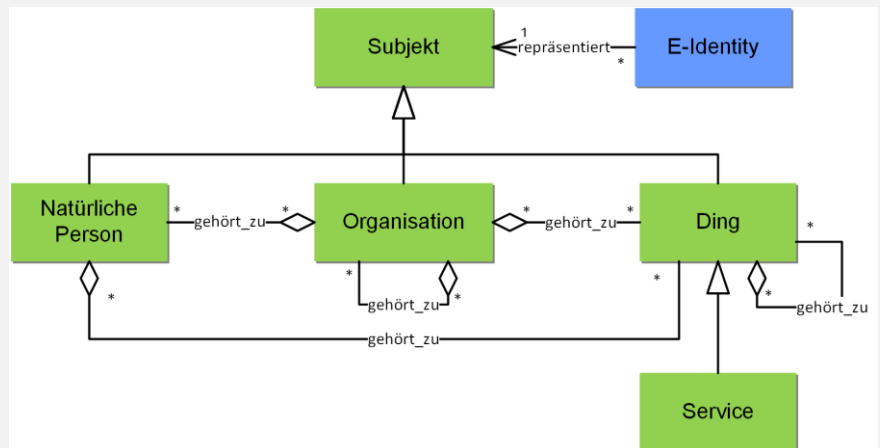


Abbildung 10 Subjekt Definition

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

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

Natürliche Personen können zu einer *Organisation* gehören.

Eine *Organisation* ist eine Gruppe aus mehreren natürlichen Personen. Eine Organisation kann (Unter-)Organisationen enthalten. Bei Organisationen wird zwischen *handelnden* und *nicht handelnden* Organisationen unterschieden. Handelnde Organisationen, z.B. Gruppen-Identitäten, können sich authentifizieren und Zugriff zu Ressourcen erhalten. Nicht handelnde Organisationen, wie z.B. juristische Personen, können sich nicht selbst authentifizieren, sondern nur über die dazugehörige natürliche Person.

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

Ein *Ding* ist eine existierende oder abstrakte Einheit, die eindeutig identifizierbar ist. Dinge können weitere Dinge enthalten. Ein Ding kann zu einer *Organisation* oder zu einer *natürlichen Person* gehören.

Ein *Service* ist ein spezielles Ding, das über ein *Netzwerk* erreichbar und darin digital identifizierbar ist.

Authentifizierungsmittel	Etwas, das ein <i>Subjekt</i> besitzt und unter seiner Kontrolle hat (ein kryptographischer Schlüssel, ein Geheimnis oder ein spezifisches Verhalten). Ein Authentifizierungsmittel kann einen (<i>single-factor authenticator</i>) oder auch mehrere unabhängige Authentifizierungsfaktoren (<i>multi-factor authenticator</i>) benutzen.
Authentifizierungsfaktor	Informationen und/oder Prozesse, die zur Authentifizierung eines <i>Subjektes</i> verwendet werden können. Authentifizierungsfaktoren können auf vier verschiedenen Merkmalen (besitzabhängig, kenntnisabhängig, inhärent oder verhaltensbasiert) oder Kombinationen davon beruhen.
Semantik	
E-Ressource	Digitale Repräsentation einer <i>Ressource</i> . Eine <i>E-Ressource</i> hat einen <i>Identifikator</i> (eindeutiger Name, oft URL/URI), welche innerhalb eines <i>Namensraumes</i> eindeutig einer <i>Ressource</i> zugewiesen werden kann.
Zugangsregel / Zugriffsrecht	Ressourcenverantwortliche definieren die <i>Zugangsregeln</i> und <i>Zugriffsrechte</i> für ihre <i>E-Ressourcen</i> . Die <i>Zugangsregeln</i> und <i>Zugriffsrechte</i> definieren die Bedingungen, unter denen ein <i>Subjekt</i> zu einer <i>Ressource</i> Zugang erhält (<i>Grobautorisierung</i>) und auf sie zugreifen darf (<i>Feinautorisierung</i>), z.B. nach erfolgreicher Authentifizierung und Bestätigung bestimmter <i>Attribute</i> .
Attribut	Semantisches Abbild einer einem <i>Subjekt</i> zugeordneten <i>Eigenschaft</i> , die das <i>Subjekt</i> näher beschreibt. Der <i>Identifikator</i> ist ebenfalls ein speziell verwendetes <i>Attribut</i> .
E-Identity	Repräsentation eines <i>Subjekts</i> . Eine <i>E-Identity</i> (<i>digitale Identität</i>) hat einen <i>Identifikator</i> (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen <i>Attributen</i> , welche innerhalb eines <i>Namensraumes</i> (und damit einer <i>Domäne</i>) eindeutig einem <i>Subjekt</i> zugewiesen werden können. Ein <i>Subjekt</i> kann mehrere <i>E-Identities</i> haben. ⁵

⁵ Die Aussage gilt (im Rahmen von eCH-0107) für organisationsübergreifende Systeme. Es wird allerdings empfohlen, bezüglich Eindeutigkeit auch organisationsintern keine Einschränkungen zu machen.

linkedID (Relation)	Im organisationsübergreifenden Kontext erlaubt die Relation <i>linkedID</i> , E-Identities aus verschiedenen <i>Domänen</i> miteinander in Beziehung zu setzen. <i>E-Identities</i> können mit <i>linkedIDs</i> 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 <i>Broker Service</i>).
Authentifikator	Funktionales Abbild des <i>Authentifizierungsmittels</i> der Realwelt. Mit der Funktion eines Authentifikators wird aus einem Eingabewert und einem geheimen Wert ein Ausgabewert erzeugt.
Schnittstelle	
Authentifizierungs- und Attributbestätigung	Eine Bestätigung der erfolgreichen <i>Authentifikation</i> eines <i>Subjektes</i> (<i>Authentifizierungsbestätigung</i> , <i>Authentication Assertion</i>) oder eine Bestätigung eines Wertes eines <i>Attributs</i> (<i>Attribute Assertion</i>). Enthält einen <i>Identifikator</i> .
Identifikator	Eine Zeichenkette, welche eine <i>E-Identity</i> oder eine <i>E-Ressource</i> innerhalb eines <i>Namensraumes</i> (<i>Domäne</i>) eindeutig bezeichnet.
Credential	Menge von Daten dar, mit der eine <i>E-Identity</i> an ein <i>Authentifizierungsmittel</i> gebunden wird, welches vom <i>Subjekt</i> besessen und kontrolliert wird.
Ausgabewert des Authentifikators	Wird durch eine mathematische Funktion (<i>Authentifikator</i> oder <i>Authentifizierungsfunktion</i>) aus einem geheimen Wert (z.B. privater Schlüssel), einem oder mehreren optionalen Aktivierungswerten (z.B. PIN oder biometrischer Informationen), und einem oder mehreren optionalen Eingabewerten (z.B. Zufallswerten oder Challenges) generiert.

Tabelle 4 Beschreibung der Elemente des Informationsmodells

6 Prozesse

Abbildung 11 zeigt eine Übersicht über die Geschäftsprozesse. Sie dient zur Veranschaulichung der Tätigkeiten, welche für eine erfolgreiche Kooperation zwischen den Rollen in einem IAM-System (siehe Definitionen in Kapitel 3.1) notwendig sind. Die blau dargestellten Prozesse bilden die Kernprozesse, die grau dargestellten bilden die Führungsprozesse und die Steuerungsprozesse.

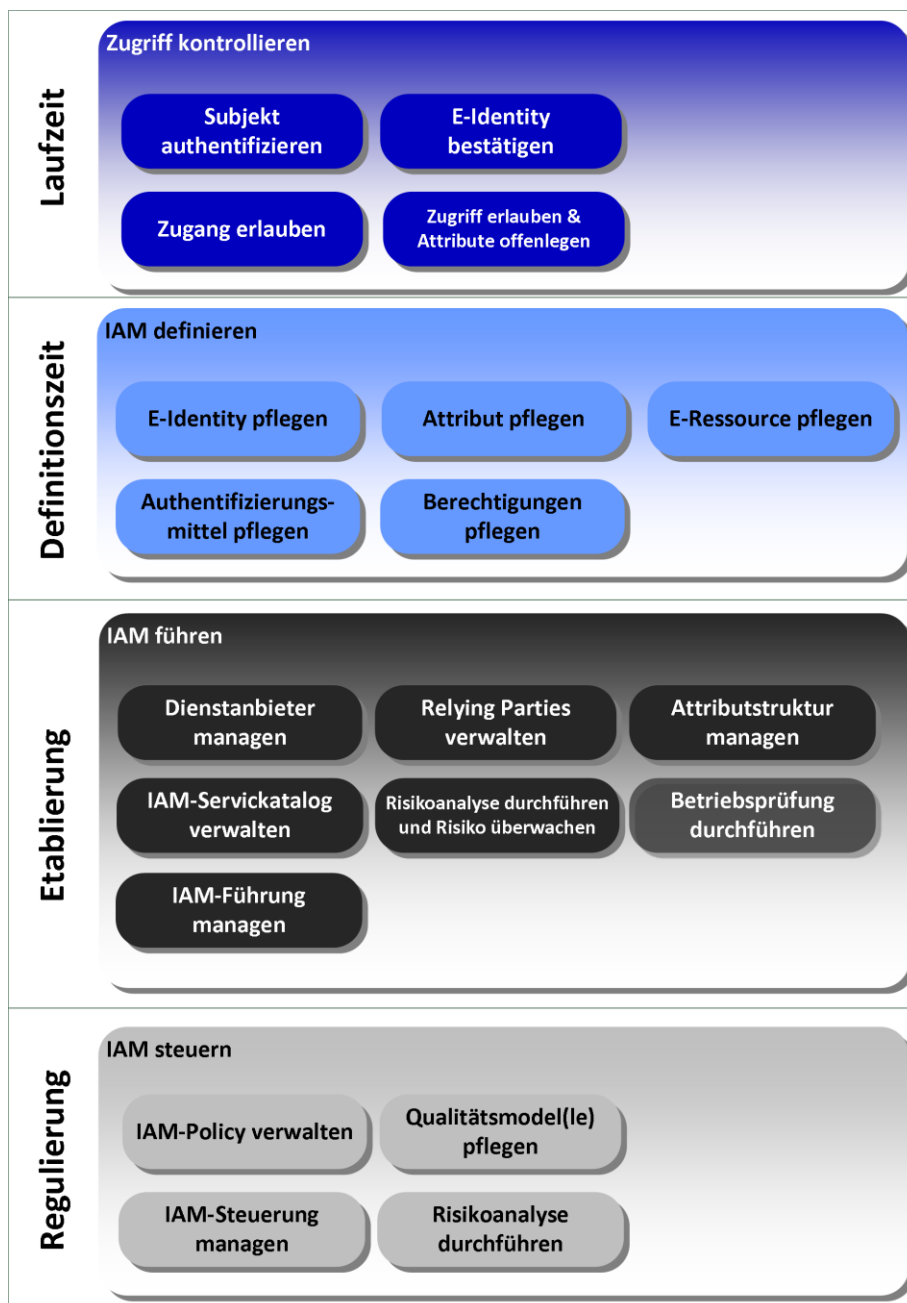


Abbildung 11 IAM-Prozesslandkarte

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

6.1 Zugriff kontrollieren (Laufzeit)

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

Die Teilprozesse von *Zugriff kontrollieren* bauen in einer festgelegten Reihenfolge aufeinander auf (siehe Abbildung 12).

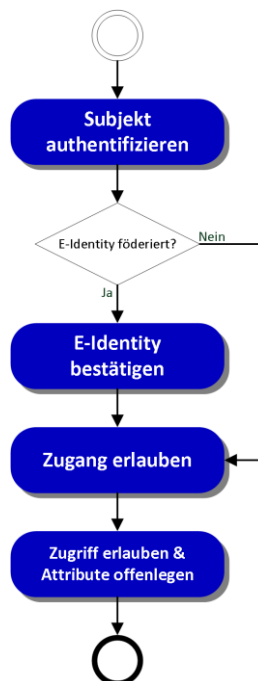


Abbildung 12 Zustandsdiagramm *Zugriff kontrollieren*

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

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 <i>E-Identity</i> eines <i>Subjekts</i> durch einen Identity Provider.
--------------------------	--

Zugehörige Rolle: IdP

Tätigkeiten:

- Das *Subjekt* verwendet ein ihm zur Verfügung gestelltes und unter seiner Kontrolle befindliches *Authentifizierungsmittel*.
- Das *Authentifizierungsmittel* generiert mit Hilfe des *Authentifikators* einen Ausgabe- wert aus den Eingaben des Subjekts (Geheimnis und optional anderen Eingabewer- ten).
- 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 und das Subjekt ist authentifiziert.

6.1.2 E-Identity bestätigen

E-Identit bestätigen	Bestätigung der E-Identity durch den IdP oder Vermittler.
----------------------	---

Zugehörige Rolle: IdP oder Vermittler

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

Tätigkeiten durch IdP:

- Der IdP überprüft, ob die RP berechtigt ist, eine Authentifizierungsbestätigung anzu- fordern.
- (optional) Der IdP holt das Einverständnis des Subjekts ein, die Authentifizierungsbe- stätigung an den aufrufenden Service (RP) zu übermitteln.
- Der IdP erzeugt Authentifizierungsbestätigung mit Zeitstempel, Signatur und optiona- ler Verschlüsselung.
- Der IdP übergibt die Authentifizierungsbestätigung an die RP.
- Die RP überprüft die Aktualität und Authentizität der Authentifizierungsbestätigung.
- In Abhängigkeit der verlangten Sicherheitsstufe muss die RP das Subjekt nach einer bestimmten Zeitdauer (unabhängig von ihren eigenen Richtlinien) erneut durch den IdP authentifizieren lassen (Re-Authentifizierung).

Tätigkeiten durch Vermittler:

- Der Vermittler überprüft, ob die RP berechtigt ist, eine Authentifizierungs- und Attri- butbestätigung anzufordern.
- (optional) Attributaggregation: Der Vermittler aggregiert die angeforderten Attribute.

- (optional) Der Vermittler holt das Einverständnis des Subjekts ein, die Authentifizierungs- und/oder Attributbestätigung an den aufrufenden Service (RP) zu übermitteln.
- Der Vermittler erzeugt eine Authentifizierungsbestätigung mit Zeitstempel, Signatur und optionaler Verschlüsselung.
- (optional) Der Vermittler erzeugt eine Attributbestätigung mit Zeitstempel, Signatur und optionaler Verschlüsselung.⁶
- Der Vermittler übergibt die Authentifizierungsbestätigung an die RP.
- (optional) Der Vermittler übergibt die Attributbestätigung an die RP.
- Die RP überprüft die Aktualität und Authentizität der Authentifizierungs- und Attributbestätigung.
- In Abhängigkeit der verlangten Sicherheitsstufe muss die RP das Subjekt nach einer bestimmten Zeitdauer (unabhängig von ihren eigenen Richtlinien) erneut durch den Vermittler authentifizieren lassen (Re-Authentifizierung).

6.1.3 Zugang erlauben

Zugang erlauben	Grobautorisierung anhand der Zugangsregeln.
-----------------	---

Zugehörige Rolle: Vermittler oder RP

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

Tätigkeiten:

- Vorbedingung einer *Autorisierung* ist die erfolgreiche *Authentifizierung* des *Subjekts*.
- Die zugehörige Rolle ermittelt die *Zugangsregeln* und für den *Zugang* auf die *E-Ressource*.
- Die zugehörige Rolle überprüft, ob der *Zugang* autorisiert ist.
- Die zugehörige Rolle erlaubt den *Zugang*.

6.1.4 Zugriff erlauben und Attribute offenlegen

Zugriff erlauben und Attribute offenlegen	Prüfen der <i>Zugriffsberechtigung</i> einer <i>autorisierten E-Identity</i> auf eine <i>E-Ressource</i> und Erteilen des <i>Zugriffs</i> auf eine <i>E-Ressource</i> zur Laufzeit.
	Offenlegen von Attributen des Subjektes.

Zugehörige Rolle: RP

⁶ Die Authentifizierungs- und Attributbestätigungen werden im Normalfall gemeinsam vom Vermittler erzeugt und an die RP übergeben.

Tätigkeiten:

- Vorbedingung für einen Zugriff ist eine erfolgreiche Autorisierung für den Zugang.
- Die RP ermittelt die *Zugriffsrechte* für den *Zugriff* auf die *E-Ressource*. Daraus werden die benötigten *Attributwerte* zur *E-Identity* abgeleitet.
- Die RP überprüft, ob die benötigten Attributwerte vorhanden sind.
- Die RP erlaubt den *Zugriff*. Das Subjekt greift anschliessend auf die *E-Ressource* zu.
- (optional) Eine RP fordert zusätzlich Attributwerte des Subjekts, wenn sie diese zur Erfüllung ihrer Funktion benötigt wird.

6.2 IAM definieren (Definitionszeit)

Während der Definitionszeit werden alle notwendigen Bedingungen geschaffen, damit zur Laufzeit bestimmt werden kann, ob ein *Subjekt* auf eine schützenswerte *E-Ressource* zugreifen darf. Die Abläufe der Definitionszeit müssen stattfinden, bevor *das Subjekt* die *E-Ressource* benutzt. 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 pflegen

E-Identity pflegen

Umfasst die Prozesse zum Registrieren, Aktualisieren und Löschen von *E-Identities*.

Zugehörige Rolle: RA oder Subjekt (bei Selbstregistrierung)

Tätigkeiten:

- Die zugehörige Rolle identifiziert das *Subjekt* (bei Selbstregistrierung sich selber) und registriert die zugehörige *E-Identity*.
- (Optional) Das Subjekt verlinkt *E-Identities* miteinander.
- Die zugehörige Rolle löscht *E-Identities*.

Anmerkungen:

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

6.2.2 Attribut pflegen

Attribut pflegen

Definition, Aktualisierung und Löschung von *Attributen*.

Zugehörige Rolle: AA

Tätigkeiten:

- Das Subjekt oder die RA beantragt einen neuen *Attributwert* oder die Aktualisierung eines bestehenden *Attributwertes* beim AA.
- Nach Überprüfung teilt die AA dem *Subjekt* dem *Attributwert* zu oder aktualisiert es.
- Die AA registriert die erhobenen *Attributwerte* zur *E-Identity*.
- Die AA löscht *Attributwerte*.

Anmerkungen:

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

6.2.3 Authentifizierungsmittel pflegen

Authentifizierungsmittel pflegen	Erstellen, Vergabe und Erneuerung von <i>Authentifizierungsmitteln</i> für eine E-Identity.
----------------------------------	---

Zugehörige Rolle: CSP

Tätigkeiten:

- Der CSP erstellt, erhebt und vergibt *Authentifizierungsmerkmale* (z.B. Passwörter, Authentisierungszertifikat).
- (optional) Der CSP publiziert die öffentlichen Elemente der *Authentifizierungsmittel* (z.B. öffentlicher Schlüssel) zur *E-Identity*.
- Der CSP händigt des *Authentifizierungsmittels* (ev. mehrere) an das *Subjekt* aus.
- Der CSP erneuert bzw. ersetzt benutzerfreundlich *Authentifizierungsmittel*.
- Der CSP revoziert *Authentifizierungsmittel*.

6.2.4 E-Ressource pflegen

E-Ressource pflegen	Identifikation, Registrierung und Löschen von <i>E-Ressourcen</i> .
---------------------	---

Zugehörige Rolle: IAM-Führung (RP)

Tätigkeiten:

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

Anmerkungen:

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

6.2.5 Berechtigungen pflegen

Berechtigungen pflegen	Zuweisen und Löschen von <i>Zugangsregeln</i> zur <i>Grobautorisierung</i> und <i>Zugriffsrechten</i> zur <i>Feinautorisierung</i> für eine <i>E-Identity</i> .
------------------------	---

Zugehörige Rolle: RP

Tätigkeiten:

- Die RP verwaltet *Zugangsregeln* und *Zugriffsrechten* unter Verwendung der verfügbaren *Attribute* von *E-Identities* und optional eigene Daten.
- Die RP weist *Zugangsregeln* und *Zugriffsrechte* zu einer oder mehreren *E-Ressourcen* zu.
- Die RP löscht *Zugangsregeln* und *Zugriffsrechte*.
- (optional) Die RP kann *Zugangsregeln* an den Vermittler auslagern.

6.3 IAM unterstützen

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

Zugehörige Rolle: IAM-Support

Tätigkeiten:

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

6.4 IAM führen (Etablierung)

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

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

6.4.1 Diensteanbieter managen

Diensteanbieter managen	Beziehungsaufnahme, -pflege und -beendung mit den IAM-Diensteanbietern des IAM-Systems inkl. der Etablierung der Ver-
-------------------------	---

trauensbeziehungen

Zugehörige Rolle: IAM-Führung (IAM-Gesamtsystem)

Tätigkeiten:

- *IAM-Dienstleister* in den Verbund aufnehmen und entfernen (z.B. wegen End-Of-Life oder Nichteinhalten der Sicherheitsvorgaben).
- Vertrags- und/oder SLA Management mit den verschiedenen IAM-Dienstleister oder Akzeptanz der geltende AGBs eines IAM-Dienstleister.
- Festlegung der IAM-Organisation (Rollen) sowie ihrer Beziehung untereinander (Zusammenarbeit).
- Festlegen der Vertrauensanker über die Auswahl der Certificate Authority (CA).
- Bestimmen und Nachführen der Vertrauensstufen für die Authentifizierung.
- (Optional) Bestimmen und Nachführen der Vertrauensstufen der Attribute.
- Definieren, Aktualisieren und Widerrufen der Vertrauensbeziehungen (*Trust*) zwischen IAM-Dienstleistern und Relying Parties. Festlegen, wie die Qualität- und Vertrauensstufen zwischen IdP/AA (oder Vermittler) und RP übermittelt werden.
- Auswirkungsanalyse vor Änderungen an den Vertrauensbeziehungen.
- Festlegen und Aktualisierung der Metadaten zu den IAM-Dienstleistern und RPs.

6.4.2 Relying Parties verwalten

Relying Parties verwalten

Aufnahme und Pflege von *Relying Parties (RP)*

Zugehörige Rolle: IAM-Führung (IAM-Gesamtsystem)

Tätigkeiten:

- Aufnahme von RPs prüfen, z.B. Erfüllung der Sicherheitsanforderungen basierend auf dem Schutzbedarf prüfen.
- Vertrags-Management mit der RP oder Akzeptanz der geltende AGBs der RPs.
- RPs in den Verbund aufnehmen und entfernen (z.B. wegen End-Of-Life, Weiterentwicklung der E-Ressource oder Nichteinhalten der Sicherheitsvorgaben).
- Prüfen der notwendigen Attribute (Vorhandensein und Qualität) und allenfalls Prozess *Attributstruktur managen* anstossen.
- Definieren, Aktualisieren und Widerrufen der Vertrauensbeziehung (Trust) zwischen IAM-Dienstleistern und Relying Party. Festlegen, wie die Qualität- und Vertrauensstufen zwischen IdP/AA (oder Vermittlern) und RP übermittelt wird.
- Auswirkungsanalyse vor Änderungen an den Vertrauensbeziehungen.

- Festlegen und Aktualisierung der Metadaten zu den IAM-Diensteanbietern.
- (Optional) Im Fall, dass es mehrere Domänen gibt, Zugehörigkeit bestimmen.

6.4.3 Attributstruktur managen

Attributstruktur managen	Definition und Weiterentwicklung der Attributdefinition.
--------------------------	--

Zugehörige Rolle: IAM-Führung (AA)

Tätigkeiten:

- Meta-Attribute definieren, harmonisieren und nachführen.
- Attribute klassifizieren (Bsp. Persönliche- und Enterprise-Attribute).

6.4.3.1 Betriebsprüfung durchführen

Betriebsprüfung durchführen	Prüfen der korrekten Umsetzung und Betriebes.
-----------------------------	---

Zugehörige Rolle: IAM-Führung

Tätigkeiten:

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

6.4.4 IAM-Servicekatalog verwalten

IAM-Servicekatalog verwalten	Erstellen und Pflegen des IAM-Servicekatalogs
------------------------------	---

Zugehörige Rolle: IAM-Führung (Diensteanbieter)

Tätigkeiten:

- Definieren der IAM Service Strategie.
- Definieren und Nachführen des Service Katalogs und die zu realisierende IAM-Architekturen.
- Marktanalyse für das Betreiben der Services (intern und extern)
- Roadmap für die Weiterentwicklung der IAM-Services.
- Informationsaustausch und Kommunikation mit den Relying Parties.
- Sicherstellen der Finanzierung für den Betrieb und für die Weiterentwicklung.
- Abwickeln von Service-Anfragen.

6.4.5 Risikoanalyse durchführen und Risiko überwachen

Risikoanalyse durchführen und Risiko überwachen	Durchführen von Risikoanalyse und Festhalten der Resultate
---	--

Zugehörige Rolle: IAM-Führung

Tätigkeiten:

- Durchführen von Risikoanalysen und Festhalten der Resultate, damit Gefahren zeitnah erkannt werden können. Überwachung des Risikopotentials.
- Schutzbedarfsanalyse des IAM-Systems: Die Schutzbedarfsanalyse gewährleistet angepasste Sicherheitsanforderungen (so viel Sicherheit wie nötig, nicht so viel wie möglich).
- Implementieren des Informations- und Datenschutzkonzepts, sowie Feedback an IAM-Regulator bezüglich des Informations- und Datenschutzkonzeptes.
- (Optional) Abstützung des Risikomanagements auf ein Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001, ISMS3⁷ oder nach ISO 33001/13001 [ref. prüfen]. Abstützung des Risikomanagements auf ein Framework wie COBIT.
- Abgleich und Abstimmung mit der IAM-Steuerung.

6.4.6 IAM-Führung managen

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

Zugehörige Rolle: IAM-Führung (IAM-Gesamtsystem)

Tätigkeiten:

- Festlegung der Zusammenarbeit den IAM-Führungen im IAM-Gesamtsystem.
- Definition und kontinuierliche Verbesserung der Kern-, Support- und Führungsprozesse.
- Erstellen von stufengerechte Kommunikationsmitteln für diverse Stakeholder.
- Führung der internen IAM-Dienstanbieter.

6.5 IAM steuern (Regulierung)

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

⁷ ISMS3 ist eine ISMS komplett auf ISO 27001 abbildbar, nimmt aber zusätzlich die Maturität der Organisation in Betracht.

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

6.5.1 IAM-Policy verwalten

IAM Policy verwalten	Festlegung der <i>IAM</i> -Policy und der Architektur des IAM-Systems.
----------------------	--

Zugehörige Rolle: IAM-Regulator

Tätigkeiten:

- Ableiten und Nachführen der Strategie aus der IAM-Policy.
- Definieren der Architektur.
- Definition der *Rollen* mit entsprechenden Aufgaben, Kompetenzen und Verantwortung.
- Erarbeiten der notwendigen Basiskonzepte basierend auf den IAM-Architekturen, z.B. Identitätstypenkonzept und Rechtstypenkonzept.
- Erarbeiten und aktualisieren der relevanten Vorgaben: Identifikation der geltenden gesetzlichen, unternehmensinternen und vertraglichen Richtlinien / Regularien.
- Definieren und Nachführen von Hilfsmitteln für die Anwendung der Architekturen und Vorgaben. Bsp. Vertrauensstufen-Rechner
- Definition der Nachvollziehbarkeitsanforderungen, z.B. das Ablegen der relevanten Dokumente und die Aufbewahrungsfristen der relevanten Daten (siehe auch ISO 29115 [7] Kapitel „Record-keeping/recording“)
- Definieren der relevanten standardisierten Kern-, Support- und Führungsprozessen. Spezialisierung zu diesem Dokument.
- Festlegen des Lebenszyklus von E-Identities, Attributen, Berechtigungen, IAM-Diensteanbietern und RPs.
- (Optional) Festlegen des Lebenszyklus einer Verknüpfung von natürlichen und juristischen Personen (z.B. Aktivierung, Aussetzung, Erneuerung, Widerruf) (siehe auch eIDAS 2015/1502 [6], Abschnitt 2.1.4).
- (Optional) Maturitätsmodell und Maturitätsstufen festlegen.

Anmerkung:

- Der Standard eCH-0172 [21] definiert IAM Maturitätsstufen für unter anderem die Einstufung für die Prozess-Maturität der Steuerung und wird ergänzt durch ein Hilfsmittel mit konkreten Fragen zur Bestimmung dieser Maturität.

6.5.2 Qualitätsmodel(le) pflegen

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

Zugehörige Rolle: IAM-Regulator

Tätigkeiten:

- Qualitätsmodell für die Authentifizierung von Subjekten, dessen Kriterien und dessen Unterteilung definieren (z.B. nach eCH-0170 [4]).
- (Optional) Qualitätsmodell der Attributwertbestätigungen, dessen Kriterien und dessen Unterteilung definieren (z.B. nach eCH-0171 [5]).
- (Optional) Die Interoperabilität zwischen den Qualitätsmodellen festlegen.

6.5.3 IAM-Führung beraten

IAM-Führung beraten	Erstellen von stufengerechte Kommunikationsmitteln für den diversen Stakeholder
---------------------	---

Zugehörige Rolle: IAM-Regulator

Tätigkeiten:

- Kommunikation und Schulung der IAM-Policy
- (Optional) Unterstützung bei IAM-Projekten und Spezialvorhaben

6.5.4 Risikoanalyse durchführen

Risikoanalyse durchführen	Abschätzen des Risikos: Welche Risiken müssen bei der Implementierung beachtet werden? Hilfestellung für die IAM-Führung, welche Risiken gemildert werden sollen.
---------------------------	---

Zugehörige Rolle: IAM-Regulator

Tätigkeiten:

- Definieren der IAM-Sicherheitsziele
- Definieren wie viel Risiko die Organisation bereit ist zu nehmen (Risikobereitschaft) und wie viel Risiko die Organisation nehmen kann (Risikotoleranz).
- Risikoanalyse durchführen, z.B. nach FAIR der Open Group [ref]
- Definieren der Kontrollmechanismen, ex-ante oder ex-post
- Abgleich und Integration mit dem Organisationsrisikomanagementsystem und Ziele.
- Erstellung des Informations- und Datenschutzkonzepts (inkl. Hilfsmittel) für die Implementierung durch die IAM-Führung.
- Analyse der Risikoberichte der IAM Führung und Freigabe dieser Berichte.
- Kontinuierliche Verbesserung des Informations- und Datenschutzkonzepts, z.B. analog ISO 27001 [ref]. Aufgrund der Ist-Situation werden periodisch Verbesserungsmöglichkeiten identifiziert, allenfalls basierend auf der Risikobereitschaft Massnahmen geplant, umgesetzt und überprüft.

- Überwachen von bekannten/publizierten externen Sicherheitsvorfälle und Risikobeurteilungsaufträge an die IAM-Führung(en) erteilen.
- (Optional) Abstützung des Risikomanagements auf **ein Informationssicherheitsmanagementsystems (ISMS)** nach ISO 27001, O-ISM3⁸ oder nach ISO 33001/13001 [ref. prüfen] Abstützung des Risikomanagements auf ein Framework wie COBIT.

6.5.5 IAM Steuerung managen

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

Zugehörige Rolle: IAM-Steuerung

Tätigkeiten:

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

⁸ O-ISM3 ist eine ISMS komplett auf ISO 27001 Abbildbar, nimmt aber zusätzlich die Maturität der Organisation in Betracht.

7 Geschäftsservices

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

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

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

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

7.1 Realweltobjekte

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

7.1.1 Subjekt

Subjekt	Eine <i>natürliche Person</i> , eine <i>Organisation (juristische Person)</i> , ein <i>Service</i> oder ein <i>Ding</i> , das auf eine <i>Ressource</i> zugreift oder zugreifen möchte. Ein Subjekt wird durch <i>E-Identities</i> 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 <i>Subjekt</i> zugreifen kann, wenn es sich <i>authentisiert</i> hat und es auf der Basis der benötigten <i>Attribute</i> <i>autorisiert</i> wurde. Dies schliesst physische Ressourcen wie Gebäude und Anlagen, deren Benutzung über IT-Systeme gesteuert wird, ein.
-----------	--

Aufgaben (zur Laufzeit):

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

7.2 Services zur Definitionszeit

In Abbildung 13 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*.

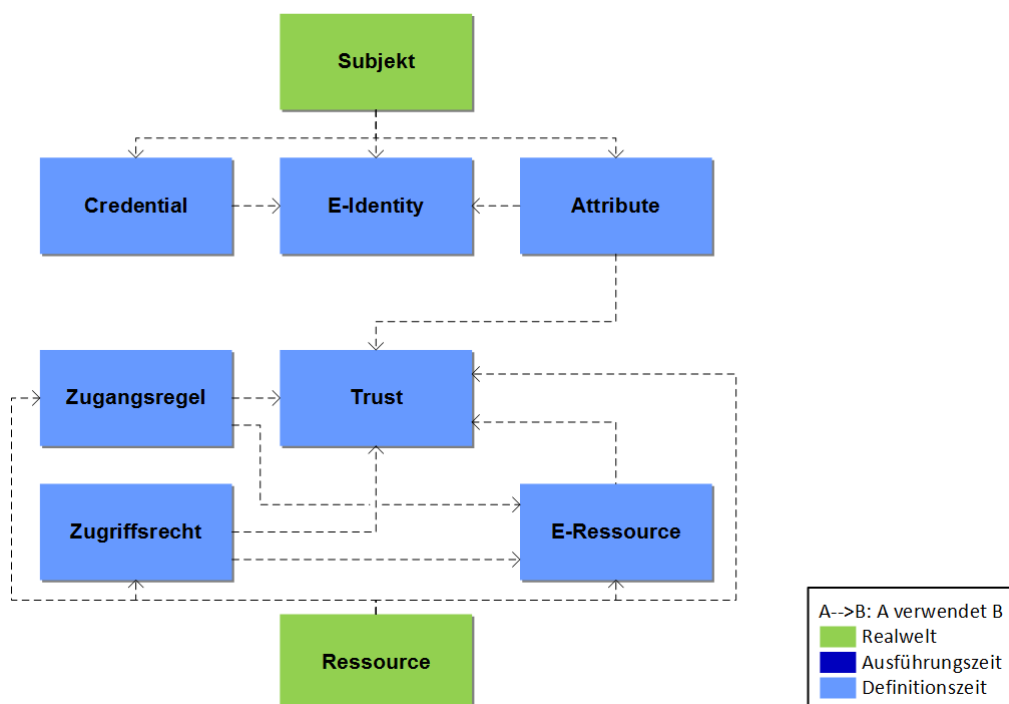


Abbildung 13 Geschäftsservices – Definitionszeit

7.2.1 E-Identity Service

E-Identity Service	Der <i>E-Identity Service</i> stellt zu <i>Subjekten</i> <i>E-Identities</i> 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 <i>Credential Service</i> gibt <i>Authentifizierungsmittel</i> aus und verwaltet sie. Er ermöglicht eine benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln. Ein <i>Authentifizierungsmittel</i> bezieht sich auf eine <i>E-Identity</i> und ist auf ein bestimmtes <i>Subjekt</i> 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 <i>Attribute Service</i> pflegt zeitaktuell ein oder mehrere <i>Attribute</i> für definierte <i>Subjekte</i> .
-------------------	--

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 <i>Trust Service</i> pflegt die akzeptierten, vertrauenswürdigen <i>IAM-Dienstleister</i> .
---------------	---

Schnittstellen:

In: Informationen darüber wer wem bezüglich was vertraut,
Metadaten der RPs und IAM-Dienstleister,
Metadaten der Attribute der AAs

Out: Trust,
Metadaten der RPs und IAM-Dienstleister,

Aufgaben:

- Registriert, pflegt und verwaltet die Vertrauensbeziehungen (inkl. deren Lebenszyklus) der Ressourcen (*Relying Party*) zu den *IAM-Dienstleistern* und den *IAM-Dienstleistern* untereinander.
- Macht Vertragsdefinitionen.
- Definiert die Trust-Anchor über die Auswahl der Credential Service Provider (CSP).
- Registriert die Services der *IAM-Dienstleister* 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 <i>E-Ressource Service</i> stellt zu <i>Ressourcen</i> <i>E-Ressourcen</i> 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 <i>Zugangsregel Service</i> verwaltet die Regeln für den Zugang zu einer <i>E-Ressource</i> . Die Regeln sind auf der Basis von <i>Authentisierung</i> oder <i>Attributen</i> 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 <i>Zugriffsrecht Service</i> verwaltet die Rechte für die Nutzung einer <i>E-Ressource</i> . Die Rechte sind auf der Basis von <i>Authentisierung</i> , <i>Attributen</i> 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 14 dargestellt. Die Abbildung enthält alle Services, die zur Abwicklung der Prozesse *Subjekt authentifizieren* und *E-Identity autorisieren* zur Laufzeit verwendet werden.

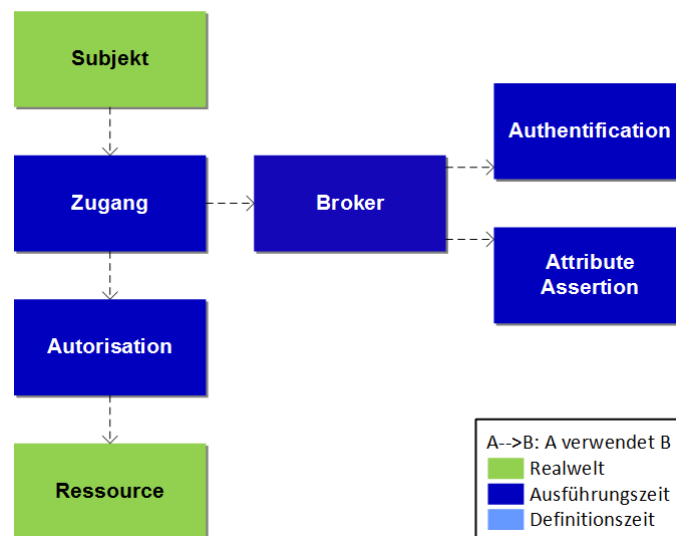


Abbildung 14 Geschäftsservices – Laufzeit

7.3.1 Authentication Service

Authentication Service	Der <i>Authentication Service</i> überprüft mittels der <i>Authentifizierungsmittel</i> , ob der Zugreifende (<i>Subjekt</i>) der ist, der er behauptet zu sein.
------------------------	--

Schnittstelle:⁹

⁹ Bei den Services zur Laufzeit werden in der Schnittstelle, die Daten angegeben, die zur Laufzeit als Informationen benötigt werden (In-Schnittstelle) bzw. die nach der Ausführung des Services zur Verfügung stehen (Out-Schnittstelle). Werden zur Ausführung zusätzliche Informationen aus der Definitionszeit oder weitere Services der Laufzeit benötigt, so werden die entspr. Services angegeben (Braucht-Schnittstelle).

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

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

Braucht: *Credential Service*, *Logging Service*

Aufgaben:

- Überprüft, ob der aufrufenden Service berechtigt ist, eine Authentifizierung zu veranlassen.
- Überprüft, die Ausgabewerte der Authentifikatoren mit Hilfe der Credentials. Ist die Prüfung positiv, ist die Authentifizierung erfolgreich und die behauptete E-Identity wird mit entsprechender Qualität der Authentifizierung (z.B. entsprechend den Vertrauensstufen nach eCH-0170 [4]) bestätigt.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.
- (optional) Holt das Einverständnis des *Subjekts* (Einschränkung auf natürliche Personen) ein, das *Authentifizierungsergebnis* an den aufrufenden Service zu übermitteln.
- (optional) Etabliert eine zeitlich befristete sichere Verbindung zum *user agent* des Subjekts (z.B. Browser oder App).
- (optional) Kann das Authentifizierungsergebnis an Services übermitteln, so lange die sichere Verbindung zum *user agent* des Subjekts besteht (unterstützt Single SignOn)

7.3.2 Attribute Assertion Service

Attribute Assertion
Service

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

Schnittstelle:

In: Attribute-Request,
Identifikator,
(*Authentifizierungsbestätigung*)

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

Braucht: *Attribute Service*, *Logging Service*

Aufgaben:

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

- Generiert berechnete und abgeleitete Attributwerte aus *Attributen* (z.B. over18).
- Bestätigt elektronisch mit entsprechender Qualität (siehe Qualitätsmodell zur Attributbestätigung eCH-0171 [1]), ob ein bestimmtes *Attribut* einem *Subjekt* zugewiesen ist oder nicht.
- Verwendet einen *Logging Service*, um Zugriffsinformationen zur vollständigen Nachvollziehbarkeit abzulegen.
- (optional) Holt das Einverständnis des *Subjekts* (Einschränkung auf natürliche Personen und persönliche Attribute) ein, die *Attributbestätigungen* an den aufrufenden Service zu übermitteln (Zustimmung).

7.3.3 Broker Service

Broker Service	Dieser Service vermittelt zwischen dem <i>Subjekt</i> , <i>Ressourcen</i> und den Services der Ausführungszeit, fördert Authentifizierung und Attributbestätigung.
----------------	--

Schnittstelle:

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

Out: *Authentifizierungsbestätigungen*,
(*Attributbestätigungen*)

Braucht: *Trust Service*, *Logging Service*

Aufgaben:

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

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

7.3.4 Zugang Service

Zugang Service	Der Service überprüft die Einhaltung der <i>Zugangsregeln</i> und erlaubt dem <i>Subjekt</i> den Zugang, wenn die entsprechenden Regeln erfüllt sind.
----------------	---

Schnittstelle:

In: *Identifikator* einer E-Ressource

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

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

7.3.5 Authorisation Service

Authorisation Service	Der Service überprüft zur Ausführungszeit die Einhaltung der Rechte für die Nutzung der <i>E-Ressource</i> und erlaubt dem <i>Subjekt</i> die Nutzung der <i>Ressource</i> , 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 berechnigte Services weiter.
- (optional) Bietet rechtlich verifizierte und verifizierbare Audit- und Monitoring-Funktionen zur vollständigen Nachvollziehbarkeit

7.4 Gesamtmodell

In Abbildung 15 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.

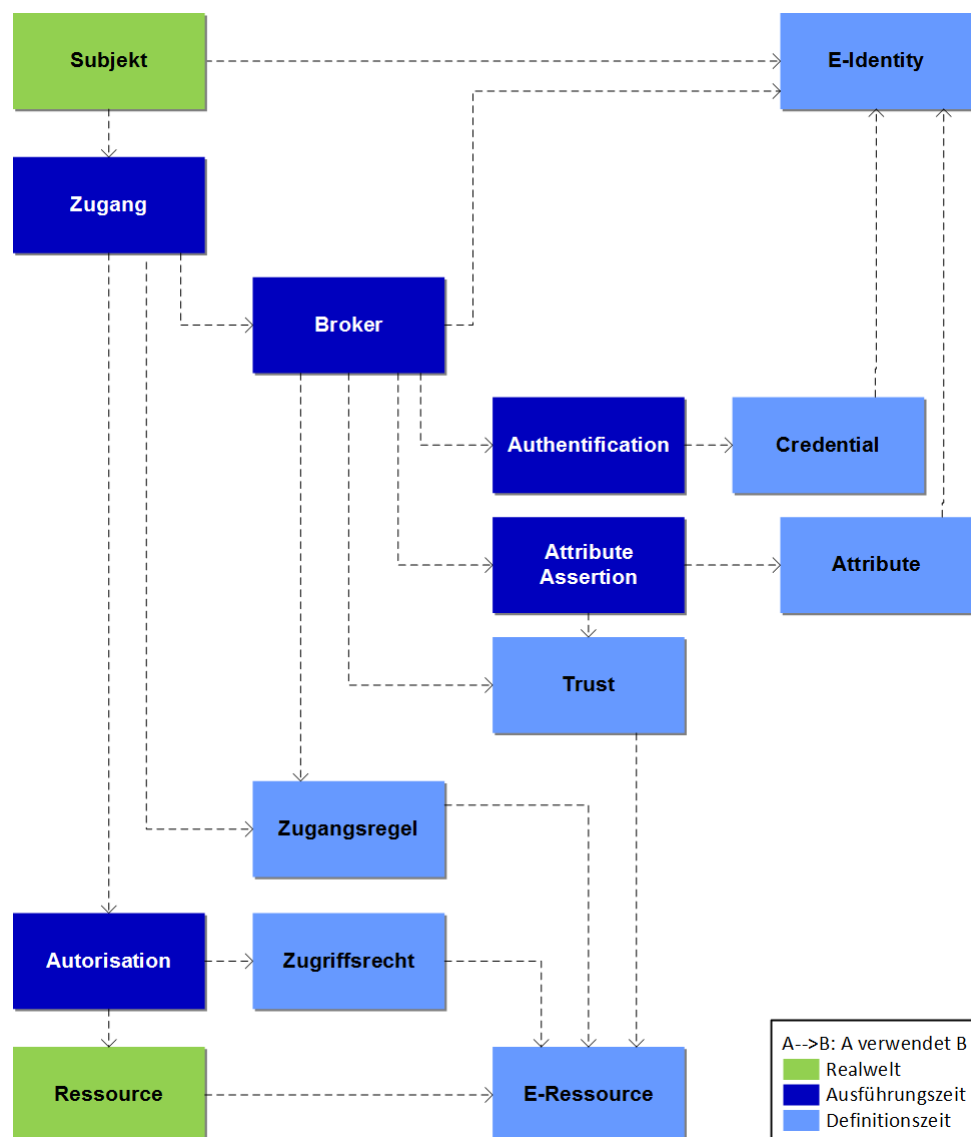


Abbildung 15 Geschäftsservices – Übersicht

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

7.5.1 Subjekt authentifizieren

Abbildung 16 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *Subjekt authentifizieren*.

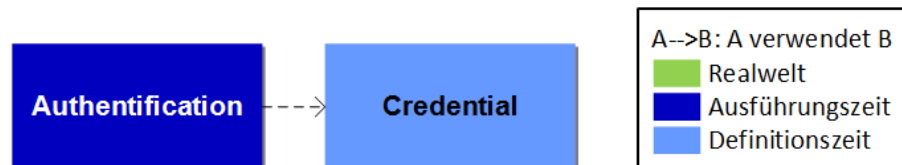


Abbildung 16 Prozessunterstützung *Subjekt authentifizieren*

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 fördern

Abbildung 17 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *Identität fördern*.

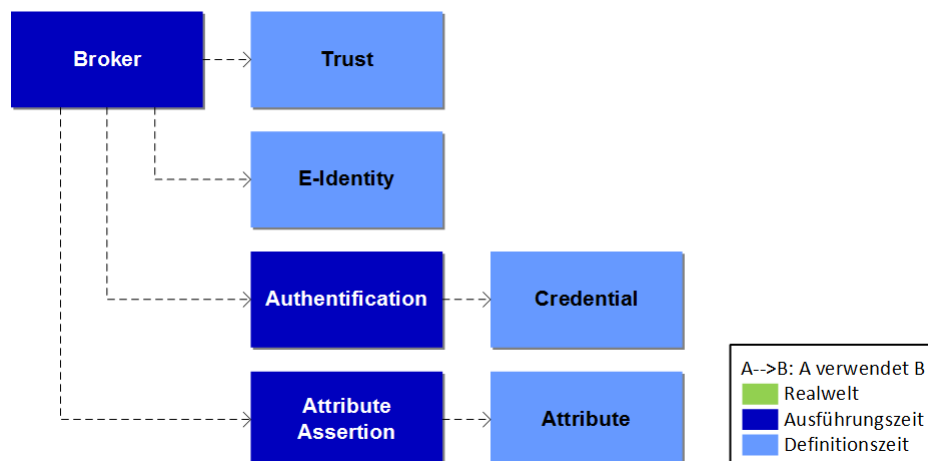


Abbildung 17 Prozessunterstützung *Identität fördern*

Identität fördern folgt dem nachstehenden Ablauf:

- Der *Broker Service* prüft, welche *Authentication* und *Attribute Assertion Service* gemäss *Trust Service* die Anforderungen des aufrufenden Service erfüllen.
- Der *Broker Service* delegiert die *Authentifizierung* des *Subjekts* an den gewählten *Authentication 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 18 zeigt die Verwendungen der Geschäftsservices im Rahmen des Prozesses *E-Identity autorisieren*.

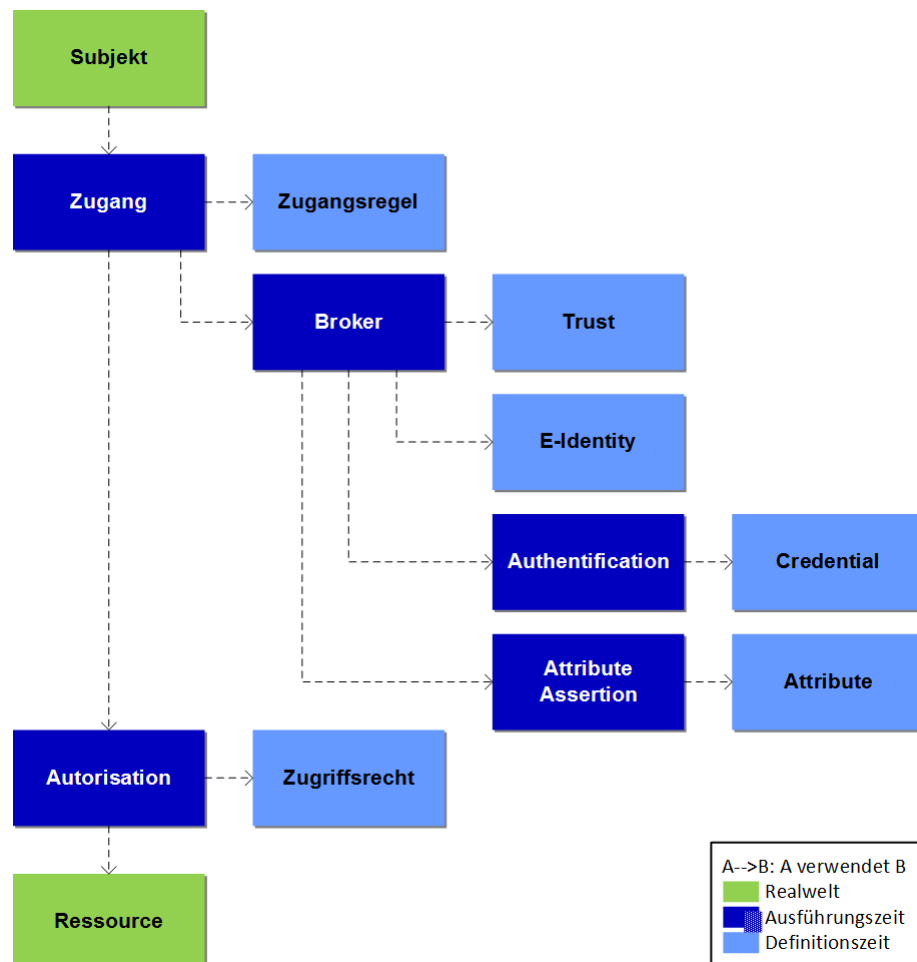


Abbildung 18 Prozessunterstützung *E-Identity autorisieren und Attribute offenlegen*

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 ¹⁰	Attribut ¹¹	Zugangsregel	Zugriffsrecht	E-Ressource	Credential	Identifikator einer E-Identity	Ausgabewert des Authentikator	Authentifizierungsbestätigung	Attributbestätigung	Identifikator einer E-Ressource
Geschäftsservice	E-Identity	B	B ¹²					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 ¹³	LB ¹³	
	Zugang			L		L		L		L	L	L
	Autorisation				L	L		L		L	L	L

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

Tabelle 5 Beziehung zwischen Services und Semantik des Informationsmodells

¹⁰ inkl. Beziehung linkedID

¹¹ inkl. Beziehung zu E-Identity

¹² B für Identifikator (ist auch ein Attribut)

¹³ B, wenn Broker selber kombinierte *Authentifizierungs- und Attributbestätigungen* ausstellt

7.7 Zuständigkeiten für Geschäftsservices

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

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

Tabelle 6 Beziehung zwischen Geschäftsservices und Stakeholder

8 IAM für das IoT

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

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

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

8.1 Spezielle Eigenschaften von Dingen

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

- Dinge können zu einer natürlichen Person oder zu einer Organisation gehören, nachfolgend als Besitzer (des Dings) bezeichnet. Der Besitzer ist für seine Dinge verantwortlich und haftet für deren Aktivitäten im IoT¹⁴.
- 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.

¹⁴ 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	<p>Dinge im IoT sollten immer einen Besitzer haben.</p> <p>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).</p> <p>Das Konzept des „Besitzers“ (von Dingen) erfordert eine zusätzliche Beziehung im Rahmen der Informationsarchitektur (vergleiche hierzu die Definition „Subjekt“ in der Informationsarchitektur).</p> <p><i>Bemerkung:</i> 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).</p>
„On behalf“ Zugriff	<p>Dinge nutzen Ressourcen „on behalf“ ihres Besitzers.</p> <p>Das Auto sucht sich einen freien Parkplatz oder eine Tankstelle, das Mobiltelefon aktualisiert lokale Daten, der Kühlschrank bestellt Milch.</p> <p>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.</p>

Eigene und übertragene Attribute	<p>Dinge haben eigene und übertragene Attribute.</p> <p>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.</p> <p>Für die Übertragung von Attributen an Dinge müssen Regeln definiert werden. Beispiele für solche Übertragungsregeln könnten sein:</p> <ul style="list-style-type: none"> • 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). <p><i>Bemerkung:</i> Die Übertragung von Attributen kann ggf. auch unabhängig vom IoT genutzt werden, um Stellvertretungen zu verwalten.</p>
Besitzer Wechsel	<p>Dinge können den Besitzer wechseln.</p> <p>Langlebige Dinge (z.B. Investitionsgüter) können im Verlauf ihrer Lebensdauer mehrfach den Besitzer wechseln.</p> <p>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.</p>
Ersatz von Dingen	<p>Dinge können ersetzt werden.</p> <p>Kurzlebige Dinge (z.B. Verbrauchsmaterial) können 1:1 ersetzt werden.</p> <p>Eigene (inhärente und dynamische) Attribute werden beim Ersatz neu definiert. Übertragene Attribute müssen automatisch auf das Ersatz-Ding übertragen werden können.</p>
Zusammengesetzte Dinge	<p>Dinge können aus Dingen zusammengesetzt sein.</p> <p>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.</p> <p>Das IAM muss in der Lage sein, auch komplexe Beziehungen von Dingen untereinander abzubilden.</p>

8.3 Auswirkung auf die IAM Geschäftsservices

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

Aspekt	Grundsatz, Beschreibung und Umsetzung im IAM
Integriertes Authentifizierungsmittel	<p>Dinge haben ein integriertes Authentifizierungsmittel.</p> <p>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).</p> <p>Der Authentication Service zur Authentifizierung von Subjekten muss die spezifischen Eigenschaften von Dingen berücksichtigen.</p> <p><i>Bemerkung:</i> Physical unclonable functions (PUF) sind mit biometrischen Verfahren vergleichbar und könnten einen interessanten Lösungsansatz für die Authentifizierung von Dingen aufzeigen.</p>
Automatische Registrierung inkl. Inventarisierung	<p>Dinge können sich automatisch registrieren.</p> <p>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.</p> <p>Der E-Identity Service und der Credential Service müssen die spezifischen Eigenschaften von Dingen berücksichtigen und insbesondere Automatisierung ermöglichen.</p>

9 Privacy

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

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

9.1 Anforderungen an Sicherheit und zum Schutz der Privatsphäre

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

ID	Name	Allgemeine Beschreibung	Typische Anwendungsszenarien
R1	Nichtbeobachtbarkeit (Unobservability)	Ein Subjekt kann auf eine Ressource zugreifen, ohne dass unberechtigte Dritte dies feststellen können.	Ein an einem Authentisierungsvorgang beteiligter IdP/AA soll ohne Drittpartei nicht feststellen können, ob und wann ein bestimmtes Subjekt auf eine Ressource zugegriffen hat. ¹⁵ Eine in einem Authentisierungsvorgang unbeteiligter Externer soll nicht feststellen können ob und wann ein bestimmter Benutzer auf eine RP oder auf eine Ressource zugegriffen hat (z.B. durch zeitliche Korrelation)
R2	Unverkettbarkeit (Unlinkability)	Ein Benutzer kann mehrmals auf eine Ressource zugreifen, ohne dass unberechtigte Dritte diese Ereignisse verbinden können.	Ein Benutzer soll auf unterschiedliche RP's bzw. auf Ressourcen zugreifen können, ohne dass die Identität durch Korrelation der Identitätsdaten durch die beteiligten RP's oder durch Dritte aufgedeckt werden kann.

¹⁵ Umgekehrt kann auch die Anforderung bestehen, dass eine beteiligte RP nicht feststellen können soll, bei welchem IdP/AA sich ein bestimmter Benutzer authentisiert hat. Diese Anforderung ist in der Praxis eher unrealistisch. Eine RP muss i.d. Regel prüfen können, bei welchem IdP/AA sich ein Benutzer authentisiert hat, um das notwendige Vertrauen aufbauen zu können.

ID	Name	Allgemeine Beschreibung	Typische Anwendungsszenarien
R3	Vertraulichkeit (Confidentiality)	Ausser einer ausstellenden Instanz (IdP/AA) und der konsumierenden RP, sowie dem Subjekt selbst, können keine an einem Authentisierungsvorgang beteiligte Dienste personenidentifizierende Information einsehen.	Ein am Authentisierungsvorgang beteiligter Vermittler oder eine nicht-vertrauenswürdige Software auf dem Client des Benutzers sollen personenidentifizierende Informationen (vermittelte Attribute) und optional die Identität des Benutzers nicht einsehen bzw. feststellen können.
R4a	Datenherkunft und Datenunversehrtheit (Authenticity & Integrity)	Eine Applikation kann die Herkunft und Unversehrtheit von Identitätsinformationen eines Benutzers bis zu ihrer Quelle zurück überprüfen.	<p>Eine RP kann überprüfen, ob Identitätsinformationen von einem berechtigten Vermittler stammen.</p> <p>Eine RP kann feststellen, ob die Authentifizierungs- und Attributbestätigungen von einer ihr bekannten autoritativen Quelle (IdP/AA) stammen.</p> <p>Eine RP kann sich davon überzeugen, dass der Überbringer einer Authentifizierungs- und Attributbestätigung der rechtmässige Inhaber ist¹⁶.</p>
R5	Einwilligung/Freigabe (Consent)	Die Freigabe von Identitätsinformationen an einen anfragenden Dienst kann ohne Einwilligung des Benutzers nicht erfolgen.	Ein Vermittler oder eine Client-Software fordert vom Benutzer die Freigabe von personenidentifizierenden Informationen und Attributen ein.
R6	Nachvollziehbarkeit (Auditability)	Die zu einem bestimmten Authentisierungsvorgang vermittelten Identitätsinformationen und ihre Metadaten liegen vor.	Die vermittelten Identitätsinformationen und ihre Metadaten können zentral eingesehen oder unter Mitwirkung aller beteiligter Entitäten im Nachhinein zusammengestellt werden.

9.2 Verwaltung und Verarbeitung von Daten von Subjekten

Dieses Kapitel gibt eine Richtlinie, was es zu beachten gibt, wenn Daten von Subjekten verwaltet und verarbeitet werden. Die wichtigste Voraussetzung ist, dass der Benutzer jederzeit sicherstellen kann, auf welche Art seine Daten verwendet werden. Dieses Kapitel beschreibt,

¹⁶ Diese allgemein formulierte Anforderung beinhaltet auch den Assertion Diebstahl über einen Browser. Diese Anforderung kann z.Zt. nur mit SAML und dem Holder-of-Key Profil (HoK) sinnvoll umgesetzt werden.

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

9.2.1 Minimierung der Datensammlung und des Datenbestands

Subjektidentifizierende Attribute dürfen von der RA für die Identifizierung und Überprüfung eines Subjektes gesammelt werden.

Ein Vermittler darf nur die Attribute an eine RP weitergeben, welche von der RP explizit angefordert wurden. In spezifischen Fällen ist es nicht nötig Attribute völlig offen zu legen. Beispielsweise wenn die RP nur wissen will, ob das Subjekt 18 Jahre oder älter ist, sollte nicht das explizite Geburtsdatum weitergegeben werden.

Ausserdem darf eine RP nur die Attribute vom Subjekt anfragen, die sie für die Erfüllung ihrer Funktion benötigt. Das Anfragen unnötiger Attribute kann das Vertrauen schwächen.

9.2.2 Verhindern von Profiling

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

9.2.3 Kenntnisnahme und Einwilligung

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

9.2.4 Nutzungsbeschränkung

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

9.2.5 Regress

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

9.2.6 Datenschutz- und Risikoanalyse

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

9.2.7 Datenschutzmassnahmen

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

10 Haftungsausschluss/Hinweise auf Rechte Dritter

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

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

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

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

11 Urheberrechte

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

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

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

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

Anhang A – Referenzen & Bibliographie

- [1] eCH, «eCH-0122: Architektur E-Government Schweiz: Grundlagen, v1.0,» 2014. [Online]. Available: <https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0122&documentVersion=1.0>.
- [2] eCH, «eCH-0219: IAM Glossar, v1.0,» 2017. [Online].
- [3] «Protokoll Expertenworkshop “Sicherheitsopportunitäten für den Wirtschaftsstandort Schweiz” vom 8.11.2012 (zu Strategie Informationsgesellschaft)».
- [4] eCH, «eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten, v2.0,» 2017. [Online]. Available: <http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170&documentVersion=2.0>.
- [5] eCH, «eCH-0171: Qualitätsmodell der Attributwertbestätigung zur eID,» 2014. [Online]. Available: <https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0171&documentVersion=1.0>.
- [6] eCH, «eCH-0168: SuisseTrustIAM technische Architektur und Prozesse, V1.0,» 2014. [Online]. Available: <https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0168&documentVersion=1.0>.

Anhang B – Mitarbeit & Überprüfung

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

Anhang C – Abkürzungen

AA	Attribute Authority
CP	Credential Provider
IAM	Identity und Access Management
IdP	Identity Provider
LB	Leistungsbezüger
LE	Leistungserbringer
RP	Relying Party
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SSO	Single Sign-On
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Anhang D – Glossar

In diesem Standard werden ausschliesslich die Begriffe aus dem eCH-Standard eCH-0219 V1.0 [2] verwendet.

Anhang E – Identity Federation Modelle

Sobald mehrere RPs und IdP/AAs im Spiel sind, spricht man von *Identity Federation* Modellen. Auf dieser Ebene sind verschiedene Szenarien möglich, welche sich je nach Ziel und Randbedingungen besser oder schlechter eignen.

Folgende fünf Umsetzungs-Varianten sind Situations-spezifisch optimal. Bei der Umsetzung einer *föderierten IAM*-Lösung gilt es eines dieser Varianten oder deren Mischform zu implementieren.

E.1 – RP-zentriertes Modell

Das *RP-zentrierte Modell* (vgl. Abbildung 19) ist für eine *Relying Party* geeignet, welche eine *Ressource* für eine grössere Anzahl Partnerorganisationen zur Verfügung stellt. Die Subjekte dieser Organisationen können sich bei ihrem Heimat-IdP oder Heimat-IdP/AA (in Abbildung 19 als Vermittler mit angeschlossenen IdP und AA) ihrer *Domäne* authentisieren und mit ihren *Attributen* auf die *Ressource* zugreifen. Der grosse Vorteil für die *Relying Party* liegt darin, dass sie die *E-Identities* nicht selbst verwalten muss. Ihr reicht die *Authentifizierungs-* und *Attributbestätigung*, um das *Subjekt* für den *Zugriff* auf die *Ressource* zu berechtigen.

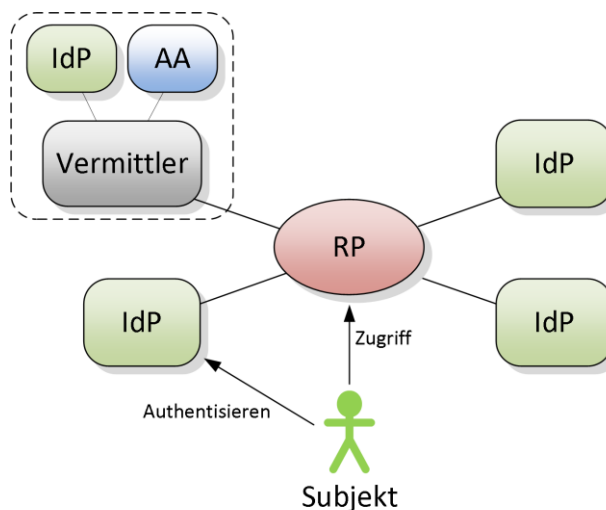


Abbildung 19 RP-zentriertes Modell

E.2 – Vermittler-zentriertes Modell

Das *Vermittler-zentrierte Modell* (vgl. Abbildung 20) wird eingesetzt, wenn mehrere *IAM*-Systeme auf einen einzigen Vermittler mit angeschlossenen IdP und AA konsolidiert werden, welches dann von möglichst vielen *Relying Parties* zur Authentifizierung und *Autorisierung* der *Subjekte* verwendet wird. Innerhalb einer Organisation ist dies meist einfach umzusetzen. Über Organisationsgrenzen hinweg hingegen gibt es vielfach grosse rechtliche Hürden, um dieses Szenario umsetzen zu können.

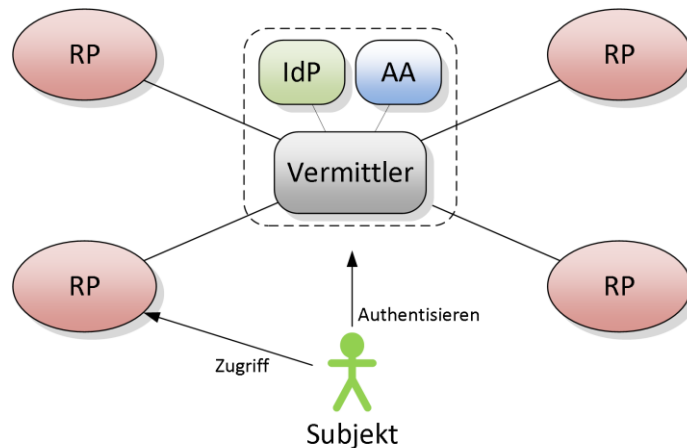


Abbildung 20 Vermittler-zentriertes Modell

E.3 – Cross Domain Modell

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

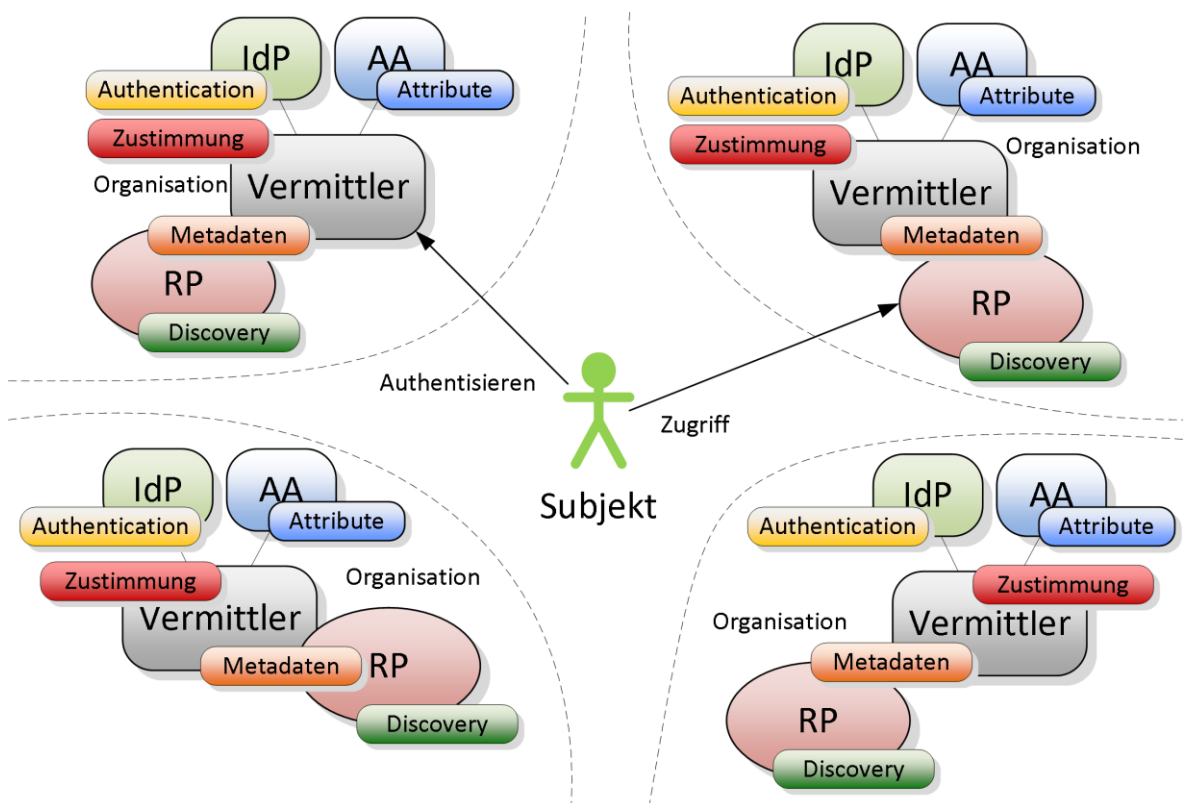


Abbildung 21 Cross Domain Modell

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 22 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).

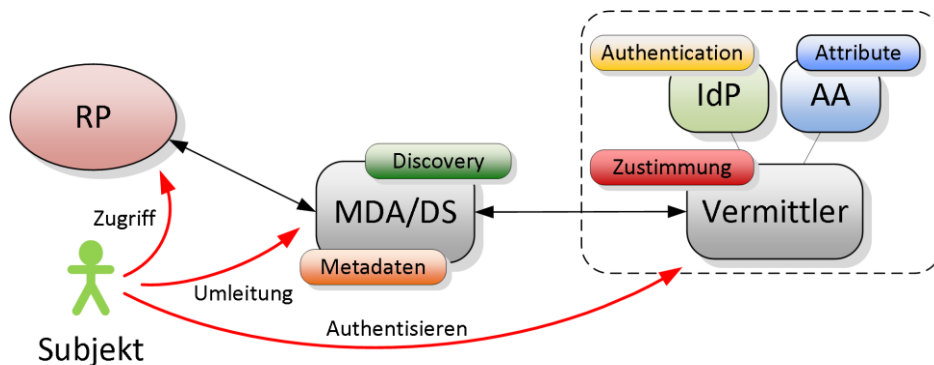


Abbildung 22 Zentralisierte Metadaten und Discovery Service

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'-Spoke¹⁷ Modell basiert auf einem zentralen *Identity Hub*, welchem alle beteiligten Parteien mit ihren Diensten vertrauen. Wie in Abbildung 23 gezeigt, kann dieser *Identity Hub* weitere Dienste von den Parteien übernehmen und zentral ausüben. Der Protokollablauf zur Laufzeit wird in diesem Modell verändert und damit direkter. Die RPs kommunizieren nur noch mit dem zentralen *Identity Hub*. Dieser unterhält eine zentrale Tabelle mit den *E-Identities* der *Subjekte* (Identity Linking). Damit kann er das *Subjekt* bei einem der angegebenen *Identity Provider* authentifizieren lassen, kann Attributinformationen von anderen Vermittlern zusammentragen und stellt diese zu einer aggregierten Antwort an die *Relying Party* zusammen.

¹⁷ Nabe und Speiche

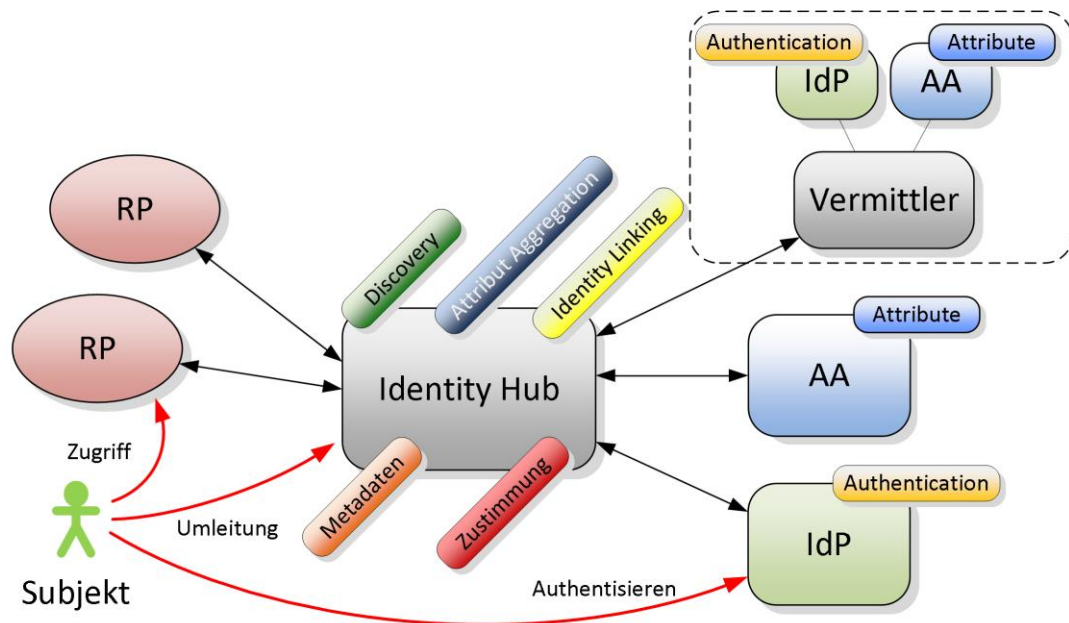


Abbildung 23 Hub-'n'-Spoke Modell

Das in Abbildung 23 dargestellte *Hub-'n'-Spoke Modell* zeigt eine Möglichkeit der Zentralisierung von Diensten auf. Es sind hier ganz verschiedene Ausprägungen der Zentralisierung möglich, wie es auch Mischformen der hier vorgestellten *Identity Federation* Modelle gibt.

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

E.6 – Proxied Federation

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

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

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

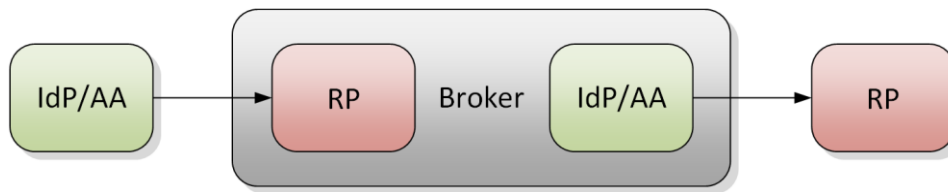


Abbildung 24 Proxied Federation

Anhang F – Änderungen gegenüber Version 2.00

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

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

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

Grundsätzliches:

- *Der Aufbau der Kapitel wurde nicht grundsätzlich geändert, sondern die einzelnen Kapitel wurden überarbeitet.*
- *V2.0 beschränkt sich konsequent auf das organisationsübergreifendes IAM.*
- *Das Glossar von V2.0 enthielt viele Begriffe aus dem IAM, die nicht im Dokument verwendet wurde. Um in Zukunft eine einheitliche Terminologie bei allen IAM-Standards verwenden zu können, wurde dieses Glossar in einen eigenen Standard (eCH-0219 [2]) ausgelagert. Im Dokument selbst werden nur einige zum Verständnis notwendigen die verwendeten Begriffe zitiert.*

Einleitung [eCH-0107 V2.0 Kapitel 2]

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

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

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

Kapitel 4 Anforderungen

Die Designprinzipien und allgemeine Anforderungen an ein föderiertes IAM System wurden überarbeitet und durch neue Erkenntnisse (z.B. aus eCH-0168[ref], eCH-0174[ref], eCH-0170[ref]) ergänzt, Sie wurden neu strukturiert, klassifiziert und begründet.

- *Die Anforderungen der verschiedenen Stakeholder wurden überarbeitet, erweitert, begründet.*

Kapitel 5

Informationsarchitektur [eCH-0107 v2.00 Kapitel 5]

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

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

- *Die Prozesse wurden aktualisiert und ergänzt.*

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

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

Kapitel 8 IAM für das IoT [neu]

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

Kapitel 9 Privacy [neu]

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

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