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

Name	IAM-Gestaltungsprinzipien
Standard-Nummer	eCH-0107
Kategorie	Best Practice
Reifegrad	Definiert
Version	1.00
Status	Aufgehoben
Genehmigt am	2011-03-18
Ausgabedatum	2014-09-03
Ersetzt Standard	
Sprachen	Deutsch
Autoren	Willy Müller, ISB, willy.mueller@isb.admin.ch Hans Häni, AFT TG, hans.haeni@tg.ch SEAC-Projektgruppe IAM
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Das vorliegende Papier definiert die Anforderungen, Prinzipien und Regeln für die IAM-Systemgestaltung, welche beim Bereitstellen von föderativen IAM-Lösungen im E-Government Schweiz berücksichtigt werden müssen, damit lokale Anwendungen und Dienste in bestehenden und neuen Infrastrukturen diese Angebote nützen können. Diese Best Practice soll auch Anwendung im E-Health Schweiz finden.

Inhaltsverzeichnis

Status des Dokuments 4

1 Einleitung 5

1.1 Anwendungsgebiet 5

1.2 IAM-Definitionen 5

2 Anforderungen 8

3 Geschäftsarchitektur 9

3.1 Übersicht 9

3.2 Allgemeine Entwurfsprinzipien 11

3.3 Identity Provider (IdP) 11

3.4 Credential Provider 11

3.5 Claim Provider (CP) 12

3.6 Authentication Provider 12

3.7 Authorization Provider 12

3.8 Access Provider 13

3.9 Ressourcenverantwortlicher 13

3.10 Überprüfungsinstanz der Rechtevergabe 14

4 Informationssystem-Architektur 15

4.1 Datenarchitektur 15

4.2 Anwendungs-Architektur 16

4.2.1 Übersicht 16

4.2.2 Allgemeine Design Prinzipien 17

4.2.3 Management Services 18

4.2.3.1 Identity Management Service 18

4.2.3.2 Credential Management Service 18

4.2.3.3 Claim Management Service 18

4.2.3.4 Rechteverwaltung Ressourcenzugang 19

4.2.3.5 Rechteverwaltung Ressourcennutzung 19

4.2.4 Access Services 19

4.2.4.1 Client 19

4.2.4.2 Identification Service 20

4.2.4.3 Access Service 20
4.2.4.4 Authentifikations-Service 21
4.2.4.5 Autorisierungs-Service 21
4.2.4.6 Ressource 22

5 Domänen und ihr Zusammenspiel 23
5.1 Design Prinzipien 24

6 Umsetzung 24

7 Haftungsausschluss/Hinweise auf Rechte Dritter 25

8 Urheberrechte 25

Anhang A – Referenzen & Bibliographie 26

Anhang B – Mitarbeit & Überprüfung 26

Anhang C – Abkürzungen 26

Anhang D – Glossar 27

Status des Dokuments

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

1 Einleitung

1.1 Anwendungsgebiet

Das vorliegende Papier definiert die Anforderungen und Design Prinzipien für die Gestaltung von Systemen für die Identitäts- und Zugriffsverwaltung (IAM). Sie sind beim Bereitstellen von föderativen IAM-Lösungen im E-Government Schweiz zu berücksichtigen, damit lokale Anwendungen und Dienste organisationsübergreifend genutzt werden können. Es dient als Anleitung für alle, welche im E-Government-Umfeld IAM-Lösungen entwerfen. Das Papier beschreibt eine konzeptionelle Architektur, die als Grundlage für den Entwurf von neuen und zur Beurteilung von bestehenden IAM-Lösungen herangezogen werden soll.

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

Die Strukturierung des Dokuments orientiert sich am Architektur-Framework von [TOGAF]. Es enthält Entwurfsprinzipien, welche in die Phasen „B. Geschäftsarchitektur“ und „C. Informationssystem-Architektur“ Anwendung finden.[1]

1.2 IAM-Definitionen

Im Kontext dieses Papiers bedeuten:

IAM	Identitäts- und Zugriffsverwaltung (Identity und Access Management)
Subjekt	Entität, die auf eine elektronische *Ressource* zugreift oder zugreifen möchte. Es kann sich um eine natürliche oder juristische Person, aber auch um eine Maschine handeln.
Ressource	Anwendung, Service, Funktion, Prozess oder Daten, auf welche ein *Subjekt* zugreifen möchte.
Client	Technische Einrichtung (Anwendung, Webbrowser etc.), mit welcher das Subjekt auf die Ressource zugreift.
Identität	Ein *Identifikator*, meist zusammen mit einer Menge von zusätzlichen Attributen, welche innerhalb eines *Namensraumes* eindeutig einem *Subjekt* zugewiesen werden können. Ein Subjekt kann mehrere Identitäten besitzen.

[1] eCH-0107 kann betrachtet werden Foundation Architecture im Sinne des Architecture Continuums gemäss TOGAF, vgl. The Open Group. TOGAF Version 9. The Open Group Architecture Framework (TOGAF), S. 543ff.

Digitale Identität	Eine *Identität*, die in einer Form kodiert ist, welche sich für die elektronische Verarbeitung eignet.
Identifikator	Eine Zeichenkette, welche ein *Subjekt* innerhalb eines *Namensraumes* eindeutig bezeichnet.
Namensraum	Anwendungsbereich, für welchen die Bedeutung einer Zeichenkette definiert ist (z.B. ein Unternehmen, ein Staat, eine Fachgemeinschaft, eine Sprachgemeinschaft).
Credential	Ausweis, mit dessen Hilfe die behauptete *Identität* eines zugreifenden *Subjekts* überprüft werden kann.
Security Token	Ein Datenpaket, welches verwendet werden kann, um den Zugriff auf eine *Ressource* zu autorisieren.
Claim	Behauptung über ein *Subjekt*, welche eine offizielle Stelle als korrekt bestätigt, z.B. "ist 18 Jahre alt", "ist Arzt". (In der IAM-Literatur sind je nach Kontext dafür auch die Begriffe 'Rolle', 'Attribut' oder 'Gruppe' gebräuchlich.).
Registrierung	Prozess zur Erlangung einer *Identität* bzw. eines *Credentials von einer* Registrierungsstelle.
Administration	In unserem Kontext: Schaffung aller notwendigen Bedingungen, damit zur Zugriffszeit bestimmt werden kann, ob ein Subjekt auf eine Ressource zugreifen darf
Authentisierung	Nachweis der eigenen Identität durch ein Subjekt[2]
Authentifikation	Vorgang der Überprüfung einer behaupteten *Identität.*
Authentifizierung	Synonym für *Authentifikation.*
Autorisierung	Erteilen einer Zugriffsberechtigung für eine authentifizierte *Identität*.
Identity Provider (IdP)	Herausgeber von *digitalen Identitäten.*
Credential Provider	Herausgeber von *Credentials*, z.B. eine Herausgeberin von elektronischen Zertifikaten.
Claim Provider (CP)	Stelle, welche *Claims* registriert und beglaubigt bestätigt, dass ein *Subjekt* einen bestimmten *Claim* erfüllt (z.B. eine bestimmte Rolle einnimmt).
Ressourcenverantwortlicher	Verantwortliche Stelle für die Vergabe von Rechten an *Claims* für den Zugriff auf die von ihm verwalteten *Ressourcen (*z.B.: Anwendungsverantwortlicher, Serviceverantwortlicher, Dateninhaber*).*

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

Access Provider	Stelle, welche den gesamten Vorgang der Authentisierung und Autorisierung zentral durchführt und die endgültige Entscheidung über den Zugriff auf Basis der zur Verfügung gestellten Credentials usw. trifft. Der Access-Provider stellt auch jene Daten zur Verfügung, die für Accounting, Billing und nutzungsbasierte Lizensierung benötigt werden.
Authentication Provider	Stelle, die *Authentifikation* als Dienstleistung anbietet.
Authorization Provider	Organisation, die *Autorisierung* als Dienstleistung anbietet.
Policy	in unserem Kontext: IAM-Policy. Schriftlich festgehaltene Regelungen und Vorschriften, welche einzuhalten sind, um die Vorgaben der betreffenden *Domäne* einzuhalten.
Policy Enforcement Point	(PEP) – Ort, wo die *Policy* durchgesetzt wird.
User	Person, die auf eine *Ressource* zugreifen möchte.
Trust-Level	Zwischen den Beteiligten abgemachtes Vertrauensniveau, das Sicherheitsanforderungen für die Prozesse und die technologischen Komponenten festlegt.
Grobautorisierung	Gewährung bzw. Verweigerung des Zugriffs auf eine Ressource.
Feinautorisierung	Gewährung bzw. Verweigerung des Zugriff auf einzelne von einer Ressource bereitgestellten Funktionen oder Daten.
Zugriff	Aktivierung einer Ressource, um eine Funktion auszuführen oder Daten zu gewinnen. Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe gespeichert.
Auditing	a) Überprüfung der Policy-Konformität. b) Aufzeichnung aller Aktionen und Entscheide zur Gewährleistung der Nachvollziehbarkeit .
Domäne	Gemeinschaft oder Organisation mit einer gemeinsamen *Policy.*
Basis-Domäne	*Domäne*, welche *Ressourcen* verwaltet und an den *Policy Enforcement Points* die Einhaltung der *Policy* durchsetzt.
Meta-Domäne	*Domäne*, welche die Zusammenarbeit zwischen zwei oder mehreren Domänen regelt.
Auditing	a) Überprüfung der *Policy*-Konformität b) Aufzeichnung aller Aktionen und Entscheide zur Gewährleistung der Nachvollziehbarkeit

Bemerkung: Für diverse Begriffe sind in der Literatur englische Bezeichnungen geläufig. Wir haben daher darauf verzichtet, konsequent deutsche Begriffe zu verwenden.

2 Anforderungen

IAM Anforderungen von Benutzern

- Ich muss meine Identität nur dort nachweisen, wo es notwendig ist.
- Ich muss meine Credentials nur dort angeben, wo sie notwendig sind.
- Ich kann auf die geschützten Ressourcen unabhängig von meinem Standort weltweit zugreifen.
- Ich benötige nur eine geringe Anzahl von elektronischen Identitäten.
- Ich muss nur eine geringe Anzahl von Credentials verwalten.
- Elektronische Identitäten und Credentials sind günstig in der Beschaffung.
- Die Beschaffung von elektronischen Identitäten und Credentials ist einfach durchzuführen.
- Die Benutzung von elektronischen Identitäten und Credentials ist einfach und unkompliziert.
- Ein eventueller Stellvertreter kann an meiner Stelle handeln. Seiner elektronischen Identität werden im Stellvertretungsfall (bestätigt durch entsprechende Claims) die notwendigen Rechte für die benötigten Ressourcen übertragen.
- Niemand kann auf meine privaten Daten zugreifen, ausser ich erteile explizit die Genehmigung dazu.
- Die Lösung ist robust.
- Ich kann einen Stellvertreter bestimmen, der an meiner Stelle handeln darf. Der Stellvertreter kann eine andere Person oder eine Maschine sein.

IAM Anforderungen von Ressourcenverantwortlichen

- Der Missbrauch von Ressourcen ist nicht möglich.
- Der Zugriff auf Ressourcen wird nur autorisierten Personen oder Systemen gestattet.
- Der Aufwand für die Administration der elektronischen Identitäten ist minimal.
- Der Aufwand für die Administration der Credentials ist minimal.
- Der Aufwand für die Verwaltung der Claims ist minimal.
- Der Aufwand für die Verwaltung der Autorisierungen ist minimal.
- Die rechtlichen Vorgaben, insbesondere zum Datenschutz, sowie alle organisationsspezifischen Sicherheitsvorgaben müssen zu jeder Zeit gewährleistet sein.

- Die Nachvollziehbarkeit und Nachweisbarkeit, welches Subjekt wann auf welche Ressource zugegriffen hat, ist gewährleistet. Der Zusammenhang zwischen der elektronischen Identität und den dazugehörigen Credentials muss zu jedem Zeitpunkt gewährleistet sein.
- Die geltenden technischen und organisatorischen Normen und Standards werden eingehalten.

3 Geschäftsarchitektur

3.1 Übersicht

In der folgenden Grafik wird die IAM-Geschäftsarchitektur schematisch dargestellt. Wesentlich ist die Unterscheidung in Definitionszeit und Ausführungszeit, da die zugeordneten Provider dabei unterschiedliche Rollen innehaben.

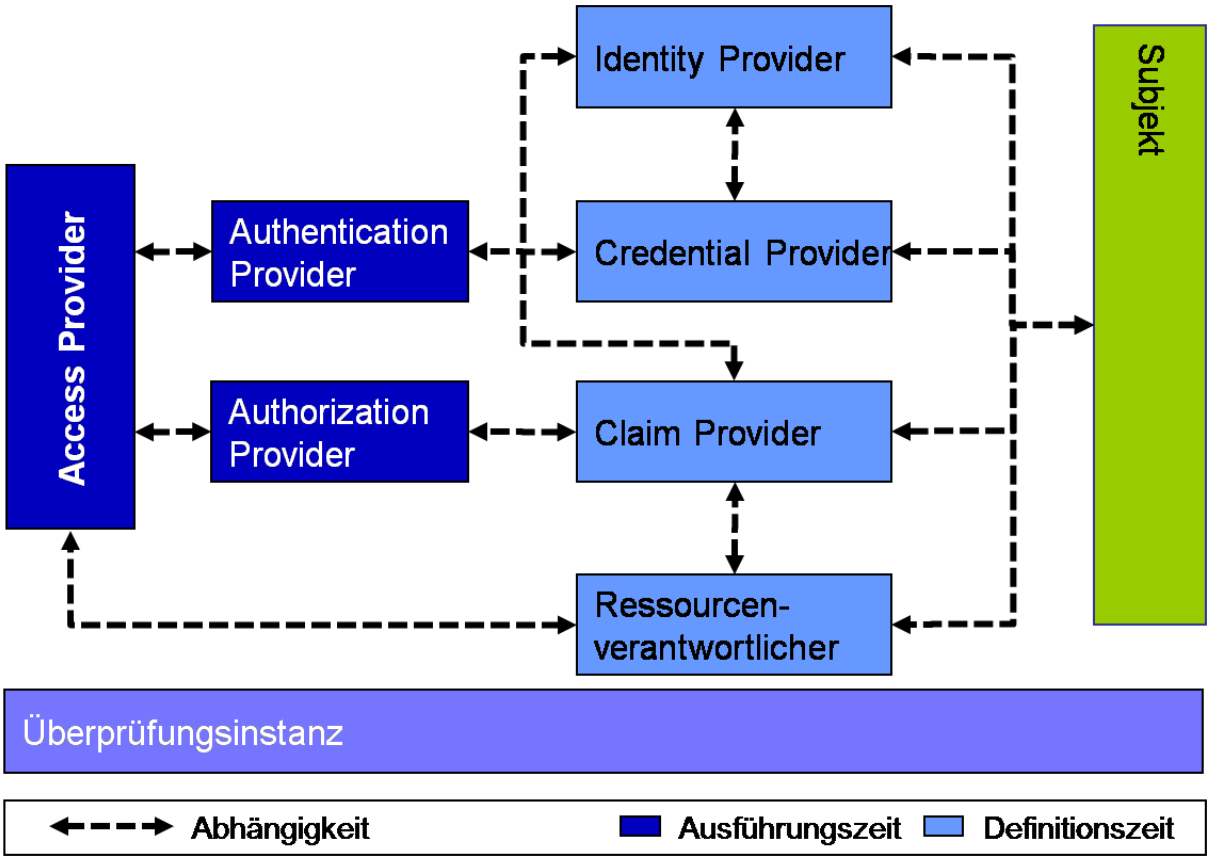

Abbildung 1: Geschäftsarchitektur

Prozesse zur Definitionszeit
Während der Definitionszeit werden alle notwendigen Bedingungen geschaffen, damit zur Zugriffszeit bestimmt werden kann, ob ein Subjekt auf eine Ressource zugreifen darf. Die Abläufe der „Definitionszeit“ müssen vor der ersten Benutzung der Ressource durch das Subjekt stattfinden:

Der Identity Provider stellt dabei die physische Identifizierung des Subjekts anhand der definierten Regeln sicher.

Auf Basis der Identität werden durch den Credential Provider Credentials bereitgestellt.

Der Claim Provider registriert die Informationen, welche er benötigt, um den Nachweis zu erbringen, dass ein Subjekt den angefragten Claim zur Ausführungszeit tatsächlich erfüllt.

Prozesse zur Ausführungszeit

Die aus Zugriffssicht relevante Stelle zur Ausführungszeit ist der Access Provider. Er steuert zentral den Zugriff auf die Ressource. Er beansprucht dazu die vom Authentication Provider und vom Authorization Provider bereitgestellten Dienste.

In der Grafik sind auch die Abhängigkeiten zwischen den Providern ersichtlich (gestrichelte Linien). Diese sind so zu verstehen, dass die Provider der Definitionszeit den Providern der Ausführungszeit die entsprechenden Daten (Zertifikate, Claims etc.) zur Verfügung stellen.

Jeder der angeführten Prozesse kann von unterschiedlichen Rollen, Organisationseinheiten, häufig gar Organisationen wahrgenommen werden (vgl. **Tabelle 1**). In den folgenden Kapiteln werden die Aufgaben der einzelnen Rollen (und damit implizit die Prozesse) kurz umschrieben.

Prozess	**Rollen**
Definitionszeit:	
Identity Management	Identity Provider
Credential Management	Credential Provider
Claim Management	Claim Provider
Rechte Management	Ressourcenverantwortlicher
Überprüfung der Rechtevergabe	Überprüfungsinstanz der Rechtevergabe
Ausführungszeit:	
Ressourcennutzung	Subjekt
Zugriffsprüfung	Access Provider
Authentifikation	Authentication Provider
Autorisierung	Authorization Provider

Tabelle 1: IAM-Prozesse und die zugehörigen Rollen bzw. Stellen

Vertrauensbeziehungen (Trust-Relationships)

Da die Management-Dienste in der Regel von fremden Organisationseinheiten oder Organisationen angeboten werden, müssen Vertrauensbeziehungen zwischen den einzelnen Providern hergestellt werden. Dies geschieht üblicherweise, indem entsprechende Verträge ausgehandelt werden. Diese überschreiten häufig Netzwerkgrenzen. In den gesamten Authentifikations- und Autorisierungsprozess werden nur Dienste von Providern einbezogen, zu denen eine Vertrauensbeziehung besteht. Angaben von anderen Providern werden nicht akzeptiert.

3.2 Allgemeine Entwurfsprinzipien

Die Prozesse und Funktionen für die Vergabe von Identifikatoren, die Herausgabe von Credentials, die Vergabe von Claims und die Zuordnung von Rechten zu den Claims können unabhängig voneinander von verschiedenen Organisationen verwaltet und die zugehörigen Ressourcen technisch unabhängig voneinander implementiert und betrieben werden.

3.3 Identity Provider (IdP)

Der Identity Provider vergibt digitale Identitäten.

Aufgaben:

- Verwaltung der Identitäten mit geeigneten Massnahmen zur Vermeidung von Doubletten
- Bereitstellen eines Auskunftsdienstes
- Der Identity Provider definiert und publiziert:
    - die Policy für die Vergabe, Verwendung und Verwaltung von Identitäten
    - die Qualität der Identifikation
    - den Gültigkeitsbereich der herausgegebenen Identitäten
    - den Prozess der Identifikation
    - die Bedingungen für die Nutzung durch die Partner

Design Prinzipien:

- Es kann unterschiedliche ID-Management-Provider geben.
- Der ID-Provider kann das Format des Identifikators frei wählen.
- Die Möglichkeit den Dienst zu überwachen und zu auditieren muss durchgängig vorhanden sein.

3.4 Credential Provider

Der Credential Provider gibt Mittel zur Überprüfung von digitalen Identitäten aus.

Aufgaben:

- Passende Credentials für eine Identität bereitstellen

- Verwalten der Verbindung zwischen Identität und Credentials

Design Prinzipien:

- Es kann unterschiedliche Credential-Provider geben.
- Die Credentials können sich bezüglich der technologischen Ausgestaltung und des damit erreichten Security-Levels unterscheiden. Der Trust-/Security-Level des Credentials ist definiert und publiziert.
- Die Prozesse für die Ausgabe, nach Verfall und Missbrauch von Credentials sind definiert.

3.5 Claim Provider (CP)

Der Claim Provider verwaltet die Informationen, die nötig sind, um zu überprüfen, ob ein Subjekt zu einem gegebenen Zeitpunkt einen Claim erfüllt.

Aufgaben:

- Verwaltung der Claim-Datenbank.
- Überprüfung, Registrierung bzw. Löschung von Claims, d.h. der Aussagen, dass eine bestimmte Identität einen definierten Claim erfüllt.
- Bestätigung der verwalteten Claims gegenüber autorisierten Anfragern.
- Definition der Prozesse für die Ausgabe, nach Verfall und Missbrauch von Claims.

Design Prinzipien:

- Der unterstützte Trust-Level für die Claim-Bestätigung ist definiert.

3.6 Authentication Provider

Der Authentication Provider stellt einen Dienst bereit, der anhand eines Credentials die Authentizität einer behaupteten digitalen Identität überprüft.

Aufgaben:

- Stellt einen elektronischen Dienst für die Authentifikation (Authentication Service) bereit.
- Verwaltet und dokumentiert die Vertrauensbeziehungen zu den Identity und Credential Providern, die er unterstützt.
- Dokumentiert die von ihm unterstützten Trust-Levels und Sicherheitstechnologien.

Design Prinzipien:

- Der Authentication Provider arbeitet zur Erbringung seiner Leistung mit den relevanten Identity und Credential Providern zusammen.

3.7 Authorization Provider

Der Authorization Provider stellt einen Dienst bereit, der überprüft ob und wie ein Subjekt auf eine Ressource zugreifen darf .

Aufgaben:

- Stellt einen elektronischen Dienst für die Autorisierung bereit.
- Verwaltet die Vertrauensbeziehungen zu den von ihm unterstützten Access und Claim Providern.
- Dokumentiert die von ihm unterstützten Claims.
- Verwaltet die Autorisierungsanforderungen für den Zugriff auf die von ihm verwalteten Ressourcen, welche ihm von den Ressourcenverantwortlichen gemeldet werden.

Design Prinzipien:

- Es werden Claims unterstützt, welche von diversen, unabhängigen Claim Providern verwaltet werden.
- Die Autorisierungsregeln werden ausschliesslich für Claims, nie für konkrete Subjekte definiert.

3.8 Access Provider

Der Access Provider stellt einen Dienst bereit, der einen Aufrufer authentifiziert und nur dann an die Ressource weiterleitet, wenn er darauf zugreifen darf.

Aufgaben:

- Stellt einen elektronischen Dienst - den Access Service - bereit, der die Durchsetzung der Vorgaben für die Absicherung der Zugriffe auf die von ihm bedienten Ressourcen gewährleistet.
- Verwaltet die Vertrauensbeziehungen zu den unterstützten Authentication und Authorization Providern.
- Gewährleistet, wenn gefordert, die lückenlose Dokumentation aller Zugriffe (Auditing) inkl. der Qualität der benutzten Credentials.

Design Prinzipien:

- Der Access Provider unterstützt unterschiedliche - idealerweise alle relevanten - Identity, Credential und Claim Provider.
- Der Access Provider unterstützt alle gängigen Trust-Levels.
- Der Access-Provider unterstützt idealerweise alle relevanten Sicherheitstechnologien (z.B. Passworte, elektronische Zertifikate, One Time Passworte für die Authentifikation).
- Der Access Provider kann die Rollen eines Authentication Providers und eines Authorization Providers übernehmen.

3.9 Ressourcenverantwortlicher

Der Ressourcenverantwortliche definiert, wer auf die Ressource zugreifen darf.

Aufgaben:

- Der Ressourcenverantwortliche ist die verantwortliche Stelle für die Vergabe von Rechten an Claims für den Zugriff auf die von ihm verwalteten Ressourcen.
- Der Ressourcenverantwortliche bestimmt die Sicherheitsanforderungen an die von ihm verwalteten Ressourcen und gibt diese dem Authorization Provider bekannt. Er definiert insbesondere:
  - den von der Ressource geforderten Trust-/Security-Level,
  - welchen Identity, Credential und Claim Providern die Ressource vertraut wird (d.h. von welchen Ausgabestellen Identitäten, Credentials und Claim-Bestätigungen akzeptiert werden),
  - welche Claims ein Subjekt erfüllen muss, um auf die Ressource zugreifen zu dürfen,
  - welche Rechte abhängig von den Claims beim Zugriff auf die Ressource gewährt werden,
- Der Ressourcenverantwortliche sorgt für die benutzerfreundliche Präsentation der Benutzungs- und Haftungsbestimmungen, welche für die Benutzung der Ressource gelten.

Design Prinzipien:

- Rechte werden immer ausschliesslich an Claims vergeben (bzw. eine Kombination davon), nie an Benutzer direkt.
- Administratoren sind den gleichen Security-Anforderungen (Zugriff und Autorisierung) unterworfen, wie andere Subjekte. Auch für die Verwaltungsaufgaben werden spezielle Claims definiert. Dieses Prinzip gilt für alle Subjekte und Ressourcen, z.B. auch für die Verwalter von Identitäten, Credentials und Claims.

3.10 Überprüfungsinstanz der Rechtevergabe

Die Überprüfungsinstanz stellt systemübergreifend sicher, dass die Rechte konsistent mit den Richtlinien für die Zugriffsgewährung vergeben werden.

4 Informationssystem-Architektur

4.1 Datenarchitektur

Die folgende Grafik zeigt in UML-Notation [UML] die wesentlichen Datenobjekte aus dem Bereich IAM und deren Beziehungen:

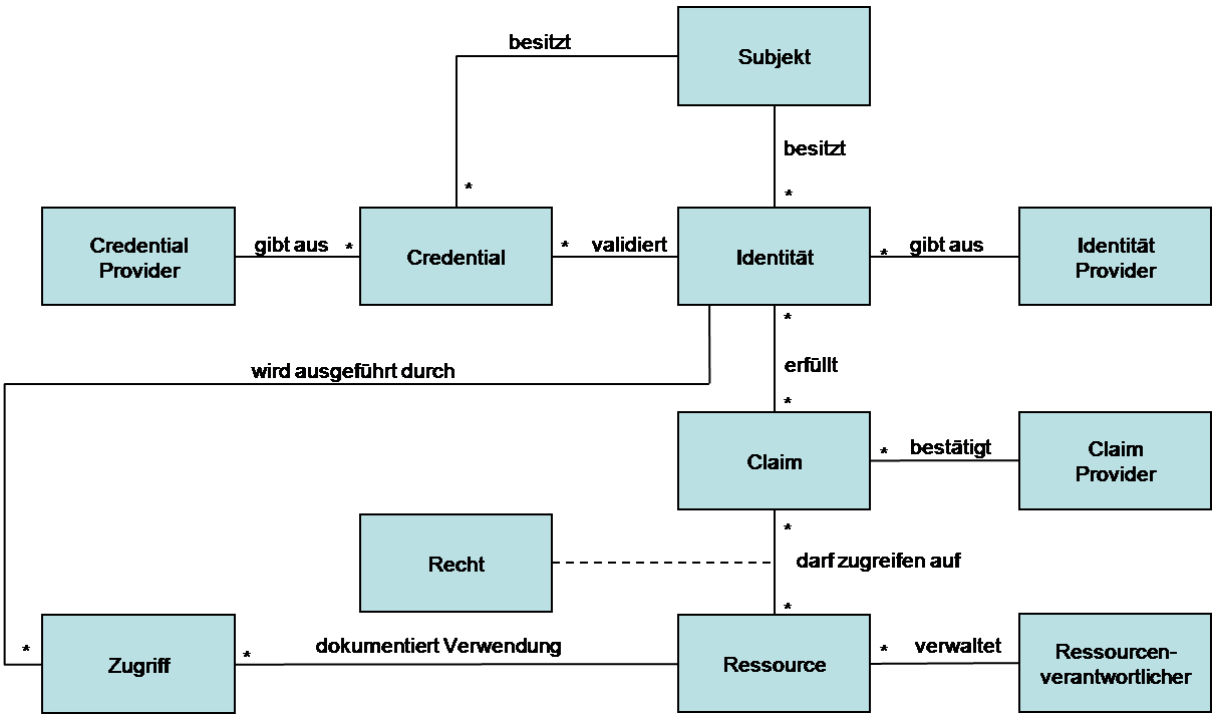

Abbildung 2: Datenarchitektur. *Ein Stern bedeutet „0 bis viele“. Ein ausgezogenes Linien-Ende ohne Stern bedeutet „genau 1“.*

Ein Subjekt kann mehrere Identitäten mit jeweils eigenen Identifikatoren besitzen. Jeder Identifikator wird üblicherweise von einem anderen Identity Provider herausgegeben.

Zu jeder Identität kann ein Subjekt mehrere Credentials besitzen, die evtl. unterschiedliche Qualität haben (z.B. Passworte, elektronische Zertifikate) und von Providern mit unterschiedlichen Sicherheitspolicies herausgegeben werden. Zu beachten ist, dass Credentials auch bereits bestehenden Identitäten zugewiesen werden können, d.h. die Identifizierung ist nur einmal notwendig, es können jedoch beliebig viele Credentials verwendet werden.

Ein Subjekt wird üblicherweise mehrere Claims erfüllen, z.B. in verschiedenen Rollen aktiv sein, wobei in der Regel nicht alle vom selben Claim Provider herausgegeben (bestätigt) werden.

Die Rechte werden vom Ressourcenverantwortlichen verwaltet. In den Rechten wird festgehalten, welcher Claim (oder welche Claim-Kombination) wie auf die Ressource zugreifen darf.

Jeder Zugriff eines Subjekts auf eine Ressource wird - soweit verlangt - dokumentiert. Die Summe der Zugriffsinformationen erlaubt die rechtlich geforderte, auditierbare Nachvollziehbarkeit. Die Zugriffsinformation kann auch für andere Zwecke, z.B. die Verrechnung von Leistungen und statistische Auswertungen herangezogen werden.

Diese Objekte sind in Kapitel 1.2 detailliert beschrieben.

4.2 Anwendungs-Architektur

4.2.1 Übersicht

Die Informationssystem-Architektur ist durch die in der folgenden Abbildung dargestellten Komponenten definiert. Es gibt eine klare Trennung zwischen Management Services (hellblau dargestellt) und operativen Services. Für den operativen Ablauf eines Zugriffes auf eine Ressource werden primär die operativen Services benötigt. In manchen Fällen benutzt das Subjekt eine Hardwarekomponente (z.B. Smartcard, Memory Stick) zur Speicherung seiner Credentials, wobei die Anwendung auf der Hardwarekomponente mit dem Client zusammenarbeitet.

Der Zugriff des Authentifikations-Services und des Autorisierungs-Services auf die entsprechenden Management Services kann je nach Anbieter direkt (synchrones Service) oder indirekt (der Management Service liefert die Daten im Sinne einer Replikation) sein.

Das Access-Service in diesem Modell entspricht, dem oftmals in der Literatur verwendeten Begriff dies Policy Enforcement Point (PEP). Der PEP ist dafür zuständig, dass die Einhaltung der definierten Policy auch durch technische Mittel garantiert wird (z.B.: durch transaktionsähnlich abgesicherte Abläufe usw.)

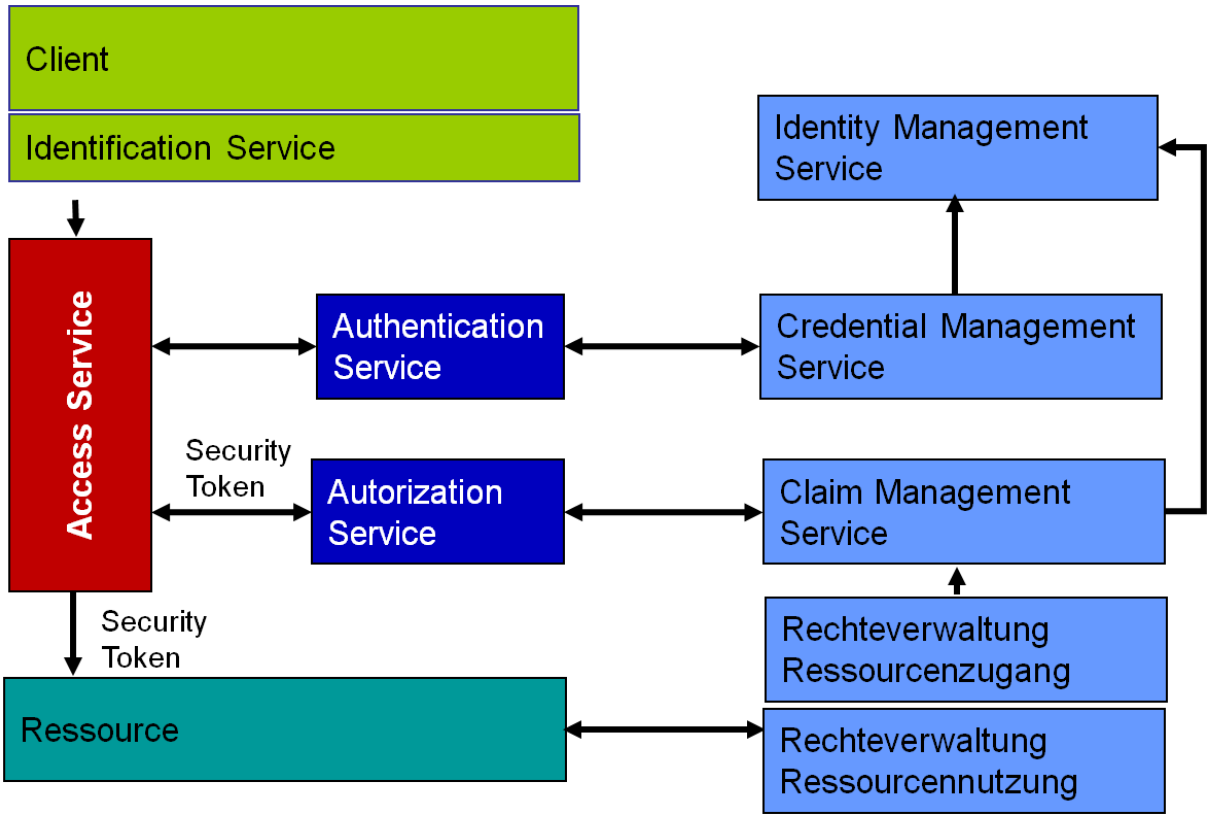

Abbildung 3: Anwendungsarchitektur

Die Rechteverwaltung steuert einerseits den Zugang zur Ressource sowie andererseits den fein-granularen Zugriff auf die, von der Ressource bereitgestellten Funktionen.

Nachfolgend werden die allgemeinen Design Prinzipien und danach die einzelnen Komponenten im Detail beschrieben.

4.2.2 Allgemeine Design Prinzipien

- Die IAM-Infrastrukturen sind modular und skalierbar aufgebaut
- Die Services arbeiten über standardisierte Schnittstellen zusammen, welche offene Standards (z.B. ‚Security Assertion Markup Language' (SAML)) benutzen.
- Ressourcen nutzen für die Authentifikation und Grob-Autorisierung ausgelagerte Dienste.
- Die je nach Benutzeranforderungen nötigen unterschiedlich starken Authentisierungsverfahren können auf derselben IAM-Infrastruktur realisiert werden.
- Bestehende Infrastrukturen können integriert werden.
- Die Authentifikation und Autorisierung für den Ressourcenzugang basiert auf im Anwendungskontext standardisierten und beglaubigten Identifikatoren, Credentials und Claims.
- Die Menge der genutzten Identifikatoren, Credentials und Claims ist minimal zu halten und womöglich zu konsolidieren.

  - Wenn immer möglich sind allgemein gültige Identifikatoren, Credentials und Claims für die Steuerung der Zugriffsrechte zu benutzen.
  - Föderative Konzepte erlauben den Aufbau von Vertrauensbeziehungen (Trusts) mit anderen Domänen und die Nutzung anderswo definierter Identifikatoren, Credentials und Claims.
- Der Autorisierung für einen Zugriff auf eine Ressource muss (sofern fachlich nötig) die Authentifikation des zugreifenden Subjekts vorausgehen.
- Wenn fachlich nicht notwendig werden keine Informationen zum zugreifenden Subjekt an die Ressource weitergegeben. (Die Autorisierung wird in jedem Fall allein auf Grund der angegebenen Claims vorgenommen.)
- Zur Förderung der Wiederverwendung soll der Zugriff auf Claim-Daten über standardisierte Protokolle und Schnittstellen erfolgen.

4.2.3 Management Services

4.2.3.1 Identity Management Service

Das Identity Management Service stellt elektronische Identitäten aus und verwaltet sie.

Aufgaben:

- Stellt Funktionen zur Ausgabe und Verwaltung von elektronischen Identitäten bereit.
- Begrenzt die Lebensdauer von elektronischen Identitäten.
- Gibt mindestens den vertrauenswürdigen Authentication Service Providern elektronischen Zugang zu ihren Identitätsinformationen.

4.2.3.2 Credential Management Service

Das Credential Management Service gibt Credentials aus und verwaltet sie. Die Credentials können von unterschiedlichem Typ sein und sind auf ein bestimmtes Subjekt ausgestellt.

Aufgaben:

- Stellt Funktionen zur Ausgabe und Verwaltung der Credentials zur Verfügung.
- Ermöglicht die Überprüfung der Gültigkeit der verwalteten Credentials und der Zugehörigkeit zu einem Identifikator.
- Begrenzt die Lebensdauer der von ihr ausgegebenen Credentials.
- Gibt mindestens den vertrauenswürdigen Authentifikations-Providern elektronischen Zugang zu ihren Credential-Informationen.

4.2.3.3 Claim Management Service

Der Claim Management Service dokumentiert zeitaktuell einen oder mehrere Claims für definierte Subjekte.

Aufgaben:

- Stellt Funktionen zur Verwaltung der Informationen bereit, welche nötig sind um zweifelsfrei bestimmen zu können, ob ein Subjekt (präzise: ein Identifikator eines Subjekts) einen definierten Claim erfüllt oder nicht (z.B. "Hans Meier ist Vermesser des Kantons Bern").
- Bestätigt elektronisch, ob ein bestimmter Claim einem Subjekt (präzise: einem Identifikator eines Subjekts) zugewiesen ist oder nicht.
- Gibt mindestens den vertrauenswürdigen Authorization Providern elektronischen Zugang zu den verwalteten Claim-Informationen.

4.2.3.4 Rechteverwaltung Ressourcenzugang

Die Rechteverwaltung für den Ressourcenzugang verwaltet die Zugriffsrechte auf eine Ressource, d.h. die Angaben darüber, welche Claims erfüllt sein müssen, damit ein Subjekt auf eine Ressource zugreifen darf (Grobautorisierung).

Aufgaben:

- Stellt Funktionen zur Verwaltung der Informationen bereit, welche Claims auf welche Ressource zugreifen dürfen.
- Gibt den vertrauenswürdigen Authorization Services elektronisch Zugang zu den verwalteten Autorisierungsinformationen.

4.2.3.5 Rechteverwaltung Ressourcennutzung

Die Rechteverwaltung für die Ressourcennutzung hält fest, welche Claims/Rollen welche Funktionen der Ressource aufrufen dürfen (Feinautorisierung).

Aufgaben:

- Stellt Funktionen zur Verwaltung der Informationen bereit, welche Claims ein Subjekt erfüllen muss, damit es auf die jeweilige Funktion der Ressource zugreifen darf.
- Gewährt der Ressource elektronisch Zugang zu die sie betreffenden Autorisierungsinformationen.

4.2.4 Access Services

4.2.4.1 Client

Der Client greift auf eine Ressource zu und authentisiert vorgängig sofern nötig das zugreifende Subjekt. Er delegiert die Authentisierung an einen Identification Service oder übernimmt selbst dessen Aufgaben.

Schnittstelle:

Out: Identifikator, Credential, [Claims]

Aufgaben:

- Ruft optional zur Authentisierung den Identification Service auf.
- Ruft die Ressource auf und übergibt ihr dabei Identifikator und Credential, evtl. auch bestätigte Claims des aufrufenden Subjekts.
- Falls es sich beim Client um eine Benutzeroberfläche handelt:
  Publiziert die Haftungsbestimmungen beim Login, wenn verlangt.

4.2.4.2 Identification Service

Der Identification Service erlaubt dem Subjekt, sich zu authentisieren, beispielsweise über Abfrage von Benutzer-Id und Passwort, eines One-Time-Passworts oder durch Auslesen der nötigen Informationen aus einer Smardcard…).

Schnittstelle:

Out: Identifikator, Credential, [Claims]

Aufgaben:

- Optional: Fragt die aufzurufende Ressource, welche Claims und Trust/Security-Levels für den Zugriff nötig sind.
- Authentisiert das Subjekt gemäss dem verlangten Trust/Security-Level (z.B. durch Login).
- Falls es sich beim Client um eine Benutzeroberfläche handelt:
  Publiziert die Haftungsbestimmungen beim Login, wenn verlangt.

4.2.4.3 Access Service

Der Access Service authentifiziert das zugreifende Subjekt und weist den Zugriff ab, wenn es nicht das Recht dazu hat.

Schnittstelle:

In: Identifikator, Credential, [Claims], Ressource

Out: Security Token

Aufgaben:

- Informiert auf Anfrage den Client über benötigte Sicherheitsinformationen (z.B. benötigte Claims, geforderter Trust-Level) bezüglich des Zugriffs.
- Ruft zur Authentifikation einen Authentifikation Service auf und bricht ab, wenn die Authentifikation nicht erfolgreich war.
- Ruft zur Überprüfung der Autorisierung einen Autorisierungs-Service auf und bricht ab, wenn für das aufrufende Subjekt (das Subjekt, für das der Identifikator steht) keine Claims mit Zugriffsrecht auf die Ressource gefunden werden können.
- Gibt im Security Token die geprüften Authentifikations- und Autorisierungsinformationen an die aufzurufende Ressource weiter.
- Erzeugt und verwaltet für Audit-Zwecke, wenn gefordert, die Zugriffsinformationen. Diese enthalten alle notwendigen Daten, welche für die vollständige Nachvollziehbarkeit benö-

tigt werden. Diese Informationen können bei Bedarf auch für Auswertungen, Verrechnungszwecke etc. herangezogen werden.

- Bietet rechtlich verifizierte und verifizierbare Audit- und Monitoring-Funktionen.
- Arbeitet optional mit dem Lizenzmanagement zusammen, z.B. um den Zugriff zu verweigern, wenn die maximale Anzahl von Concurrent Usern erreicht ist.

Design Prinzipien

- Falls das Subjekt keine Rechte für die aufzurufende Anwendung hat, wird der Aufruf nicht an die Ressource weitergeleitet.
- Der Access-Service funktioniert über Netzwerkzonen und Domänengrenzen hinweg.
- Er kann eingesetzt werden zur Sicherung der Zugriffe auf unterschiedlichste Ressourcen.
- Bei Bedarf kann er mit mehr als einem Authentifikations-Service und Autorisierungs-Service zusammenarbeiten.
- Soweit vom Trust-Level her möglich, können bestehende Identitäten, Credentials und Claims von anderen Stellen übernommen werden (Föderation).

4.2.4.4 Authentifikations-Service

Der Authentifikations-Service überprüft mittels des Credentials, ob der Zugreifende der ist, der er behauptet zu sein.

Schnittstelle:

In: Identifikator, Credentials

Out: Überprüfte Id, Angabe, ob die Überprüfung der Identität positiv ausgefallen ist, oder nicht

Aufgaben:

- Überprüft, ob die gelieferten Credentials zur Identität zu gelieferten Identifikator gehören
- Bestätigt im positiven Fall die Identität des aufrufenden Subjekts.

4.2.4.5 Autorisierungs-Service

Der Autorisierungs-Service prüft, ob der Aufrufer das Recht hat, auf die Ressource zuzugreifen.

Schnittstelle:

In: Überprüfte Id, Credentials, Ressource, [Claims]

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

Aufgaben:

- Eruiert die Claims, welche Zugriff auf die Ressource haben (sofern nicht als Eingabeparameter übergeben)

- Überprüft, ob die überprüfte Id einen oder mehrere der, von der Ressource geforderten Claims erfüllt.
- Erzeugt ein Security Token für das Subjekt mit der überprüften Id und den im Zugriffskontext relevanten, bestätigten Claims.
- begrenzt die Lebensdauer des Security Tokens.

Design Prinzipien

- Es werden Claims (Rollen oder Attribute) von unterschiedlichen Claim Management Services akzeptiert.
- Falls die Ressource nicht wissen muss, wer auf sie zugreift, wird die Id nicht in das Security Token aufgenommen.

4.2.4.6 Ressource

Die Ressource gibt dem aufrufenden Subjekt gerade so viele Funktionen frei, wie er gemäss den ihm zugewiesenen Rechten nutzen darf.

Schnittstelle:

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

Aufgaben:

- Die Ressource nimmt ein standardisiertes Security Token entgegen und nimmt darauf basierend den Feinzugriff vor. Sie verhindert einen Zugriff, wenn das Subjekt auf Grund der im Security Token gelieferten Informationen dazu nicht autorisiert ist.
- Die Funktionalitäten der Authentisierung und der Autorisierung sind von der aufgerufenen Ressource getrennt.
- Die Definition der Berechtigungen geschieht ausschliesslich auf Grund von Claims, welche der Ressource übergeben werden.
- Die Ressource bietet - wo gefordert - rechtlich verifizierte und verifizierbare Audit- und Monitoring-Funktionalitäten.

Bemerkungen:

Dadurch, dass die Ressource über standardisierte Interfaces und Standard-Security Token aufgerufen wird, ist sie bei Bedarf in Portale einbindbar.

5 Domänen und ihr Zusammenspiel

E-Government erfordert die elektronische Zusammenarbeit über Organisationsgrenzen hinweg. Eine Möglichkeit, die daraus entstehenden IAM-Probleme zu lösen, besteht darin, dass jedes Subjekt in jedem Anwendungskontext separat mit einem Identifikator ausgezeichnet wird, ein eigenes Credential bekommt und den relevanten Claims/Rollen zugewiesen wird. Jeder Anwendungskontext wird als eigene, isolierte *Domäne* (ein „Silo“) behandelt. Für alle Beteiligten steigt damit der Aufwand. Die Subjekte müssen mit einer Unzahl von Identitäten und Credentials umgehen. Der Verwaltungsaufwand für die Rechteverwaltung wird enorm. Gleichzeitig steigt die Gefahr von Fehlern und Missbrauch.

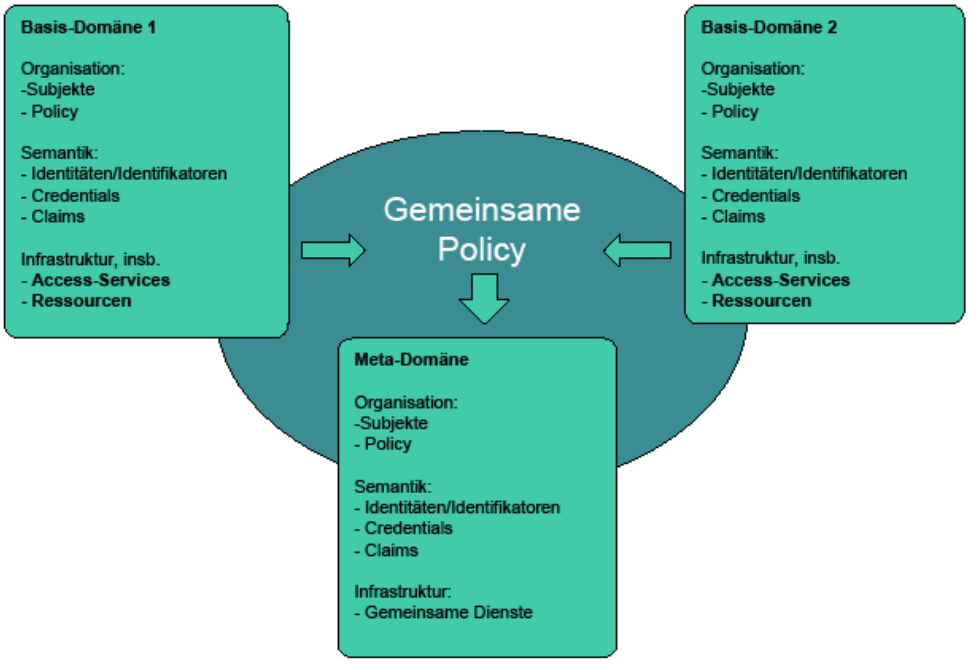

Abbildung 4: Domänen und ihr Zusammenspiel

Ein anderer Lösungsansatz ist in den meisten Fällen vorzuziehen (vgl. Abbildung 1): Möchten verschiedene Organisationen zusammenarbeiten, legen sie in einer gemeinsamen Policy fest, wie sie bestehende Definitionen (insb. Identitäten, Credentials und Claims) gemeinsam nutzen möchten. D.h. sie bilden eine gemeinsame Meta-Domäne mit einer eigenen Policy, welche für alle Beteiligten bindend ist. Die Meta-Domäne regelt u.a. folgende Punkte:

- Welche Subjekte gehören zur Domäne?
- Wie werden die Subjekte der Domäne eindeutig identifiziert?
- Welche Credentials mit welcher Qualität werden zur Authentifikation der Subjekte akzeptiert?
- Welche Claims mit welcher Qualität werden für Zugriffe auf Ressourcen der Domäne benötigt?
- Welchen Identity, Credential und Claim Providern wird vertraut?

5.1 Design Prinzipien

- Die Policy einer Domäne ist schriftlich festzuhalten und für alle Teilnehmer der Domäne zugreifbar zu publizieren.
- Die Menge der Domänen ist minimal zu halten. Wo möglich soll man sich an eine vorhandene übergeordnete Domäne anschliessen, statt eine eigene neue zu definieren.
- Wo möglich sollen vorhandene Identitäten, Credentials und Claims wiederverwendet werden (z.B. durch Föderierung, ein gemeinsames Meta-Directory…).
- Wo möglich sollen vorhandene Identity, Credential und Claim-Provider berücksichtigt werden.

6 Umsetzung

Die vorliegenden Entwurfsprinzipien beschreiben – wie der Titel nahelegt – wie ein E-Government-kompatibles IAM-System gestaltet werden sollte. Es beschreibt nicht eine konkrete Lösung. Bei der Umsetzung sind eine Reihe von zusätzlichen Ergebnissen zu erstellen, u.a.:

- Messbare Anforderungsdefinitionen
- Datenschutz- und Datensicherheitskonzept
- Rollenkonzepte
- Policies
- Lösungsarchitektur.

-

7 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.

8 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

[IAM Wiki] www.iam-wiki.org

[UML] http://www.uml.org/

[TOGAF] http://www.opengroup.org/togaf/

Anhang B – Mitarbeit & Überprüfung

Fischer Markus	
Gantenbein Reto	Sun Microsystems (Schweiz) AG
Häni Hans	TG
Itin Markus	ZH
Jensen Rüdiger	Swisstopo
Lambelet Erich	BEDAG
Lippuner Mathias	SG
Mathys Wolfram	BEDAG
Meyer Elias	Abraxas
Müller Willy	ISB
Ottinger Vincent	Genève
Perroud Thierry	BIT
Petralia Andreas	Adnovum
Ueltschi Andreas	Sun/Oracle

Anhang C – Abkürzungen

IAM	Identity und Access Management
IdP	Identity Provider
CP	Credential Provider
UML	Unified Modelling Language
PEP	Policy Enforcement Point
SAML	Security Assertion Markup Language
TOGAF.	The Open Group Architecture Framework

Anhang D – Glossar

Vgl. Kap. 1.2