Fachgruppe Identity & Access Management IAM

Referenzmodell IAM

(Whitepaper No.: IAM-2007-01)

Version V 1.1

(Autoren: N. Haenni, M. Itin, V. Kulhavy, H. Rüger, C. Winteregg)

eCH

23. April 2007

Inhaltsverzeichnis

0. Verwaltung des Dokumentes

Identifikation des Dokumentes

Filename	eCH_Referenzmodell_IAM_V_1_1.doc

Autoren

Identification Code	Name	Firma
CW	Christophe Winteregg	Novell Schweiz AG
NH	Nicolas Haenni	Kanton Genf
MI	Mark Itin	Kanton Zürich
HR	Hubert Rüger	Siemens Enterprise Communications AG (bis 2006 HVC)
VK	Vladimir Kulhavy	Siemens Enterprise Communications AG

Änderungen

Datum	Version	Autor	Status	Änderungsgrund
23.04.07	1.1	NH	Publikation	-
18.04.07	1.0i	MI, CW, NH	Endversion	Eingliedern von Identity Federation + Enddokument erstellen
29.03.07	1.0h	Alle	In Bearbeitung	Review 070329 (Skype)
14.03.07	1.0e	Alle - Vladi	In Bearbeitung	
13.12.06	1.0d	Alle	Feedback SUN	Review SUN Microsystems
17.11.06	1.0	Alle	Released	Release durch Research Gruppe (interner release: 1.0c)

Verteiler

Name	Organisation
Fachgruppe IAM Research	eCH

1. Research Team

Das Research Team hatte zur Aufgabe, das Umfeld der bestehenden oder entstehenden Standards, Normen und "best practices" für IAM zusammenzustellen. Da kein bestehender Standard übernommen wurde, musste anhand der Recherche-Ergebnisse ein Referenzmodell zusammengestellt werden, um alle Bereiche des IAM abzudecken.

Es zeigt sich, dass viele bestehende Standards sich auf einzelne Aspekte oder technische Bereiche des Identity Management oder des Access Management konzentrieren. Insbesondere orientieren sich die Standards (vorgeschlagene und akzeptierte) an existierenden (technischen) Lösungen (z.B. PKI), die aber die „business“ und „soziale“ Problematik unbehandelt lassen. In den meisten Ansätzen wird das Thema Identity Management entweder nicht behandelt oder man geht davon voraus, dass es bereits existiert.

Die Arbeiten der Gruppe beinhalten die folgenden Themen:

- **Ziel des IAM festlegen und Arbeitshypothesen aufsetzen**
  Dies erlaubt die Wahl und Analyse der relevanten Standards nach Relevanz zu kategorisieren.

  > Im IAM geht es darum, den Berechtigten einen Zugriff auf Informationsressourcen und Anwendungen zu ermöglichen. Dabei müssen die Prinzipien der *Authentizität*, *Vertraulichkeit* und *Integrität* der Information und die *Nichtabstreitbarkeit* des Zugriffs garantiert werden. Dies impliziert, dass Relevanz, Vertraulichkeit, persönlicher Daten und Datenschutzbestimmungen beachtet werden müssen.

  Die Arbeitshypothesen bauen auf gesellschaftlichen (nicht technischen) Gewohnheiten von natürlichen und juristischen Personen und deren Handhabung von Identitäten auf.
- **Relevante Standards und Forschungsergebnisse**
  Dies beinhaltet eine Zusammenstellung der relevanten Standards unter Beachtung unserer Hypothesen und dient der Zusammenstellung des Referenzmodells.
- **Referenzmodell**
  Das Referenzmodell dient einer übergeordneten Zusammenstellung sowohl der Handhabung von Identitäten und Rollen wie auch der Verteilung und Überprüfung der Identitäten. Das Modell dient der Zuordnung der existierenden Standards und gilt als Referenz, welche eine Standardisierung von IAM beinhalten sollte. Sie garantiert die Unabhängigkeit der Instanzen Identitätenverwaltung, Autorisierung und Authentisierung bei Ressourcenzugriff.

Als nächste Schritte wäre es empfehlenswert, Arbeitspakete zu definieren und Abstimmungen mit anderen Arbeitsgruppen zu erreichen.

Als Arbeitspakete können Anwendungsbereiche wie Online-Taxation, Lohnmeldewesen, EJPD-Anwendungen oder Strafregister compliance dienen. Als weitere Arbeitsgruppen, auf die man sich abstimmen sollte (auch solche ausserhalb von eCH), sind insbesondere Glossare, PKI, eCH: Meldewesen, Bundesapplikationen: Flüchtlingswesen, InfoStar denkbar.

2. Ziel des IAM

Die grundlegende Mission des IAM ist, einen kontrollierten Zugriff auf Informationsressourcen und Anwendungen unter Berücksichtigung nicht technischer Randbedingungen zu ermöglichen.

Dabei müssen folgende Punkte beachtet werden:

- **Sicherheitskriterien:** Authentizität, Vertraulichkeit, Integrität, Nichtabstreitbarkeit
- **Relevanz der Information:** Um diesen Punkt zu erfüllen, müssen vorgängig die Informationen kategorisiert sein in z.B. öffentlich, intern, vertraulich, geheim, etc.
- **Missbrauchsgefahr.** Es muss wirkungsvoll verhindert werden, dass unberechtigte Personen Zugang auf nicht für sie erlaubte Informationen haben.
  - Das **„need-to-know-Prinzip“** muss daher bei den Berechtigungen der Benutzer umgesetzt sein.
  - Das **„Eigentümerprinzip“** garantiert auf der Anbieterseite, dass für jedes System klar definierte Hoheitsrechte existieren (Aufgaben, Verantwortung, Kompetenz).
  - Damit sind die **Verantwortlichen bekannt**, welche für die korrekte Verwendung ihrer Systeme sorgen und bei Vorfällen zur Rechenschaft gezogen werden können.
- **Datenschutz:** Bei der Verwendung einer einheitlichen Identität besteht das Risiko, dass Einzelzugriffe auf Ressourcen über die Grenzen der Applikation hinweg in Zusammenhang gebracht werden können. Dadurch können unter Umständen bewusste Datenschutzmassnahmen in Frage gestellt werden.

3. Arbeitshypothesen

Um das Referenzmodell zusammenzustellen, müssen Arbeitshypothesen festgelegt werden, um anschliessend Grundsätze und Abgrenzungen des Modells festzuhalten. Die folgenden Arbeitshypothesen repräsentieren somit Einschränkungen, die von einem IAM Standard berücksichtigt werden sollten:

- Eine Person ist immer eineindeutig[1].
- Eine Person kann mehrere Identitäten haben.
- Es haftet die Person und nicht die Identität.
- Rollen sind Gruppierungen von Personen mit ähnlichen Verantwortlichkeiten, Aufgaben und Kompetenzen. Als Grundlage für solche Rollen können folgende Dimensionen dienen:
    - Organisationsstruktur
    - Funktion (Richtposition)
    - Ort (Location)
    - Dienstleistung (Service)

Grundsätzlich muss man von dem *Need-to-Know* Prinzip ausgehen. Dies bedeutet, dass nur diejenigen Informationen zur Verfügung gestellt werden, die notwendig sind, um in einem gewissen Kontext IAM zu realisieren und um Datenschutzanforderungen zu genügen. Die Verwendung der Information muss technisch und inhaltlich begründbar sein.

Ebenfalls muss beachtet werden, dass Identitäten "verloren gehen" und/oder "gestohlen" werden. Die Handhabung dieser Ereignisse muss von Anfang an berücksichtig werden.

Bei genauerer Betrachtung einer Identität ergeben sich daraus folgende Konsequenzen:

- Identitäten können mit zusätzlichen Informationen in Abhängigkeit von ihrem Gebrauch, bereichert werden.
- Es gibt materielle und immaterielle Repräsentationen von Identitäten:
    - Identitäten existieren nur innerhalb eines *Kontextes*.
    - Zugriffsbereiche von Identitäten können an andere *delegiert* werden.
    - Identitäten können von mehreren Personen gebraucht werden (gemeinsame Identitäten, Anforderung der Praxis).
- Identitäten setzen eine Haftung von natürlichen und juristischen Personen voraus. Die Instanz einer Identität ist die Instanz der Haftung.
- Es gibt technische Identitäten (Identitäten für Sachen), deren Haftung letztendlich von natürlichen oder juristischen Personen getragen wird.
    - Beispiel: CPU, Maschinen, Server, Transaktionen, Applikationen, etc.

Dieser Ansatz entspricht der Umsetzung des Eigentümerprinzips und deren eineindeutigen Koppelung mit den Personen[2].

---

1 Eine Möglichkeit eine Identität in die reale Welt zu referenzieren, könnte beispielsweise der eCH-Standard 0010 Postadresse einer natürlichen Person sein.

2 Damit ist auch die Haftung geregelt. Bemerkung: Aufgabe, Kompetenz, Haftung

4. Relevante Standards – Themenschwerpunkte

Wir haben uns mit dem Themenumfeld *Identität – Authentisierung – Autorisierung – Privatheit* befasst und mit Unterstützung aller Beteiligten der Fachgruppe *Identity & Access Management* zahlreiche internationale Standards sowie *SAGA.ch* beschafft und gesichtet. Generell lässt sich zusammenfassen, dass sich 'viele Experten dieser Welt' seit einiger Zeit profund mit dem Themenumfeld beschäftigen und auch beachtliche Grundlagen erarbeitet haben. Diese beziehen sich meist auf fach-, länder- oder beziehungsspezifische Anforderungen, d.h. sie geben wertvolle Hinweise zur Aufgabenstellung der *e*CH Fachgruppe IAM, ohne jedoch das Patentrezept pfannenfertig zu liefern.

In Anbetracht des äusserst breiten Spektrums, der sehr unterschiedlichen Anforderungen wie auch divergierender Anwendungsbereiche (scope), haben wir uns auf ein Auswahl relevanter Standards beschränken müssen und diese bis dato grob durchforstet. Insbesondere SAGA.ch ist technisch umfassend und ausgereift. Er kann den zukünftigen *e*CH Standard zu IAM in der Umsetzung ergänzen und unterstützen, auch durch die weit fortgeschrittenen Begriffsklärungen im Anhang *Glossar*.

Die folgenden Standards dienten als Grundlage zur Erarbeitung des eigenen Referenzmodells (Kapitel 6) und werden bei den weiteren Arbeiten berücksichtigt. Zudem wird deren Entwicklung aktiv verfolgt.

Die Standards mit ihren Themenschwerpunkten sind:

*e*CH	**SAGA.ch** (eCH-0014, Version 3-0) – **S**tandards und **A**rchitekturen für E-**G**overnment-**A**nwendungen Schweiz – *verdichtete, technische Richtlinien für die Umsetzung von eGovernment Anwendungen*
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik – *Grundschutz Handbuch*
	SAGA – Standards und **A**rchitekturen für E-**G**overnment-**A**nwendungen (Bundesministerium des Innern) – *E-Government Handbuch*
	SIGA – Sichere **I**ntegration von E-**G**overnment-**A**nwendungen - *E-Government Architektur*
CEN	**C**omité **E**uropéen de **N**ormalisation – Grundlage zu **PET P**rivacy **E**nhancing **T**echnologies und **IMS I**dentity **M**anagement **S**ystems – *Workshop Agreement, nicht offizieller CEN Standard*
LIBERTY ALLIANCE	Ein modellhafter Privacy & Security Best Practices Industriestandard mit Beteiligung von 150 Firmen, Fokus auf B2B resp. G2B, EU, Canada, USA
NIST	**N**ational **I**nstitue of **S**tandards and **T**echnology – US Department of Commerce – Electronic Authentication Guideline, 4 levels of authentication assurance
	RBAC – Role **B**ased **A**ccess **C**ontrol Implementation Standard, Draft, Jan. 06, mit den Komponenten Core RBAC, Hierarchical RBAC, Static Separation of Duty (SSD) Relations, Dynamic Separation of Duties (DSD) Relations.
	Personal **I**dentity **V**erification **PIV** Card Management Report → technical specifications for PKI smart card management system,
	Codes for the Identification of Federal and Federally Assisted Organizations
	Federal **I**nformation **P**rocessing **S**tandard
PRIME	**Pr**ivacy and **I**dentity **M**anagement for **E**urope – *White Paper* – Public Private Partnership, Europa

5. Kategorisierungsansätze der Standards

Diese Ansätze geben den Stand Nov. 06 wieder und werden im Rahmen der weiteren Arbeiten bedarfsgerecht vertieft beigezogen. Bisher zeichnet sich ab, dass Technologieaspekte bei Authentisierung, Autorisierung und Festlegung der Identität(en) stärker im Vordergrund stehen als Personen, Organisationen und Prozesse.

	Person/Organisationen (nat. & jur.)	Prozesse	Technologie
Authentisierung	BSI: 0	0	1
	SIGA: 0	0	4
	CEN: 0	0	0
	SAGA.ch: 1	3	5
	LIBERTY: 3	1	4
	NIST: 4	0	4
Autorisierung	BSI: 2 *	2*	3 *
	SIGA: 0	0	4
	CEN: 0	0	0
	SAGA.ch: 1	2	4
	LIBERTY: 3	1	4
	NIST: 0	0	0
Identität(en)	BSI: 0	0	1 *
	SIGA: 0	0	3
	CEN: 3 **	1**	3 **
	SAGA.ch: 0	0	0
	LIBERTY: 2	1	4
	NIST: 3	0	3

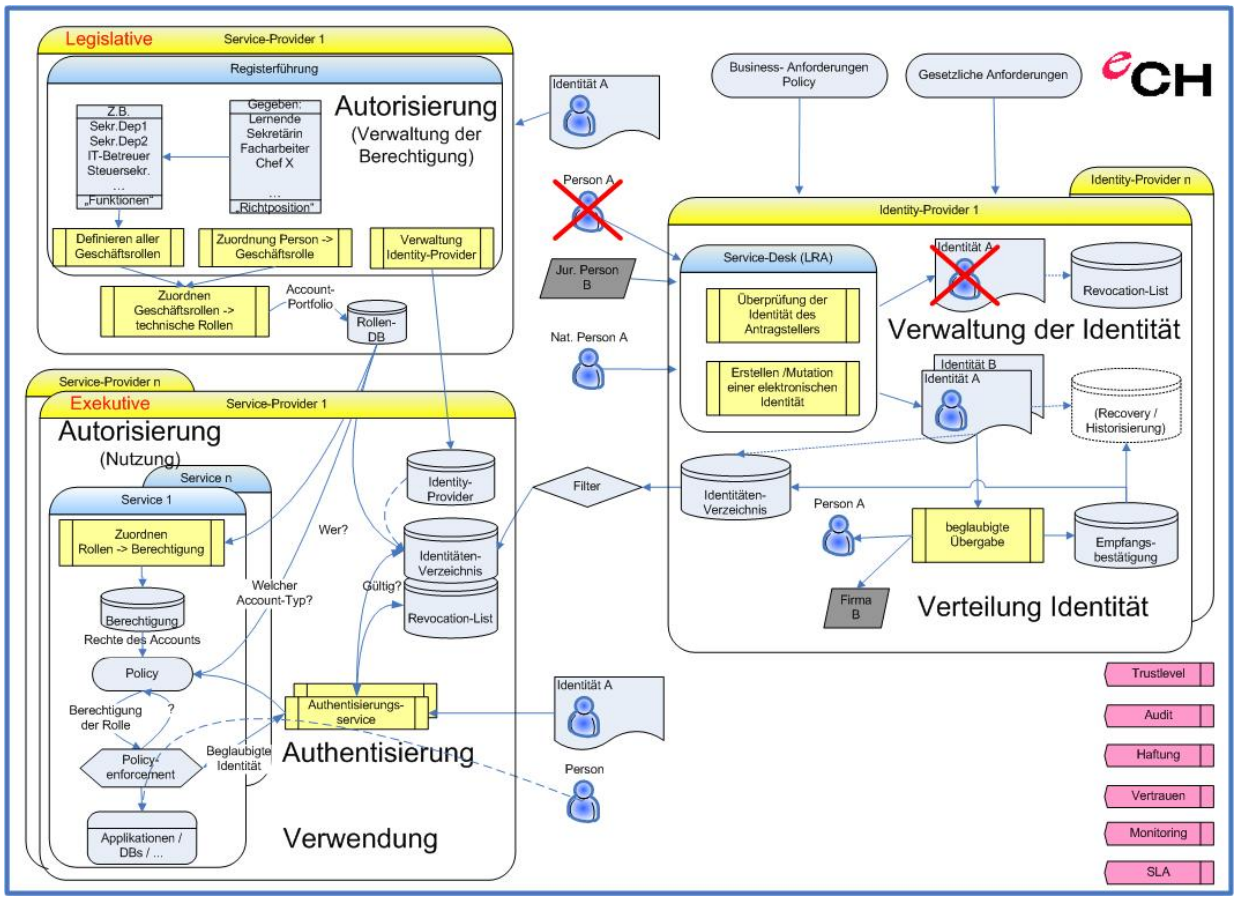
Maturitätslevel (angelehnt an COBIT):

0	nicht existent	nicht existent
1	Initial / Ad hoc	sehr wenig
2	Wiederholbar, aber intuitiv	wenig
3	definierte Prozesse	genügend
4	verwaltet und messbar	gut
5	optimiert	sehr gut

* zu wenig

** focus on 'pseudo-identity' → separation of data and identity protector

6. Management Summary



Kurzbeschreibung IAM-Modell

Rahmenbedingungen

Es wird von folgenden Rahmenbedingungen ausgegangen:

- Business Anforderungen
- Gesetzliche Anforderungen

Die Informatik-Infrastruktur soll die gewünschte Funktionalität bieten, welche benötigt wird, um den Geschäftszweck optimal zu unterstützen. Werden die Aufgaben von verschiedenen Partnern wahrgenommen, benötigt es neben einem guten Vertrauensverhältnis auch Vereinbarungen zwischen den beteiligten Partnern (SLA), welche die Aufgaben, Verantwortungen (Haftung) und Kompetenzen regeln. Ein Monitoring einzelner Teile des Prozesses oder bei Bedarf sogar des ganzen Prozesses soll machbar sein, für Audits müssen die nötigen Kontrollmechanismen implementiert sein.

Identity-Provider

Aufgabe	• Erstellung und Verwaltung einer digitalen Identität. • Sichere Übergabe dieser Identität an den rechtmässigen Besitzer. • Führen eines Verzeichnisses, welches über die gültigen und vorzeitig zurückgerufenen digitalen Identitäten Auskunft gibt.
Verantwortung	• Sicherstellen der Authentizität des Antragstellers. • Sicherer Betrieb der dazu benötigten Infrastruktur. • Optimale Prozesse über den gesamten Life-cycle einer digitalen Identität.
Kompetenzen	• Auswahl und Design der Infrastruktur und Prozesse.

Bemerkungen:

- Bei Bedarf können die Dienste von mehreren Identity-Provider genutzt werden.
- Der Identity-Provider kann innerhalb eines Unternehmens angesiedelt sein, es können auch die Dienste von externen Anbietern genutzt werden.

Service-Provider (Legislative)

Aufgabe	• Sicherstellen, dass ein Benutzer genau die Rechte erhält, welche er benötigt, um seine Aufgaben zu erfüllen. • Definition der Muss-Anforderungen an einen Identity-Provider. • Verwaltung der zugelassenen Identity-Provider und der mit ihnen ausgehandelten SLAs.
Verantwortung	• Optimale Prozesse über den gesamten Life-cycle der Rechte einer digitalen Identität. • Optimale Prozesse über den gesamten Life-cycle eines Identity-Providers.
Kompetenzen	• Auswahl und Design der Infrastruktur und Prozesse.

Service-Provider (Executive)

Aufgabe	• Technische Umsetzung des Zugriffs auf die entsprechenden Services (Wer darf was wann in welcher Qualität?) unter Berücksichtigung der Rahmenbedingungen.
Verantwortung	• Sichere Verfahren für Authentisierung und Autorisierung gemäss den Anforderungen des Service-Eigentümers. • Funktionstüchtige Infrastruktur gemäss SLA.
Kompetenzen	• Auswahl und Design der Infrastruktur und Prozesse für jeden einzelnen Service.

Bemerkungen:

- Ein Benutzer soll grundsätzlich die Dienste mehrerer Service-Provider mit seiner virtuellen Identität in Anspruch nehmen können.

Ein Service-Provider (Executive) kann eine oder mehrere Dienstleistungen zur Verfügung stellen, wobei die Dienstleistungen gesammelt oder einzeln, je nach SLA, verwaltet werden können.

7. Detailbeschreibung

7.1 Einführung

Das vorliegende Referenzmodell für ein übergeordnetes und skalierbares Identity und Access Modell sollte die folgenden Anforderungen erfüllen:

- Skalierbarkeit
- Multi Vender Fähigkeit
- Ermöglichung des Einsatzes von Standard Applikationen
- Konformität zu bestehenden Standards

Das nachfolgende Modell beschreibt das Identity und Access Modell in einer stark abstrahierten Weise und unterteilt das IAM in die folgenden Teilsysteme:

- Verwaltung der Identität
- Verteilung der Identität
- Rollenmanagement
- Verwendung der Identität

Neben dem Benutzer – sei es nun eine natürliche oder juristische Person – treten noch folgende Instanzen in Erscheinung:

- Der Identity-Provider. Er ist zuständig für die Erstellung und sichere Auslieferung der digitalen Identität an den Benutzer. Es können mehrere Identity Provider existieren.
- Der Service-Provider. Hier wird unterschieden zwischen:
  - Legislative Instanz: Sie ist zuständig, dass für den Benutzer die Voraussetzung geschaffen resp. entzogen wird, den entsprechenden Service zu nutzen.
    Die legislative Instanz ist zuständig, die vertrauenswürdigen Identity-Provider zu verwalten.
  - Exekutive Instanz: Hier wird einem Benutzer gemäss den Definitionen der legislativen Instanz Zugang zum Service gewährt oder verwehrt.

Der Kern des Konzepts basiert auf der Verwaltung der Identität. Dabei wird eine elektronisch bearbeitbare Identität generiert. Es ist unerheblich, ob es sich um eine digitale Signatur, eine Username Passwort Kombination oder irgendeine dem Stand der Technik entsprechende Identität handelt. Wichtig ist, dass diese Identität an einem wohl definierten Ort generiert, mit einem SLA versehen verwaltet und gegebenenfalls in einem Identitätsverzeichnis publiziert wird. Diese elektronische Identität wird einer physischen Person zugewiesen und erhält ihre Gültigkeit, nachdem sie beglaubigt der entsprechenden Person übergeben worden ist.

Im Rahmen des Rollenmanagements erfolgt eine Abbildung von realen Personen oder Funktionen einer Organisationseinheit zu einer digitalen Identität. Bei dieser Zuordnung hat die entsprechende Organisationseinheit weitgehende Selbständigkeit. Wird diese Zuordnung gegenüber anderen Organisationseinheiten oder Fachapplikationen verwendet, dann regeln ein entsprechendes SLA und NDA[3] die Verwendung und Haftung.

Bei der Verwendung der Identität ist wichtig, dass auf eine Gewaltentrennung zu achten ist. Diese Gewaltentrennung ist wie folgt zu verstehen:

[3] NDA: Non Disclosure Agreement (Stillschweigeabkommen)

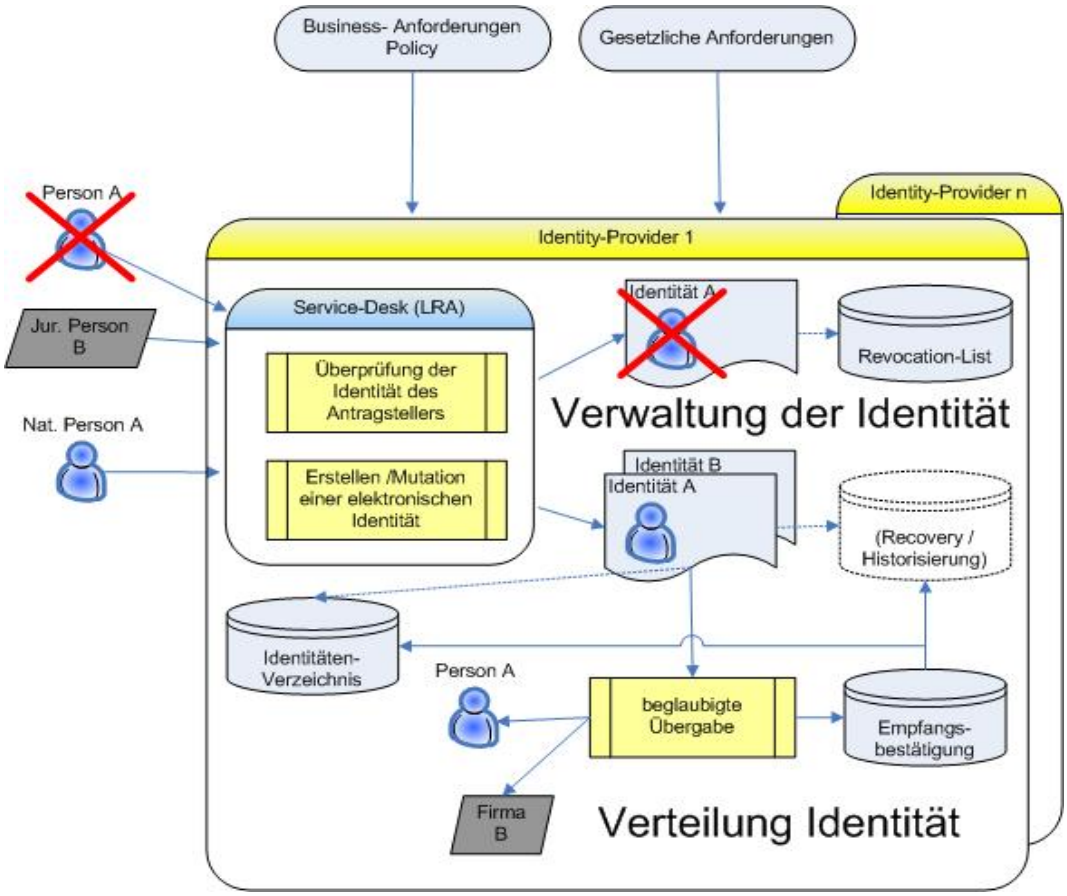
Es wird unterschieden zwischen der Stelle, welche festlegt, wer zugreifen darf (Policy Decision Point) und der Stelle, welche den Zugriff schaltet (Policy Enforcement) und der Stelle, welche die Authentisierung der Person (Authentication Provider) durchführt. Es ist empfehlenswert, diese Stellen organisatorisch zu trennen.

Auf diese Weise werden bestehende Applikationen (Legacy Systeme) oder handelsübliche Applikationen integral eingebunden.

7.2 Verwaltung der Identität

Die Verwaltung von Identitäten stellt eine besondere Herausforderung dar. Während es im Alltag klar ist, Identitäten als Personen zu verstehen und anhand von persönlichen Merkmalen wie Gesichtsform oder Sprache eindeutig zu identifizieren, oder anhand eines Personalausweises mit Foto, entstehen bei computergestützten Abläufen in diesem Bereich höhere Anforderungen.

So ist die Einführung von biometrischen Verfahren in Computersystemen ein aufwendiges Unterfangen und aus diesem Grund wenig verbreitet.



Daher werden Personen in Computersystemen indirekt über Geheimnise authentisiert. Solche Geheimnisse können sein:

- Wissen eines Passwortes, Passphrase oder erweiterte Verfahren
- Besitzen eines Tokens mit erweiterten Verfahren wie Einmal-Passwort oder digitalem Schlüssel.

Auf jeden Fall aber müssen diese Geheimnisse von einer vertrauenswürdigen Stelle bestimmt, vergeben und gewahrt werden. Dies ist eine Aufgabe des Authentisierungsservices. Er entspricht weitgehend dem Dienst eines heute bekannten Passbüros.

Da es unterschiedliche Verfahren der Identitätsprüfung gibt, welche allesamt am Markt stark verbreitet sind und deren Kosten, Nutzen und Risiken anders zu bewerten sind, wird es in nächster Zeit schwer möglich sein, ein einziges Verfahren zur Authentisierung durchzusetzen und ist auch nicht immer zweckmässig.

Aus diesem Grund definiert der Service-Eigentümer eine Risikoklasse für seine Applikation. Aus der Risikoklasse wird durch den Authentisierungsservice eine adäquate Authentisierungsmethode abgeleitet.

7.2.1 Massnahmen

Der Einsatz von digitalen Schlüsseln, zusammen mit einer Public Key Infrastruktur ist ein effektiver Weg, um eine Authentisierung mit hoher Güte effektiv zu realisieren. Aus diesem Grund wird auf diese Technologie vertieft eingegangen.

7.2.1.1 Zuständigkeiten

Ein IAM-System steht und fällt mit der Qualität der vom System erzeugten Identitäten. Das Erzeugen einer virtuellen Identität und der anschliessenden Zuordnung zur physischen Identität stellt einen kritischen Erfolgsfaktor dar.

Unser Referenzmodell setzt voraus, dass **eine oder mehrere zentrale Stellen für diese Aufgabe** zuständig sind. Damit kann erreicht werden, dass überall

- die gleichen Standards gelten
- nach den gleichen Standards gearbeitet wird
- die virtuellen Identitäten klar definierten Qualitätsstandards entsprechen und dementsprechend eingesetzt werden können.

Schliesslich ist mit jeder Identität eine Haftung verbunden. Zentralisation soll hier nicht geographisch verstanden werden. Es macht im Gegenteil Sinn, dass einzelne Komponenten, insbesondere das v*irtuelle Passbüro* so nahe wie möglich beim Antragsteller sind, also dort, wo man ihn sowieso schon kennt, z.B. Gemeinde, Post, Arbeitgeber. Die Zentralisation soll die organisatorischen Aspekte abdecken.

7.2.1.2 Pflichtenheft

Das *virtuelle Passbüro* – im weiteren *Identity-Provider* genannt – muss sich in einem komplexen Umfeld behaupten, so z.B.:

- Gesetzliche Anforderungen müssen eingehalten werden
- Betriebliche Anforderungen müssen erfüllt werden
- Im internationalen Umfeld muss sich die Lösung bewähren.

Aus diesen Gründen müssen klare Vorgaben definiert werden für

- Anforderungen an den Identity-Provider wie Aufbau, Infrastruktur, physische und logische Sicherheit und Kontrollen
- Anforderungen an die Unternehmen, Verwaltungen und ihre Mitarbeitenden, insbesondere Aufgaben, Verantwortung, Kompetenzen.
- Anforderungen an Prozesse z.B. Antragswesen, Feststellen der physischen Identität, Erstellen und Übergabe der virtuellen Identität.
- Handhabung für Spezialfälle.

Es drängt sich ein Vergleich auf mit einer **P**ublic **K**ey **I**nfrastruktur (PKI). Dort werden in verschiedenen Dokumenten die Arbeitsprinzipien beschrieben. Kernpunkte sind der Registrierungsprozess, Handhabung der vertraulichen Daten und Informationen, zentrale oder dezentrale Schlüsselerzeugung, technischer Schutz der PKI-Systeme sowie rechtliche Zusicherungen. Meistens werden diese Angaben in folgenden Dokumenten festgehalten:

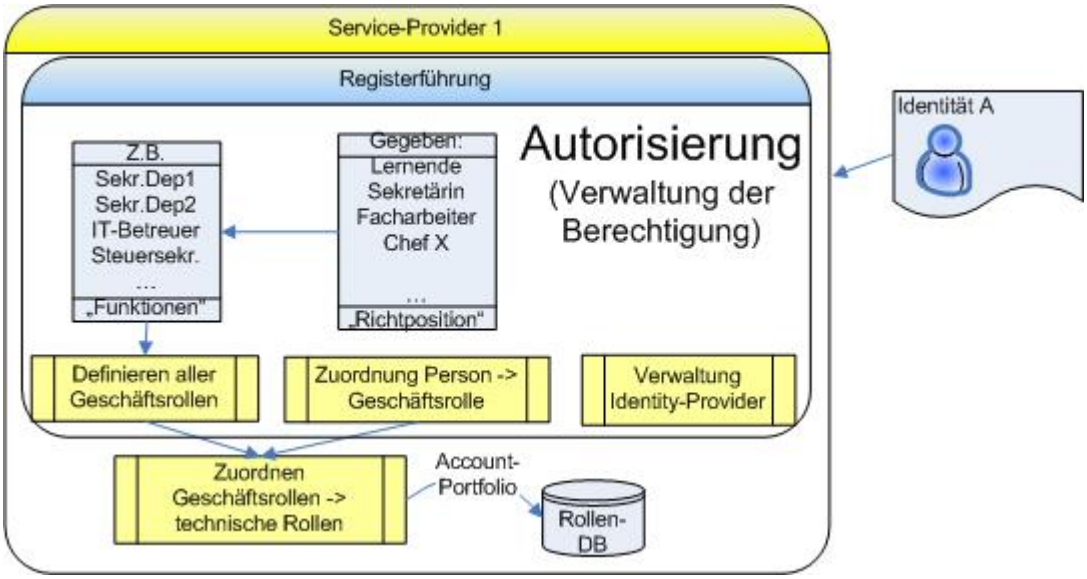
- CP (Certificate Policy): In diesem Dokument beschreibt die PKI ihr Anforderungsprofil an ihre eigene Arbeitsweise. Es dient Dritten zur Analyse der Vertrauenswürdigkeit und damit zur Aufnahme der Zertifikate.
- CPS (Certificate Practice Statement): Hier wird die konkrete Umsetzung der Anforderungen aus der CP in die PKI beschrieben.

7.2.2 Verwaltung der Identität beim Identity-Provider

Der Identity-Provider erfasst Identitäten und führt ein Register. Im Register ist klar ersichtlich, welche Identität mit welchen Verfahren registriert und authentisiert werden kann.

Der Identity-Provider stellt dabei selber solche elektronische Identitätsausweise aus oder beauftragt einen Dritten dafür.

7.3 Verwaltung der Identität beim Service-Provider (Legislative)



7.3.1 Definition der benötigten Geschäftsrollen

Hier werden sämtliche Rollen, die in einer Organisation eingesetzt werden, verwaltet.

7.3.2 Zuordnung von Person zu Geschäftsrollen

In Abhängigkeit von Funktion und Position, werden der Person eine oder mehrere Rollen zugeordnet.

7.3.3 Verwaltung der Identität beim Service Eigentümer

Der Service-Eigentümer definiert, welche Zugriffsrechte für welche Anwender gültig sind und die Güte der Authentisierung.

Für die Wahl der Güte hat sich heutzutage die folgende Kategorisierung bewährt:

- Keine Authentisierung
- Einfache Authentisierung (z.B. UID, PW)
- Industrie Standard Authentisierung (z.B. Domänen-Login)
- Behörden Authentisierung (z.B. PKI)
- Besondere Authentisierung gemäss Risikoanalyse

Es ist davon auszugehen, dass eine Verfeinerung dieser Abstufung sinnvoll sein könnte.

7.3.4 Zuordnung von Geschäftsrollen zu technischen Rollen

In Abhängigkeit zu den anzubietenden Services müssen die technischen Rollen mit den entsprechenden Berechtigungen in einem ersten Schritt definiert und in einem zweiten Schritt den Geschäftsrollen zugeordnet werden. Diese Definitionen werden anschliessend in einer entsprechenden Datenbank abgelegt.

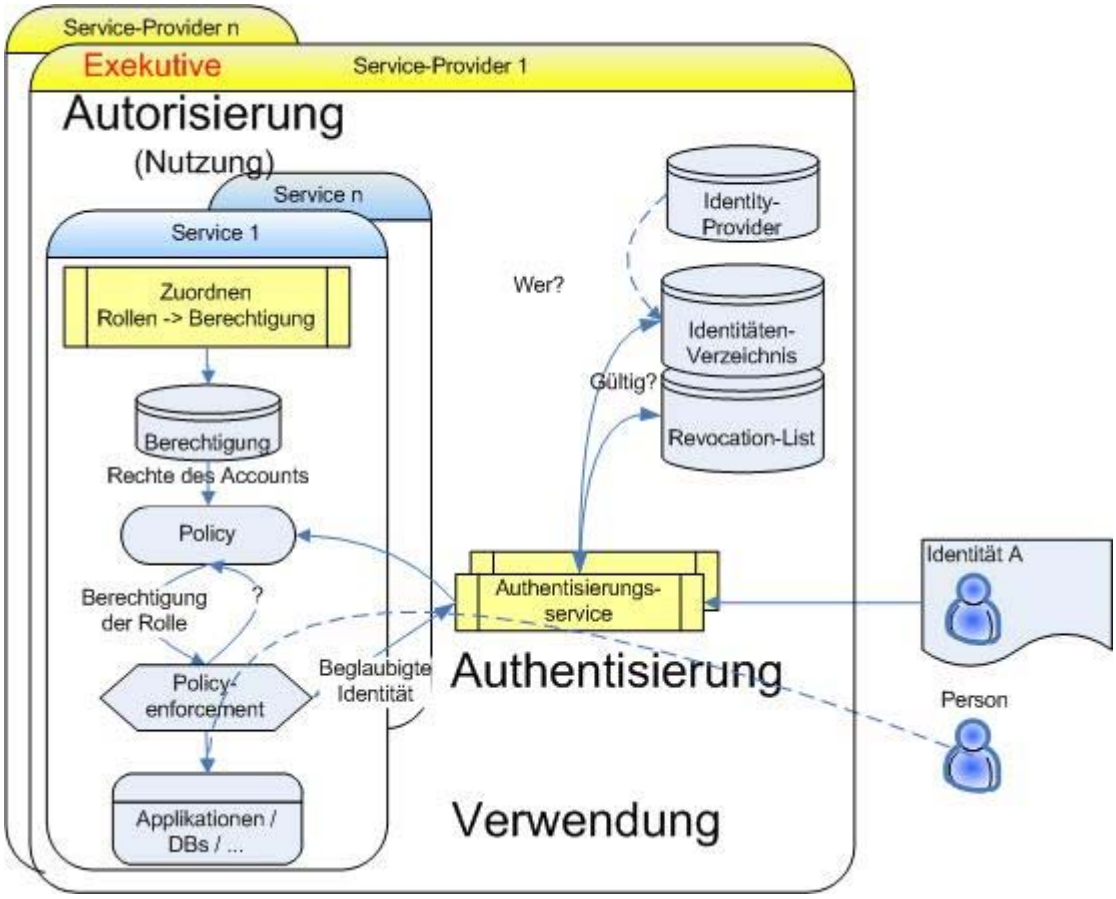
7.3.5 Verwaltung der Identity-Provider

Diese Verwaltung beinhaltet die folgenden Aktivitäten:

- Definition der Mindestvoraussetzungen für einen Identity-Provider.

- Prüfung eines potentiellen Identity-Providers und erstellen entsprechender SLA, wenn Mindestvoraussetzungen erfüllt sind.
- Initialisierung der Integration ins System.

7.4 Verwaltung der Identität beim Service-Provider (Exekutive)



Der Service-Provider hat sicherzustellen, dass die Qualität der Authentisierung mindestens der vom Service-Eigentümer geforderten Güte entspricht. Der Service-Provider verfügt über eine entsprechende Schnittstelle zum für ihn relevanten Teil des Registers des Authentisierungsdienstes.

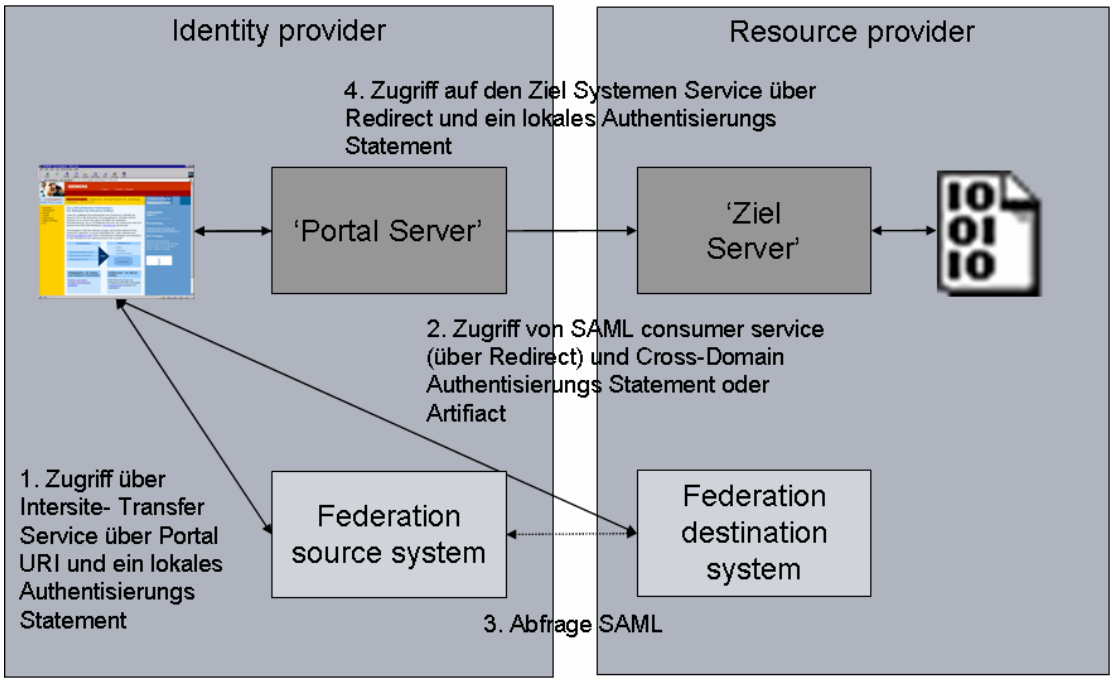
8. IAM + andere Standards

eCH hat bereits mehrere Standards verabschiedet. Nachfolgend werden relevante eCH Standards aufgezeigt und ihre Relation zum hier definierten IAM Standard.

8.1 Federation - Liberty Alliance

Federation ist eine Form der Organisation, bei der mehrere Teilnehmer, die über eine gewisse Eigenständigkeit verfügen über die Unternehmensgrenzen hinweg zusammengeschlossen werden[4].

Liberty Alliance, ein typisches Beispiel einer Federation von Identitäten, ist ein Zusammenschluss von namhaften Industrie Firmen mit dem Ziel einen Standard zu definieren, bei welchem unterschiedliche Organisationen miteinander auf eine kostenwirksame und sichere Art Daten austauschen können.



Dabei wird zwischen den beiden Partnern eine Verbindung mit einem limitierten Vertrauensverhältnis aufgebaut. Es wird zwischen einem Identity-Provider und einem Service-Provider (Ressourcen-Provider) unterschieden.

Der Ressourcen-Provider anerkennt dabei die Authentisierung des Identity-Providers und gewährt entsprechenden Zugriff auf die definierte Infrastruktur.

Dieses Modell ist weitgehend im Einklang mit dem von uns definierten Modell.

Es existieren grundsätzlich zwei Arten der Identity Federation: Browser basierend und Dokument basierend, die im Folgenden kurz skizziert werden.

[4] http://www.iam-wiki.org/Federation

8.1.1 Browser basierend

Voraussetzung:

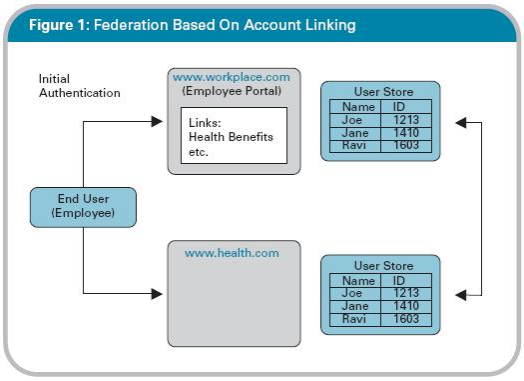
- Die Mitarbeiter von „workplace.com“ sind bei ihrem Arbeitgeber eingeloggt

Vorgehen:

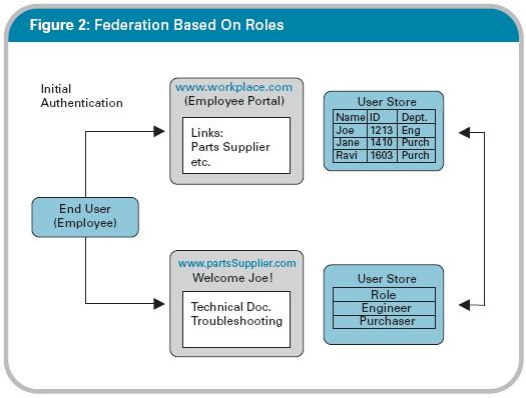
- Der Mitarbeiter findet auf dem Mitarbeiterportal von „workplace.com“ einen Link auf die Seite des entsprechenden Service-Providers und bekommt durch anklicken auf diesen Link „seinen“ Zugriff auf die für ihn vorgesehenen Services

Technik:

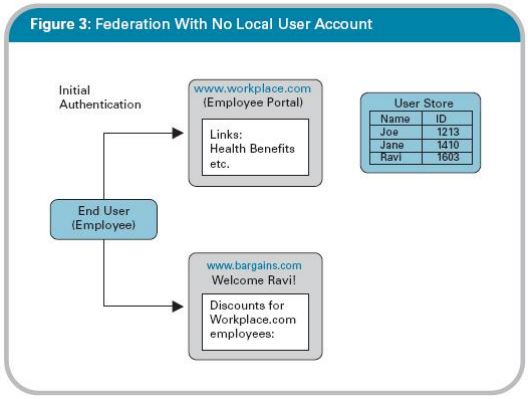
- **Szenario 1: Account Linking**
  Bei diesem Szenario werden zwei oder mehrere Services miteinander verbunden. Nach dem erstmaligen Einloggen beim Service-Provider wird eine eindeutige Identität erstellt (zufällig erstellte Nummer), wenn sich der Benutzer einverstanden erklärt, seine Accounts zu "federieren". Voraussetzung ist, dass beide Accounts bereits existieren. Greift ein Mitarbeiter von „workplace.com“ auf die Seite von „health.com“ zu, wird auf sichere Art die eindeutige Identität übertragen. Dies erlaubt dem Service-Provider, die Authentisierung des Benutzers sicher zu stellen und die Services entsprechend anzubieten.



- **Szenario 2: Role based**
  Anstatt dass der Service-Provider Accounts seiner Kunden pflegt, definiert er einige Rollen, so z.B. die Rollen „engineer“ und „purchaser“. Der Kunde überträgt beim Zugriff auf die Webseite des Service-Providers auch seine Rolle, welche anschliessend authentisiert wird.



- **Szenario 3: Authentication only**
  Vom Service-Provider werden weder Identitäten noch Rollen gepflegt, er erlaubt lediglich allen Mitarbeitern der Firma „workplace.com“ die Nutzung seiner Dienste. Er benötigt lediglich eine Bestätigung der Authentisierung vom Identity-Provider, welche automatisch im Hintergrund auf sichere Weise übertragen wird. Zusätzliche Attribute dienen nur zum Personalisieren des Benutzer-Interfaces.



8.1.2 Dokument basierend

Identity federation wird nicht nur für personenorientierte Authentisierungen und "single sign on" (SSO) eingesetzt, sondern auch für andere automatische Authentisierungen, die z.B. auf Web-Services basiert sind. Der technische Ablauf ist unter der Beschreibung von "Dokument basierte" federation zu finden (Liberty Alliance Standard). Der Fokus des Referenzmodells IAM ist mehrheitlich auf natürliche und juristische Personen ausgelegt.

8.2 eCH

Im Rahmen der Registrierung, im Besonderen der Verwaltung von Identitäten, ist eine Anlehnung an diese Vorgaben zu achten (Stand Oktober 2006).

- XML Standards
- eForms -> Registrierung
- eHealth -> Patientenidentifikation
- Meldewesen -> Handhabung der Umzüge
- AHV/IV
- Datenstandard Ausländerkategorien
- Datenstandard Gemeinden -> GemeindeID
- Datenstandard Staaten -> StaatsID
- Meldegründe

Harmonisierung eCH Standards nötig

Die Verwendung von Identitäten und Standard Applikationen schränkt die Freiheit bei der Verwendung der entsprechenden Daten ein. Daher sollten die folgenden Standards genauer auf eine Verträglichkeit untersucht werden:

- Records Management
- PKI-Zertifikatsklassen
- Digitale Verträge
- Digitale Signaturen
- PKI -> Digitales Zertifikat

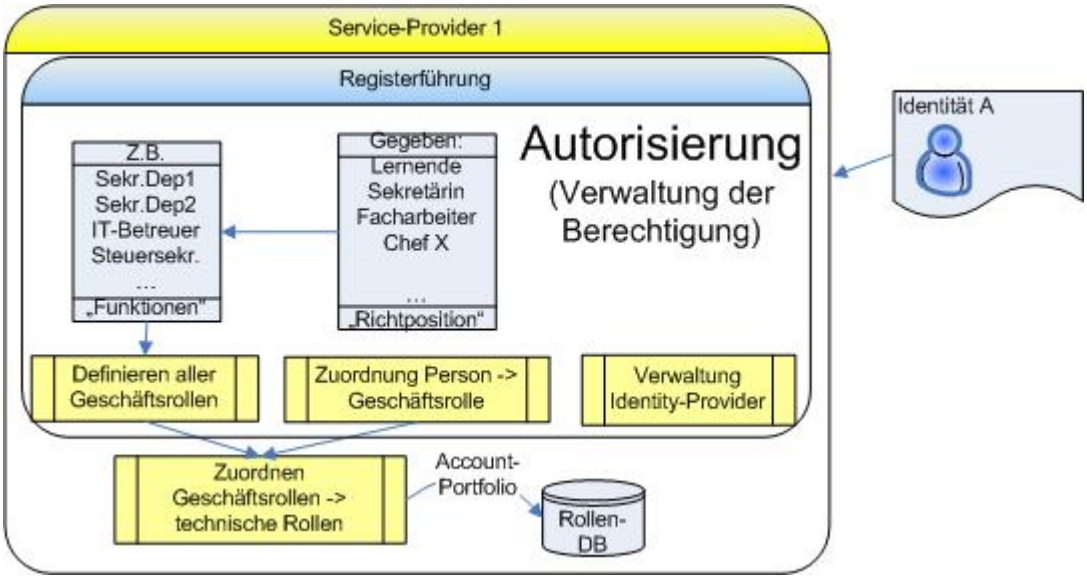
9. Policies

Kontext basierte Zugriffsrechte respektiv Rollen, werden in der nächsten Version des Referenzmodells behandelt.

10. Rollen

Im Rahmen des Rollenmanagements wird der folgende Ansatz verfolgt:

Sowohl die Organisationseinheiten als auch die Fachapplikationen verfügen in der Regel über ein Rollenmanagement. Die Herausforderung besteht darin, die Rollen der Organisationseinheiten mit dem Rollenmodell der Fachapplikationen abzugleichen. Zudem wechseln die Benutzer in den Organisationseinheiten laufend ihre Rollen (Beförderungen, Stellvertretungen, neue Aufgabengebiete, andere Pflichten, …).



Ein Lösungsansatz besteht darin, eine Transformation zwischen dem Rollenmodell der Unternehmung und den jeweiligen Fachapplikationen zu definieren. Diese Transformation ist für jede Organisationseinheit individuell. Die entsprechende Fachapplikation definiert dabei das Rollenmodell und die Organisationseinheit erstellt die entsprechende Transformation. Für Einzelheiten verweisen wir auf den NIST Standard RBAC.

10.1 Rahmenbedingungen

Für den geordneten Betrieb sind gewisse Rahmenbedingungen einzuhalten. Die Grundlage für diese Rahmenbedingungen bilden die jeweiligen Anforderungen des Betriebs und dessen Betriebsprozesse. So sind grundsätzlich die folgenden Regelungen festzulegen:

- **Service Level Agreement** zur Regelung der gegenseitigen Obliegenheiten beider Seiten bei der Zuweisung und Verwendung der entsprechenden Rollenmodelle.
- **Geheimhaltungsvereinbarung**, in welcher geregelt wird, wie in Falle von Verstössen gegen die Vertraulichkeit und Geheimhaltung verfahren wird.

10.1.1 Sicherheitskonzept

Im Sicherheitskonzept wird geregelt, welche Sensitivität, Integrität und Verfügbarkeit im Prozess bearbeitet und mit welchen Massnahmen diese Eigenschaften geschützt werden. Dabei ist darauf zu achten, dass die Massnahmen verhältnismässig sind.

10.1.2 Betriebliche Anforderungen (z.B. Stellvertretung)

Betriebliche Anforderungen bestehen oft in den jeweiligen Organisationen. Besondere betriebliche Anforderungen stellen das IAM erfahrungsgemäss vor Herausforderungen:

- **Stellvertretung**
- **Schichtbetrieb**
- **Prozesse, welche verbindliche Aktionen auslösen**
- **Pseudonyme**
- **Anonymität**

Diese Formen erfordern eine genaue Erörterung und fallweise Integration in das IAM System.

10.1.3 Geschäftsprozess

Der zugrunde liegende Geschäftsprozess sollte durch das IAM System so wenig wie möglich verändert werden.

Es ist zu beachten, dass der Geschäftsprozess von einem Prozess Eigentümer gesteuert und verwaltet wird. Oft sind in diesem Prozess mehrere Fachapplikationen einbezogen, so dass auch die Identitätsverwaltung eine erhebliche Rolle spielt.

10.2 Warum braucht es Rollen?

10.2.1 Entkopplung von Rollen, Funktionen und Personen

Das Ziel für ein Identitätsmanagement ist, die Entkoppelung der Einzelpersonen von Funktionen und Rollen in den Fachapplikationen und Prozessmodellen. So kann der Verwaltungsaufwand deutlich reduziert werden und der Missbrauch durch nicht aktuelle Berechtigungen weitgehend vermieden werden.

10.2.2 Rollenzuordnung

Jeder ID kann mindestens eine Rolle zugeordnet werden. Es ist darauf zu achten, dass – wo es die Applikation erlaubt – grundsätzlich nur mit Rollen gearbeitet wird und nicht mit Einzelpersonenrechten.

10.2.3 Eine Rolle ist Voraussetzung für eine Berechtigung

Es ist darauf zu achten, dass alle Berechtigungen an eine Rolle vergeben werden. Dadurch kann die Pflege der Berechtigungen modellhaft für alle Rollen unabhängig von den individuellen Berechtigungen stattfinden und eine weitgehende Loslösung von Sachzwängen erreicht werden.

10.2.4 Garantie, dass Identitäten nur innerhalb dem Bereich der Rollen operieren können

Da die Berechtigungen einer Rolle am Prozess orientiert sind, kann erreicht werden, dass die Einzelperson auch die notwendigen Rechte zur Ausübung der Aufgabe des jeweiligen Geschäftsprozesses besitzt.

11. Verwendung

11.1 Ziel / Nutzen

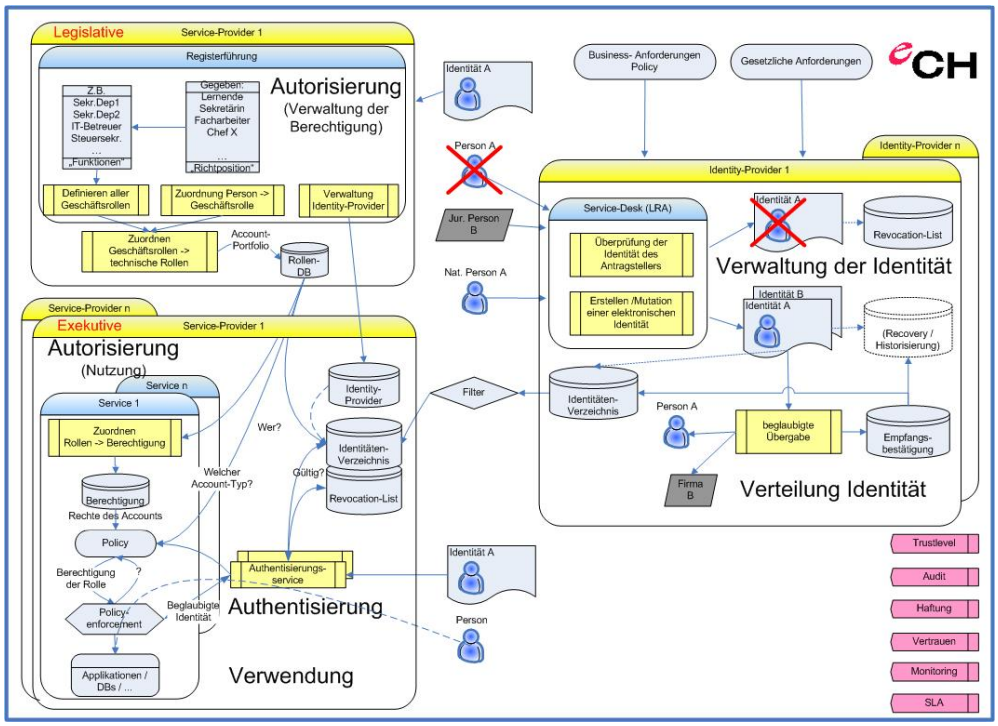
Das Ziel des Referenzmodells ist eine einheitliche Handhabung von bestehenden und zukünftigen elektronisch abzuwickelnden Geschäftsprozessen. Dabei müssen die technischen Plattformen konform zu geltenden Gesetzen, Verträgen und Übereinkommen sein.

Dabei wird der Grundsatz eines skalierbaren, universellen Sicherheitsmodells verfolgt. Dies bedeutet, dass die Risikoanalyse eines Services definiert, wie hoch die Sicherheitsmassnahmen sein müssen. Durch eine Gewaltentrennung zwischen Service, Zugriffsentscheid und Zugriffsteuerung kann eine optimale Entkoppelung von Sachzwängen und somit eine flexible Integration in unterschiedliche Zielumgebungen erreicht werden.

Durch IAM wird der Service zusätzlich geschützt. Dies ermöglicht eine globale Verwendung von Legacy-Systemen.

11.2 Übersicht

Die nachfolgende Grafik zeichnet die Grundkomponenten des Referenzmodells auf.



Das Referenzmodell stellt dar, wie eine handelsübliche Applikation in eine konforme Systemlandschaft eingebettet werden kann und wie die behördenspezifischen Anforderungen entweder mit zusätzlichen Schnittstellen, Komponenten oder Vereinbarungen erfüllt werden können.

Im Zentrum steht die handelsübliche Applikation, welche isoliert für einen Geschäftsfall eingesetzt wird. In der Regel haben diese Applikationen schon bestehende recht- und rollenbasierende Zugriffsschutzmechanismen, welche einer in der Applikation definierten Rolle entsprechen und mit lokal in der Applikation definierten Rechten funktionieren.

Das Grundsätzliche an diesem Modell ist, dass die Zugriffsrechte für eine Identität mit einem als gesondert zu betrachtenden Authentisierungsservice gekoppelt werden. Die Policy, welche die Ap-

plikation umsetzt, fällt den Entscheid, ob ein Zugriff für eine bestimmte Identität durchgeführt werden darf. Die eigentliche Rechtesteuerung erfolgt durch einen Policy Enforcement Point. Damit wird eine einfache Gewaltentrennung erreicht.

Eine Policy Engine bezieht ihre Informationen aus dem für die Applikation lokal enthaltenem Rechtesystem und dem Rollenmodell, welches vom Service-Verantwortlichen definiert wurde. Die Identität des Anwenders wird vom Authentisierungsservice ermittelt und beglaubigt.

Der Authentisierungsservice ist eine abgekoppelte Einheit, welche zum einen mit dem Service-Verantwortlichen und zum anderen mit den unterschiedlichen Registrierungsstellen ein SLA abschliesst.

Die Registrierungsstellen publizieren ihre Register in einem Identitätsverzeichnis zuhanden der Authentisierungsstellen. Zum Identitätsverzeichnis wird auch der Status dieser Identität mit publiziert. Dieser kann entweder in einer Statusinformation im Register oder mit gesonderten Sperrlisten (Revocation List) erfolgen.

11.3 Prinzipien (Massnahmen)

11.3.1 Gewaltentrennung

Der Entwickler der Applikation, der Betreiber der Applikation und der Owner des Business Prozesses sind getrennt zu betrachten. So ist darauf zu achten, dass die Authentisierung, der Entscheid des Zugriffs und die Schaltung des Zugriffs getrennte Instanzen durchführen.

11.3.2 Authentisierungsservice

Der Authentisierungsdienst hat die Aufgabe, die Identität festzustellen. Je nach Anwendung muss dabei der Benutzer bekannt sein oder er kann auch anonym bleiben.

Der Authentisierungsdienst kann eine vollständig selbstständige Dienstleistung sein, welche gemäss einem SLA Identitäten ermittelt.

11.3.3 Rollen basierte Rechte

Es ist darauf zu achten, dass – wo es die Applikation erlaubt – keine Rechte direkt an reale Personen vergeben werden, sondern nur an Rollen.

11.3.4 Referenzieren des Identitätsverzeichnis

Jede Identität, auch ein Pseudonym oder eine Anonymität hat irgendwo einen Eintrag in einem Verzeichnis, welcher Auskunft darüber gibt, ob die Identität existiert und gültig ist. Das Verzeichnis muss nicht öffentlich zugänglich sein.

11.3.5 Policy Management

Im Policy Management werden die Zugriffsregeln vom Eigentümer des Geschäftsprozesses definiert.

11.3.6 Policy Decision Point

Im Policy Decision Point werden die Regeln auf die jeweiligen Systeme umgesetzt.

11.3.7 Policy Enforcement Point

Im Policy Enforment Point werden die Zugriffe gemäss Policy auf die jeweilige Applikation durchgesetzt.

11.4 Applikation

Eine Applikation unterstützt in der Regel einen Geschäfts-Prozess. Meistens basieren Geschäfts-Prozesse auf mehreren Applikationen. Um die Aufwände der IT in den Griff zu bekommen, wird vermehrt auf Standard Applikationen gesetzt.

11.4.1 Standard Applikation (Handelsware)

Standard Applikationen haben den Vorteil, dass sie einen grossen Funktionsumfang zu einem wirtschaftlichen Preis bieten. Allerdings ist eine kundenspezifische Anpassung in der Regel aufwendig oder gar nicht möglich. So kann insbesondere das in der Applikation eingebaute Rollenmodell selten direkt in das konkrete betriebliche Umfeld integriert werden. Aus diesem Grund ist eine Zwischenschicht notwendig, welche diese Transformation durchführt.

11.4.2 Vorgelagerter Access-Control

Zusätzliche Schnittstellen der vorgelagerten Komponenten zur spezifischen Rechteprüfung und Steuerung können eingesetzt werden, um die Mängel der Standardsoftware zu kompensieren.

Die zusätzlichen Funktionen für die Gewaltentrennung können entweder durch zusätzliche Software- oder Hardwarekomponenten oder Systeme realisiert werden.

11.5 Rollenverzeichnis

Die Fachapplikation verfügt über ein eigenes Rollenmodell. Da dieses Rollenmodell in der Regel nicht dem Rollenmodell der Organisationseinheiten entspricht, muss es von Eigentümer des Prozesses entsprechend transformiert werden.

11.6 Identitätsverzeichnis

Das Identitätsverzeichnis bildet die Grundlage für den Authentisierungsdienst, um festzustellen, ob eine Identität gültig ist. Das Identitätsverzeichnis wird im Rahmen der Verwaltung der Identität gepflegt und gefiltert publiziert, so dass Authentisierungsdienste dieses nutzen können.

11.6.1 Liste von referenziellen Identitäten

Es kann eine Liste von referenziellen, maschinenlesbaren Identitäten enthalten. Hinzu kommt dann der Status dieser Identitäten.

Es gibt aber auch andere Systeme, bei denen diese Liste nicht besteht.

11.6.2 Liste von ungültigen referenziellen Identitäten

Gut verbreitet ist die sogenannte Sperrliste (revocation list in einer PKI-Umgebung). Darin werden die Identitäten geführt, welche nicht gültig sind. Dieses Verfahren wird dann eingesetzt, wenn die Listen mit den referenziellen Identitäten und deren Status nicht besteht.

11.7 Authentisierungs-Service

Der Authentisierungsdienst überprüft die Identität. Jeder Authentisierungsdienst hat eine gewisse Güte, mit welcher die Identität erkannt werden kann. Es ist Sache des Sicherheitskonzeptes, die Anforderungen an die Authentizität der Identität festzulegen. Grundsätzlich bestehen die folgenden Stufungen der Authentizität:

- Identifikation durch Wissen wie Passwort, PIN.
- Identifikation durch Besitz wie Token, Streichliste.
- Identifikation durch persönliche Merkmale (Biometrie).

Der Authentisierungsdienst authentisiert die Identität, indem die technische Identifizierung durchgeführt wird und anschliessend die Gültigkeit entweder anhand eines Verzeichnisses mit Statusinformationen oder anhand einer Sperrliste geprüft wird.

Der Authentisierungsdienst kann auch extern durchgeführt werden. Ein Beispiel eines solchen Systems wird bei *Federated Identity* beschrieben. In diesem Fall authentisieren die Partner ihre eigenen Benutzer und übermitteln diese Informationen jeweils an die externen Partner. Es besteht ein limitiertes Vertrauensverhältnis zwischen diesen Partnern, welches über ein SLA und NDA geregelt wird.

11.8 Policy

Die Policy definiert, welche Rollen unter welchen Umständen auf die Ressourcen zugreifen dürfen. Dazu können unter anderem folgende Parameter benutzt werden:

- Zeitpunkt
- Gültigkeit
- Kontext
- Güte der Authentisierung
- Standort

11.9 Policy Decision

Die Entscheidung über den Zugriff erfolgt an einem Entscheidungspunkt, dem Policy Decision Point. Dieser signalisiert dem Policy Enforcement Point, ob ein Zugriff erlaubt werden darf.

11.10 Policy Enforcement

Durchsetzung der Policy basierend auf den Faktoren Standort, Güte der Authentisierung, Kontext, Gültigkeit und Zeitpunkt.

12. Weitere Aspekte

Die folgenden Aspekte sind in allen Bereichen des IAM mit unterschiedlicher Intensität vorhanden. Sie tragen entscheidend zur erfolgreichen Akzeptanz des IAM bei.

12.1 Vertrauen

Die breite Akzeptanz und der Gebrauch von IAM hängen von dem Vertrauen der Identitätsträger und -nutzer ab. Das Vertrauen ist eine grundlegende Voraussetzung, um Transaktionen (elektronische oder sonstige) anzuerkennen und nachzuvollziehen und beinhalten das Grundprinzip des gegenseitigen Vertrauens. Nachprüfbarkeit und Transparenz fördern wiederkehrende Transaktionen mit gleichen Entitäten.

12.2 Monitoring

Erlaubt ein Nachvollziehen in *real-time* aller Prozesse und Attribute, bei denen eine Identität benutzt wird. Damit wird Transparenz und die Reaktionsfähigkeit erhöht, um Handelsspielraum (z.B. Zeit) zu gewinnen und proaktiv zu agieren.

12.3 Audit

Kontrolle durch eine Drittpartei führt eine Dimension der Unabhängigkeit ein. Sie dient zur Nachvollziehbarkeit, Einhaltung einer Konformität (Standards & Normen) und einer Vorbeugung gegen Missbrauch.

12.4 Haftung

Jegliche Art von Geschäftstätigkeit basiert auf dem Eingehen von Verpflichtungen, welche entweder in Form von schriftlichen oder mündlichen Verträgen oder SLA abgeschlossen werden. Wird einer solchen Verpflichtung nicht nachgekommen, haftet die den Vertrag nicht eingehaltene Partei.

12.5 Trustlevels

Trustlevels dienen der Einstufung einer Identität nach erfolgter Authentisierung in eine Vertrauens-Kategorie. Die Trustlevels werden durch eine verbindliche Politik (*policy*) definiert. Somit lässt sich ein System mit rollenbasierten Zugriffsrechten aufbauen, die den nicht-technischen Anforderungen (*business needs*) gerecht werden können. Der Feinheitsgrad der Levels wird vorgegeben (*business constraint*). Dies gilt ebenfalls für die *policies*: es kann eine einzige Politik für alle Dienstleistungen existieren oder es kann für jede Dienstleistung eine oder n-*policies* geben.

Die Politik beinhaltet die *business rules*, die von einer Dienstleistung oder von einer Menge von Dienstleistungen berücksichtigt werden müssen.

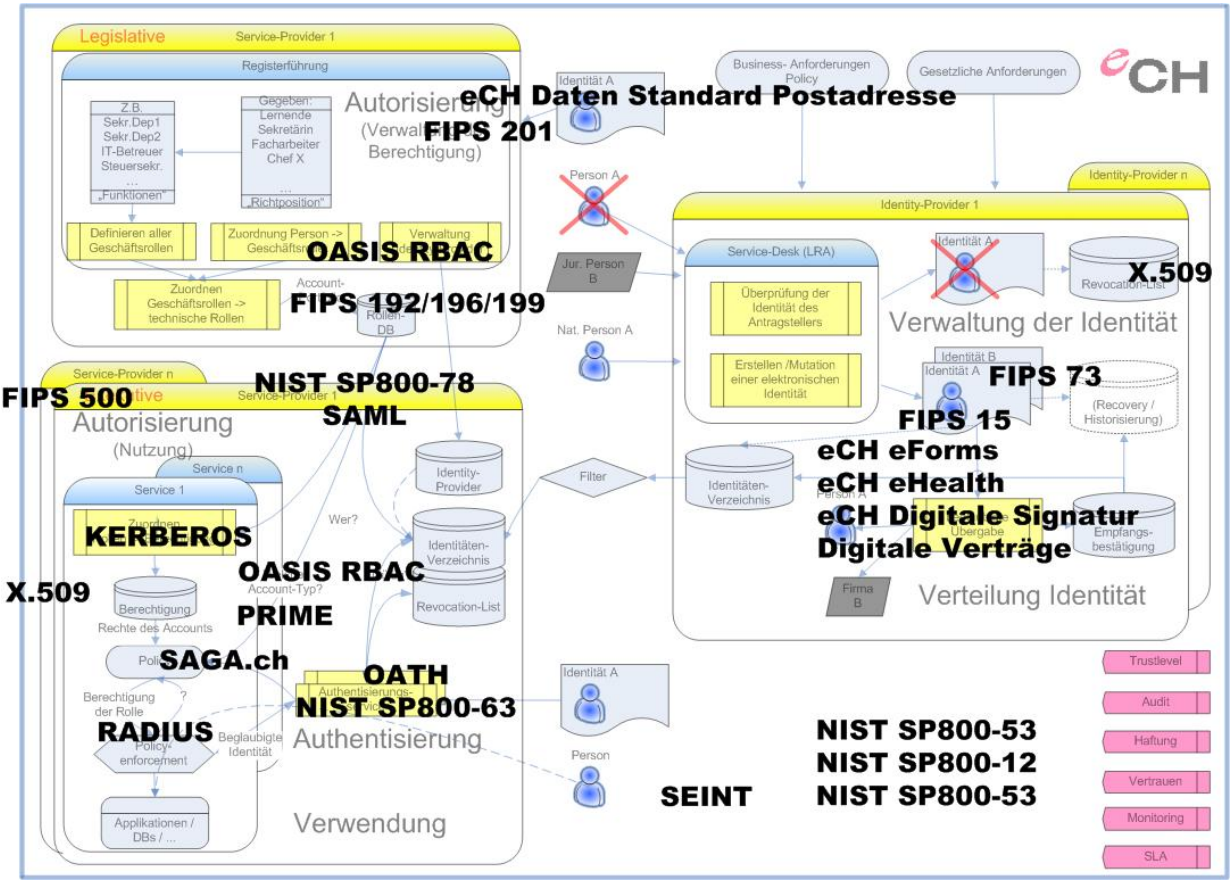
Um einen guten Austausch (intern oder extern) zwischen Systemen zu garantieren, müssen die Trustlevels ebenfalls standardisiert werden.

12.6 SLA

Der Begriff Service Level Agreement (SLA) oder Dienstleistungs-Vereinbarung bezeichnet eine Vereinbarung zwischen Auftraggeber und Dienstleister, die wiederkehrende Dienstleistungen für den Auftraggeber in den Kontrollmöglichkeiten transparenter gestaltet durch genaue Beschreibung zugesicherter Leistungseigenschaften wie etwa Reaktionszeit, Umfang und Schnelligkeit. Wichtiger Bestandteil ist hierbei die Qualität.

13. Positionierung existierender Standards

Die nachfolgende Grafik zeigt schemenhaft auf, welche internationalen Standards in welchen Bereichen des Modells wirksam sind.



Grundsätzlich kann festgestellt werden, dass die meisten Standards sehr technisch und konkret gewisse Teilbereiche des Modells beschreiben. Wenige Standards beschreiben aber das Thema des Identitiy und Access Managements umfassend.

Besonders hervorheben kann man die USA Standards von NIST, FIPS, welche in einem Standard Werk einen grossen Teil abzudecken vermögen.

14. Glossary

Da Englisch die Fachsprache in der Informatik ist, dienen als Basis für dieses Glossary die englischen Fachausdrücke. Im Alltag wird jedoch in der Schweiz ein Mix aus englischen und Ausdrücken und Begriffen aus der jeweiligen Landessprache verwendet. Da zudem einzelne Begriffe mehrdeutig sind, wird hier versucht, eine einheitliche Basis zu schaffen.

Eine ganz besondere Problematik besteht in diesem Werk, dass es nicht für alle Sprachen eine entsprechende Übersetzung gibt.

Unser Wunsch wäre, dass mit der Zeit ein (online) Nachschlagewerk entsteht, welches neben den englischen Begriffen auch die drei Landessprachen der Schweiz abdeckt. Dabei soll es primär um die Übersetzung der Begriffe gehen, zudem soll in allen Sprachen eine kurze Erklärung verfügbar sein. Die folgende Liste soll als Input dienen für ein solches Werk. Vielleicht entsteht eine neue Fachgruppe eCH?

FRANCAIS	DEUTSCH	ENGLISH	Bedeutung D
architecture à deux niveaux		2-tier architecture	
architecture à trois niveaux		3-tier architecture	Dreischichtige Architektur. Die drei Aufgaben Präsentation, Geschäftslogik und Datenhaltung sind voneinander getrennt.
	Zugriffsberechtigung	access authorization	Regelung, welche Benutzer Zugang zu welchen Daten haben.
possibilité d'accès	Zugriffsmöglichkeit	access capability	
contrôle d'accès	Zugriffskontrolle, Zutrittskontrolle, Zugriffssteuerung	access control	Prozess, welcher sicherstellt, dass nur berechtigte Benutzer Zugriff oder Zugang zu bestimmten IT-Ressourcen haben. Kann auf logischer oder physischer Ebene umgesetzt werden. Setzt sich zusammen aus der Authentifizierung und der Autorisierung.
permission, privilège, droits d'accès	Zugriffsrechte, Privilegien	access right	Regelt, was der berechtigte Benutzer mit den Daten machen darf (lesen, schreiben, modifizieren, löschen)
compte	Konto, Benutzerkonto, Nutzerkonto	account	Zugang zu einem IT-System. Einem Benutzerkonto werden verschiedene Zugriffsrechte oder Privilegien zugeordnet.
ACL, liste de contrôle d'accès	ACL, Zugriffstabelle	ACL, access control list, access control table	Interne Tabelle mit Zugriffsregeln für User und Terminals
authentification	Authentisierung, Authentifizierug	authentication	Vorgang des Nachweises einer Identität, Bestätigung der Identität. Nachdem man behauptet hat, jemand zu sein (z.B. durch Eingabe einer User-ID) muss diese Behauptung überprüft werden. Es stehen folgende Möglichkeiten zur Verfügung: - Wissen (z.B. Passwort, PIN) - Besitz (z.B. Schlüssel, Karte) - körperliches (biometrisches) Merkmal: Fingerabdruck, Iris
autorisation	Genehmigung	authorization	Erteilung von Berechtigungen
		B2A, business to administration	(elektronische) Kommunikationsbeziehungen zwischen Unternehmen und Behörden.
B2B, cybercomerce interentreprise	B2B, business to business	B2B, business to business	steht allgemein für Beziehungen zwischen (min. zwei) Unternehmen.

B2C, cybercommerce de détail	B2C, business to consumer	B2C, business to consumer	(elektronische) Kommunikationsbeziehungen zwischen Unternehmen und Privatpersonen (Konsumenten)
		B2G, business to government	(elektronische) Kommunikationsbeziehungen zwischen Unternehmen und Behörden
commerce électronique consommateur – entreprise	C2B, consumer to business	C2B, consumer to business	elektronische Geschäftsbeziehung zwischen dem Kunden und dem Anbieter einer Ware der Dienstleistung
consommateur à consommateur, transactions inter-consommateurs	C2C, consumer to consumer	C2C, consumer to consumer	elektronische Geschäftsbeziehungen zwischen Privatpersonen
CA, Certification authority AC, autorité de certifiction	CA, Certification Authority, Zertifizierungsstelle	CA, certificate authority	Eine Zertifizierungsstelle ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermaßen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie sie mit ihrer eigenen digitalen Unterschrift versieht.
		certificate policy	RFC 2527
		certification path	RFC 2527
CPS, Certification Practice Statement	CPS, Certification Practice Statement	CPS, Certification Practice Statement	Hier wird die konkrete Umsetzung der Anforderungen in die PKI beschrieben. Dieses Dokument beschreibt die Umsetzung der Certification Policy.
CRL, liste de certificats révoqués	CRL, Zertifikatssperrliste	CRL, Certificate Revocation List	Eine Zertifikatsperrliste ist eine Liste, die Informationen über die Gültigkeit von Zertifikaten enthält. Sie ermöglicht es, festzustellen, ob ein Zertifikat zum aktuellen Zeitpunkt gültig ist, ob es gesperrt / widerrufen wurde und warum. Solche Sperrlisten dienen vor allem dazu, Schlüssel zu sperren / widerrufen, die nicht mehr sicher sind, weil sie in falsche Hände geraten sind oder „geknackt“ wurden - in solchen Fällen muss das Zertifikat noch vor dem eigentlichen Ablaufdatum gesperrt werden, damit der Schlüssel nicht weiter verwendet wird. Sie sind daher ein wichtiger Teil der PKI.
DAC, Discretionary Access Controls	DAC, Discretionary Access Controls	DAC, Discretionary Access Controls	Der Datenbesitzer selbst erteilt die Erlaubnis, wer auf seine Daten zugreifen darf und wenn ja mit welchen Rechten.
détendeur des données	Datenbesitzer	data owner	Verantwortlich für die Datenintegrität, das Reporting und die Benutzung der Daten
signature numérique	digitale Unterschrift	digital signature	Bestätigt die Authentizität des Absenders. Ein Hash-Wert der Meldung wird erstellt und mit dem Private-Key des Absenders verschlüsselt. Mit dem Public-Key des Absenders kann der Hash-Wert wieder erstellt werden, andererseits kann an den Hash-Wert der empfangenen Meldung selbst erstellen und diese beiden Werte vergleichen.
administration électronique, cyberadministration, administration en ligne	elektronischer Behördenverkehr, elektronische Verwaltung	e-administration	(elektronische) Kommunikationsbeziehungen mit Behörden, im Gegensatz zu Kommunikationsbeziehungen zu anderen Unternehmen oder Privatpersonen

commerce électronique, commerce en ligne, cybercommerce	elektronischer Handel, Internethandel, E-Commerce	e-commerce	(elektronischer) Ein- & Verkauf von Waren und Dienstleistungen
impôts en lingne, taxation en ligne	elektronische Steuern	e-taxes	
vote électronique	elektronische Stmmabgabe	e-voting	
fédération	Föderation	federation	Federation ist eine Form der Organisation, bei der mehrere Teilnehmer, die über eine gewisse Eigenständigkeit verfügen über die Unternehmensgrenzen hinweg zusammengeschlossen werden
droit	Recht, Gesetz	law	
		logon IDs	
	anmelden	logon, login, log in, signon, sign on	Der Anmeldeprozess bei einem Computer
LRA, Local Registration Authority	LRA, Local Registration Authority	LRA, Local Registration Authority	
MAC, Mandatory Access Control	MAC, Mandatory Access Control	MAC, Mandatory Access Control	Logische Filter für die Zugangskontrolle. Einfache zwingende Regeln, welche nicht umgangen werden können. Alle MA auf Level x haben Zugriff auf eine bestimmte Ressource
mot de passe unique	Einmalpasswort	one-time password	Das Passwort ird nur einmal zur Authentisierung verwendet und anschliessend für ungültig erklärt. Sie gelten daher als besonders sicher und werden vor allem im Online-Banking-Bereich verwendet
mot de passe	Passwort	password	Mittel zur Authentifizierung eines Benutzers. Nach der Eigabe der User-ID behauptet der Benutzer, jemand zu sein, mit Hilfe des Passworts wird diese Behauptung überprüft. Der Wahl eines guten Passworts muss daher besondere Aufmerksamkeit geschenkt werden.
	Passwort Administration	password administration	Darunter versteht man folgende Tätigkeiten: - Erstellen eines Initialpassworts, in der Regel durch den Admministrator beim Anlegen eines Accounts - Passwortänderungen, in der Regel durch den Benutzer - Passwort zurücksetzen (bei Passwortverlust).
identité réelle	physische Identität	physical identity	Natürliche oder juristische Person
	PIN, persönliche Identifikationsnummer	PIN, personal identification number	eine spezielle Form eines Passwortes. Es werden ausschliesslich Zahlen verwendet, sind meist 4 Stellen lang und können nicht immer vom Benutzer frei gewählt werden. Häufig im Einsatz bei Bank- & Kreditkarten
IGC, infrastructure de gestion de clefs, ICP, infrastructure à clefs publiques	PKI	PKI, public key infrastructure	RFC 2527: Ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate sind meist auf Personen oder Maschinen festgelegt und werden zur Absicherung computergestützter Kommunikation verwendet.
	Grundsatz, Leitbild, Politik	policy	Politik, beinhalten die Geschäftsphilosophie über ein bestimmtes Thema
		provisioning	Verteilung von Informationen von einem System ins andere
pseudonyme, surnom	Pseudonym	pseudonym	Kontext bezogene Identität, z.B. User-ID eines Mitarbeiters, Spitzname, ... Ist oft nicht eindeutig einer Person zuzuordnen. Wird oft auch eingesetzt, um die wahre Identität zu verbergen.

clé public	öffentlicher Schlüssel	public key	Unter einem öffentlichen Schlüssel (englisch public key) versteht man in asymmetrischen Kryptosystemen Schlüssel, die jedem bekannt sein dürfen und zur Verschlüsselung eines Klartextes in einen Geheimtext genutzt werden können. Die Geheimtexte können hierbei später nur mit dem geheimen Schlüssel wieder entschlüsselt werden.
	public key encryption	public key encryption	Verschlüsselungsverfahren, welches zwei Schlüssel benötigt: Ein Schlüssel wird zum verschlüsseln gebraucht, der andere zum Entschlüsseln.
RA, Registration Authority AE, Autorité d'enregistrement	RA, Registration Authority	RA, Registration Authority	RFC 2527: Organisation, bei der Personen, Maschinen oder auch untergeordnete Zertifizierungsstellen Zertifikate beantragen können. Diese prüft die Richtigkeit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag der dann durch die Zertifizierungsstelle signiert wird.
rôles	Rollen	roles	Zusamenfassung von Tätigkeiten
single signon	Einmalanmeldeverfahren, Single Signon	single sign-on	SSO: Nach einmaligem Anmelden stehen dem Benutzer sämtliche Applikationen zur Verfügung, er muss sich nicht mehr von neuem in irgend ein System einloggen.
Identité technique	technische Identität	technical identity	Maschinen, Server, Applikationen usw. Es muss hier ein Owner definiert sein, um auch Haftungsfragen eindeutig klären zu können.
		trustlevel	Beziffert, wie vertrauenswürdig eine digitale Identität ist
administration des utilisateurs	Benutzerverwaltung	user management	Erfassung der Benutzer im EDV-System und Erteilung der entsprechenden Berechtigung. Deckt den gesamten Life-Cycle des Benutzer ab
Identité virtuelle	virtuelle Identität	virtual identity	Alle Ausweise, welche eindeutig einer Identität zugeordnet weden können

15. Spezialfälle zum generischen Modell

In diesem Bereich wird kurz die Rechtslage in der Schweiz aus juristischer Sicht aufgezeigt.

Gemäss schweizerischer Rechtssprechung ist ein Vertrag gültig, wenn sich zwei Parteien geeinigt haben. Es gilt der einfache, formfreie Vertrag. Aus diesem Grund sind ein abgeschlossenes SLA und NDA ein gültiger Vertrag.

Neben dem einfachen, formfreien Vertrag gibt es branchenspezifische Abweichungen, bei welchen die Form oder die Schriftlichkeit oder eine spezielle Registerführung gefordert wird.

Solche Spezialfälle sind:

- Arbeitsvertrag
- Handelsregister
- Grundbuch
- Baugesuch

15.1 Einfacher formfreier Vertrag

In der Schweiz ist in der Regel ein Vertrag formfrei.

Sofern die Vertragsparteien sich einigen können, ist der Vertrag gültig.

In Spezialgebieten können von Branchen her anderweitige Formulierungen gefordert werden.

15.2 Spezielle Registerführung

Das Gesetz benennt Verträge, welche eine spezielle Registerführung erfordern:

- Handelsregister
- Grundbuch
- ...

15.3 Öffentliche Beurkundung

Das Gesetz benennt Verträge, bei welchem eine öffentliche Beurkundung notwendig ist:

- Grundbuch
- Baugesuch
- ...

15.4 Kollektive Unterschrift

Spezielle Policy bei welcher eine Authentisierung zwei Identitäten gleichzeitig benötigt.

Dadurch entstehen zusätzliche Anforderungen an die entsprechenden Fachapplikationen.

15.5 Internationale Geschäftsverhältnisse

Internationale Verträge haben besondere Regeln.

Spezielle internationale Vereinbarungen werden in Apostille formuliert.

15.6 Delegation

Prüfung der Authentizität der Identität kann auch von externem Service Provider erfolgen.

Die Details werden zwischen Service-Eigentümer, Applikationsentwickler und dem Authentisierungs-Service Provider abgesprochen

Vertrauensbeziehungen bestehenden aus Güte und Haftung zwischen Authentisierungs-Service Provider und Fachapplikations-Eigentümer.

15.7 Stellvertretung

Die Stellvertreter Regelung ist ein Spezialfall der Delegation.

15.8 Pseudonyme

In vielen Fällen ist eine Verwendung von Pseudonymen angebracht. Pseudonyme lassen sich auf Identitäten zurückführen. Der Service-Eigentümer definiert das Vertrauensverhältnis für die Verarbeitung von Pseudonymen mit dem Service Provider.

15.9 Anonymität

Spezialfall von Pseudonym

Das verwendete Pseudonym lässt sich nicht auf eine referentielle Identität zurückverfolgen

15.10 Lizenzvertrag

Eine interessante Variante ist der **Linzenzvertrag**, bei welchem die Nutzung im Rahmen einer Lizenz definiert wird.

15.11 Kontextbasiertes Rollenmodell

- Richter in einem Fall Richter im anderen Angeklagter