Generalversammlung eCH

13. März 2009, Luzern

eCH-Fachgruppe IAM (Identity und Access Management)

Co-Fachgruppenleiter: Hans Häni AFI Kanton Thurgau

Identity und Access Management

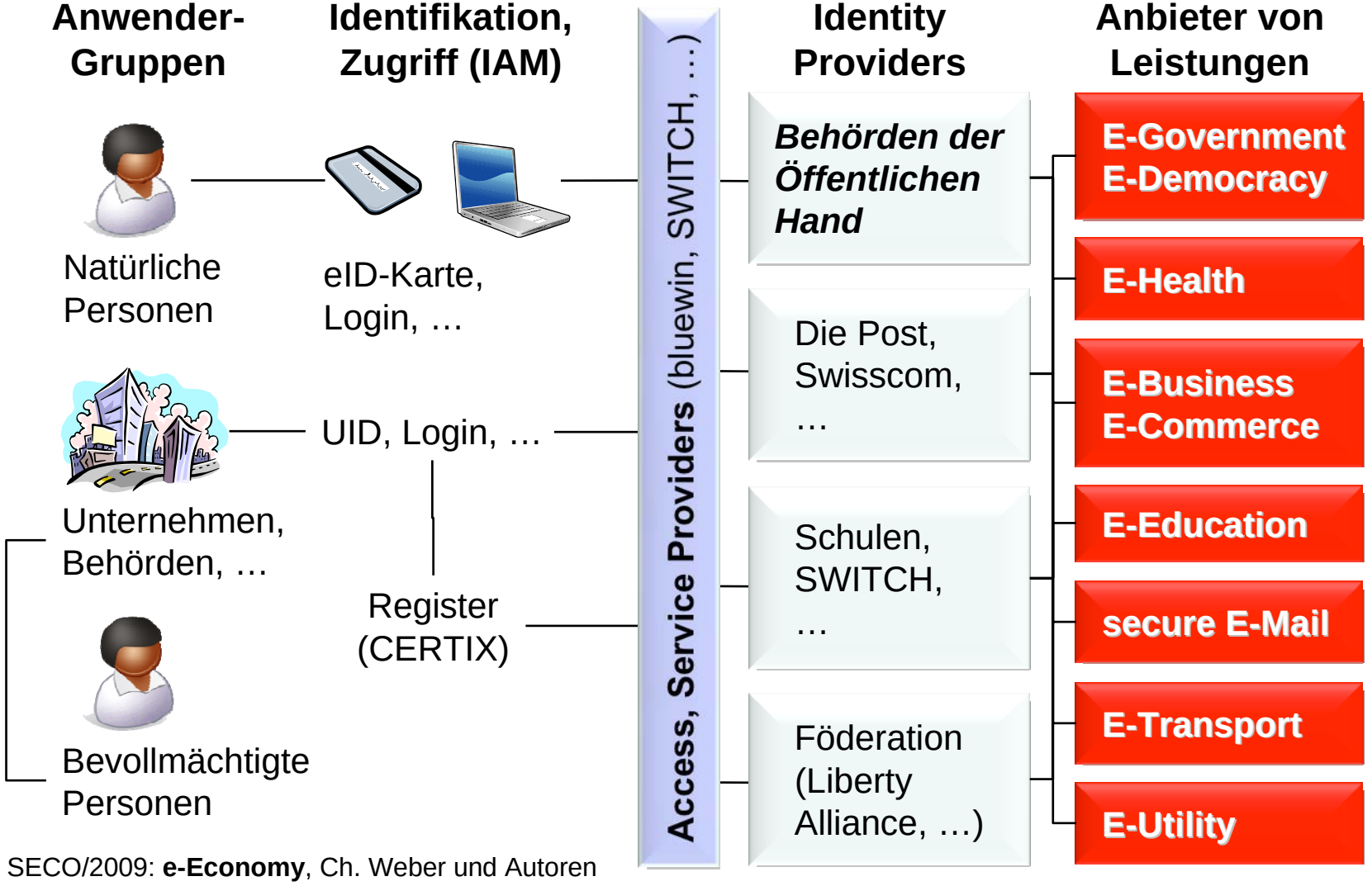
Basisbausteine für Anwendungen E-Government / E-Health

Identity und Access Management

- Einsatzbereich
- Generelle Anforderungen
- IAM-Referenzmodell
- Generische IT-Architektur
- Prozess/Architektur-Hauptfunktionen
- Implementierung
- Interoperabilität
- eCH-Standards
- Pilotprojekte

Identity und Access Management

Einsatz im E-Wirtschaftsraum



SECO/2009: **e-Economy**, Ch. Weber und Autoren

Identity und Access Management

Governance, Risk-Management, Compliance (GRC)

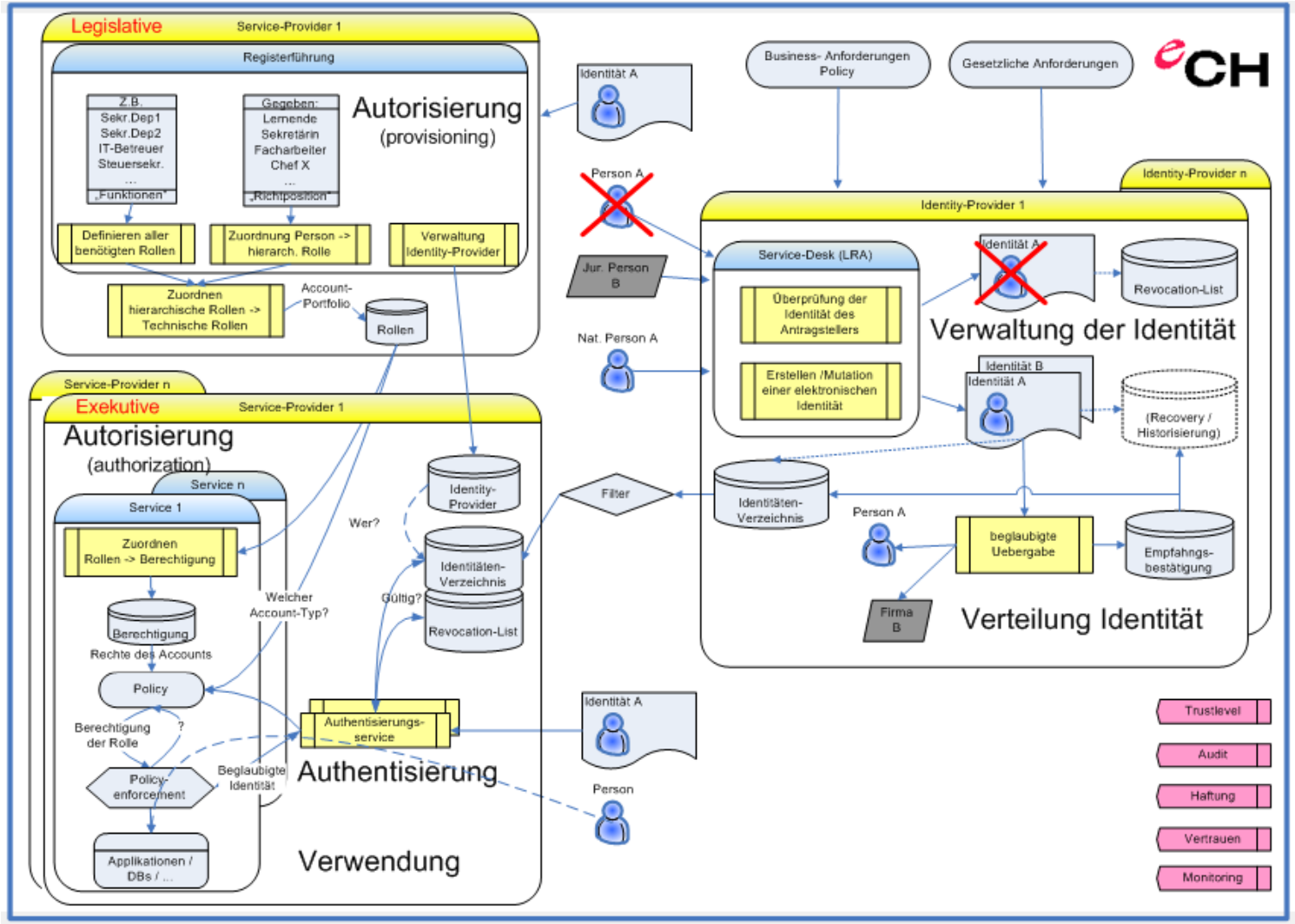
- Bestandteil und Grundlage für einen rechtlich und operationell sicheren E-Sozial- und E-Wirtschaftsraum.
- Unterstützt die Informationssicherheit gemäss ISO 27001.
- Risiko-Analyse aus Sicht Angebot bestimmt Schutzbedarf.
- Garantiert den Datenschutz in jedem Rechtskontext.
- Basiert auf Interoperabilität, national und international.
- Basiert auf international kompatiblen Modellen und Architekturen.
- Möglichst schlank und transparent.
- Verifizierbar und auditierbar.

Anforderungen seitens der Benutzer

- Registriert sich nur einmal, nach dem Motto „nur soviel wie notwendig“, um mit allen föderierten Systemen zu interagieren.
- Benötigt nur eine (seine) Client-SW, um mit allen föderierten Systemen zu interagieren.
- Muss darauf vertrauen können, dass sein Datenschutz und seine weiteren rechtlichen Belange jederzeit gewahrt sind.
- Bleibt unbehelligt von Einflüssen föderaler Entscheide und Erweiterungen.

Identity und Access Management

IAM-Referenzmodell



Identity und Access Management

IAM-Meta-Prozesse

Legislative = Prozess-Organisation

„Autorisierung des Angebots“
„Autorisierung der „Zugriffsautorisierer und Regeln“

- Prozessorganisations-Verantwortlicher	(Prozess-Autorisierung)
- Prozess-Beteiligte (Identity-, Service Provider)	(Autorisierungs-Management)
- Prozess-Auditor	(Revision)

Exekutive = Prozess-Management

„Registrierung“
„Authentisierung“
„Applikation/Service-Autorisierung“

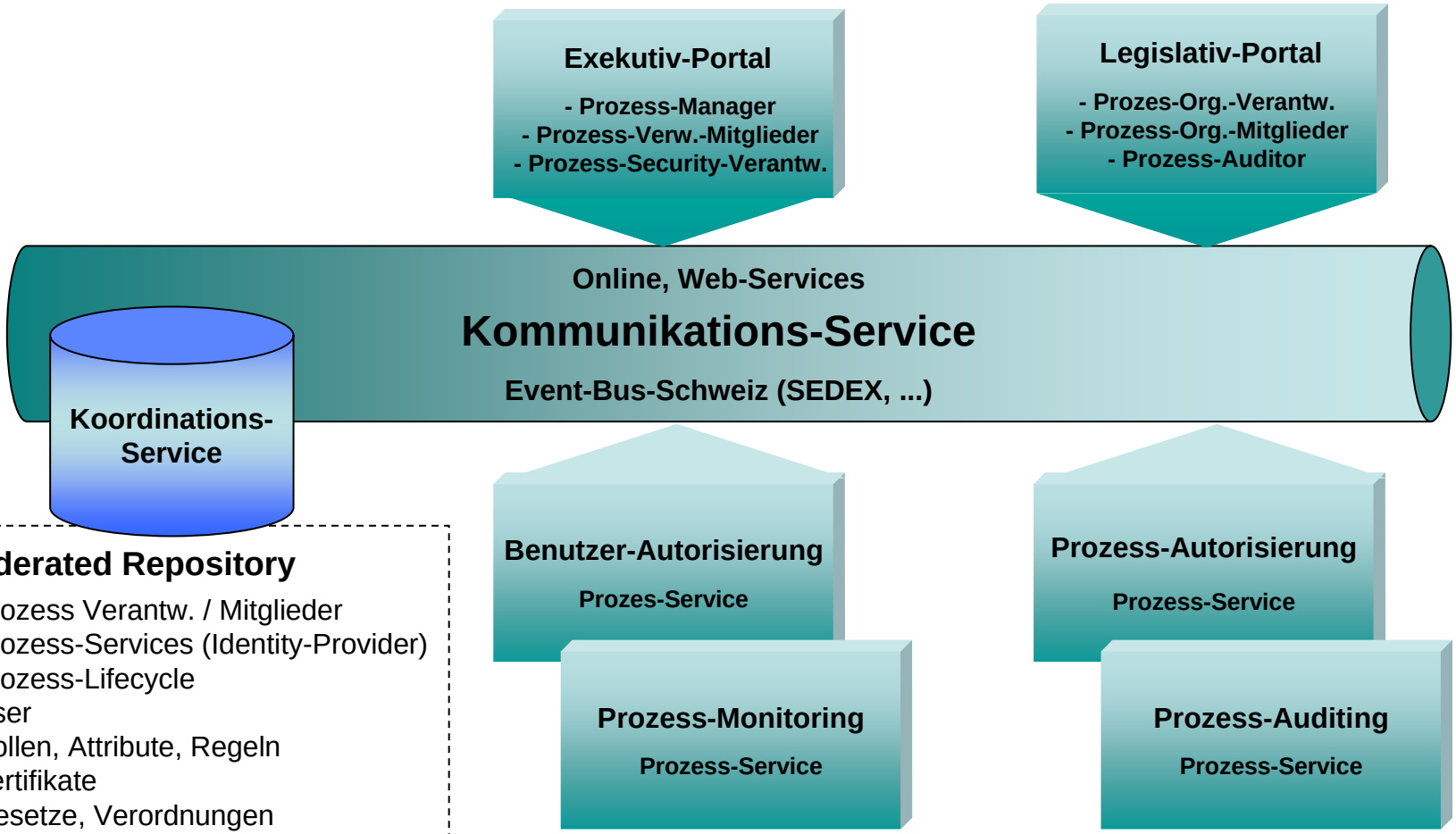
- Prozess-Manager	(Rolle, Attribute, Regeln)	(User-Autorisierung)
- Prozess-Verwaltungsmitglieder		(User-Management)
- Prozess-Security-Verantwortlicher		(Monitoring)

IAM-IT-Architektur = SOA (Service Oriented Architecture)

- Prozess-Portal	Zugang im Berechtigungskontext
- Prozess-Services	Koordinations-, Kommunikations- und Portaldienste
- Prozess-SLA	Gesetze, Verträge, Serviceleistungen
- Prozess-Monitoring	Security, Revision

Identity und Access Management

IAM-IT-Architektur = SOA



Identity Management

- Die relevanten Identifikatoren (PID, UID, ...), Credentials und Attribute (z.B. Rolle) sind durch den Applikations/Serviceanbieter zu bestimmen (Risiko-Management →Schutzbedarf).
- Forderung von sicheren Identifikatoren, welche via entsprechender Register verifizierbare sind.
- Zweckmässige, mehrfach verwendbare Credentials und Attribute, welche in zugäglichen Repositories verwaltet sind.
- ID-Daten sind automatisch verarbeitbar, d.h. mit Verarbeitungsregeln von einem Kontext in einen anderen umsetzbar.
- ID-Daten sind in zweckorientierten ID-Repositories zu halten, welche untereinander synchronisierbar sind.

Registrierung der Identität

- Der Benutzer (Individuum, Ressource) wird der Registrierstelle des Applikations/Serviceanbieters bekannt gemacht.
- Die Aufnahme ins Identity-Repository erfolgt nach einer Authentisierung des Benutzers aufgrund der vorbestimmten notwendigen Identitätsdaten (Identifikatoren, Credentials).
- Akzeptanz von verschiedenen, im Applikations/Service-Angebotsbereich (inkl. föderierter Bereiche) bekannten und verifizierbaren Identitätsdaten.
- Präferenz für allgemein rechtlich anerkannter Identifikatoren, welche mittels eines Registers (inkl. Revoke-Liste) online verifizierbar sind.

Autorisierung (Berechtigungs-Management)

- Das konkrete Zuteilen von zuvor definierten Rechten an eine Identität, gemäss deren Rolle oder relevanten Attribute, zu einer Applikation oder einen Service, nachdem diese mit dem notwendigen Sicherheits-Level authentisiert wurde.
- Zuteilung nur so vieler Rechte in bestimmter Funktion, wie notwendig, in der Breite, Tiefe und bezüglich Zeitraum.
- Die Zugangs-Autorisierung für eine Applikation, einen Service ist bestimmt durch:
  - die von der Applikation, dem Service vorgegeben Bedingungen, insbes. dem notwendigen Sicherheitslevel
  - eine entsprechend notwendige Authentisierung vor dem Zugang
- Autorisierung bedeutet also Zuordnung von Benutzern zur Applikation oder zum Service.

Bestimmung des Sicherheits-Levels

- Wird bestimmt durch die Schutzbedarfsanforderungen der Applikation oder Services bezüglich:
  - Authentizität
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- Ermittelt durch eine Risko-Analyse, gemäss ISO 27001, durch Betrachtung der Eintretenswahrscheinlichkeit und dem möglichen Schadensausmass von unrechtlichen Interaktionen.
- 4 Sicherheits-Levels für Authentifikation (**AAL's**, gemäss EU/IDABC)
  - **L1: Minimal Assurance (= Password)**
  - **L2: Low Assurance (= Passwordprotectedtransport)**
  - **L3: Substantial Assurance (= Software PKI)**
  - **L4: High Assurance (= Smartcard PKI)**

(EU/**IDABC** = EU **I**nteroperable **D**elivery of European e-government services to public **A**dministrations, **B**usinesse and **C**itizens)

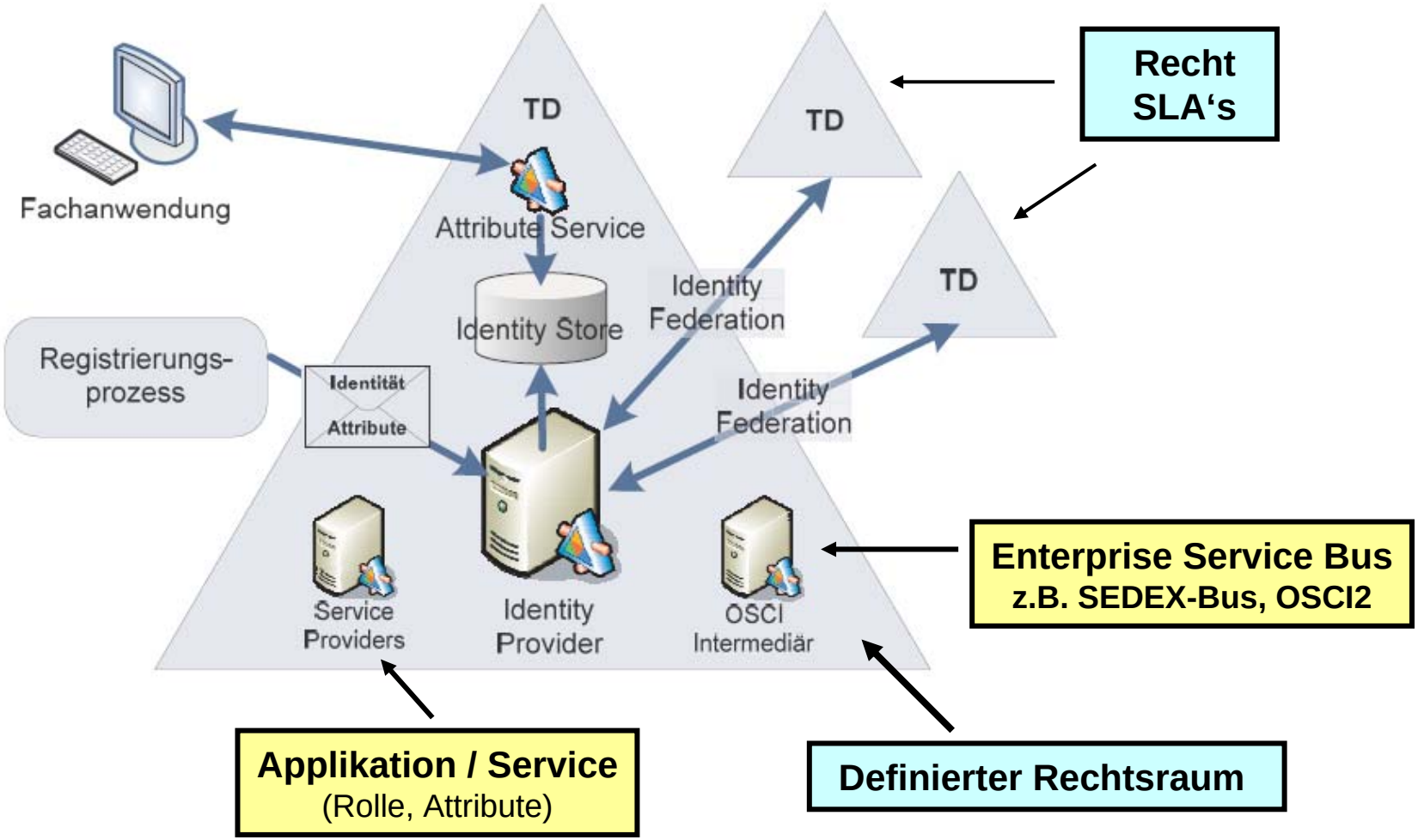
Auditing / Monitoring

- Sind die Prozesse und Services autorisiert und von wem, wann und bis wann? (Legislative)
- Wer ist autorisiert für diese Prozesse und Services die Zugangs-berechtigungen vorzunehmen und nach welchen autorisierten Regeln wird der Zugang automatisch erstellt? (Legislative)
- Was für Benutzer haben gem. SLA mit welchem Sicherheitslevel (Authentisierung) von wann bis wann den Zugang?
- Sind die verwendeten Identifikatoren und Credentials über frei zugängliche, rechtlich zuverlässige Register und Repositories verifizierbar?
- Werden in den föderierten Domänen die notwendigen Sicher-heitsstandards und die rechtlichen Bedingungen eingehalten?
- Was muss, was darf „monitored“ und an wen gemeldet werden?

Identity und Access Management

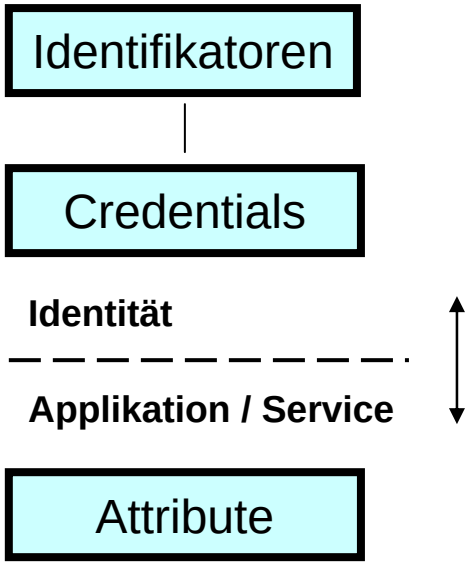
Implementierung von IAM in der Domäne

(Aus SAFE-Grobkonzept D, Dez. 2007)



Identity und Access Management

IAM-Implementierungsschritte



Registrierung / Authentisierung

Der Sicherheitslevel (AAL) der Applikation, des Services bestimmt die Art der Registrierung, nach dem Prinzip **„Nur soviel wie notwendig“**

Identity Provider (Register, SLA‘s)

Autorisierung

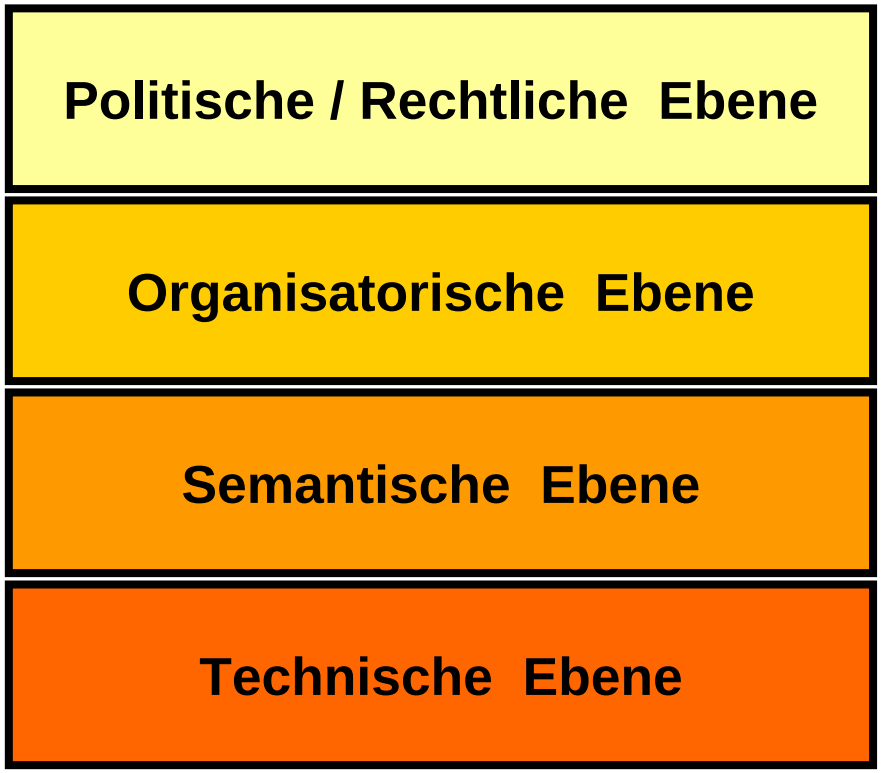
„Mapping“ Identities zu Applikation / Service, gemäss festgelegter Identifikatoren, Credentials und Attribute

Identity Store, Attribute Service, Application

1. **Risk-Assessment --> AAL (Authentication Assurance Level)**
2. **Registrierungs- / Authentisieungs-Prozess**
3. **Service Level Agreement (Rechtsbasis, SLA‘s)**
4. **Validierung, Auditierung**

Identity und Access Management

Interoperabilitäts-Ebenen



- Gesetze, Verordnungen
- Vereinbarungen, SLA‘s

- Standardisierte Prozesse
- Koordinationsprozesse

- Terminologien
- Nomenklaturen

- Internationale Standards
- Nat. und intenat. Normen

→ **Roadmap for a pan-european eIDM-Framework by 2010**
→ **eID Interoperability for PEGS (Pan-European E-Gov Services)**
→ **EU/IDABC Authentication Policy**

Identity und Access Management

eCH-Standards

- eCH-00xx IAM-Referenzmodell (Whitepaper)
  Nach- und Ausarbeitung Whitepaper vom April 2007
- eCH-00xx IAM-SOA (**S**ervice **O**riented **A**rchitecture)
  SEAC: Im Rahmen eGov/eHealth-Architektur
- eCH-00xx IAM-Design (Anforderungen, Prinzipien und Regeln)
  SEAC/IAM: in Arbeit bis Sommer 2009
- eCH-0014 SAGA 5 (i.S. Kap. 8)
  Einsatz internationaler technischer Standards
- eCH-00xx IAM-Maturitätsanalyse / Vorgehen
  Instrument für IST-Analyse und „Best Practice“-Vorgehen (CMMI)

SEAC = **S**wiss **E**-Government **A**rchitecture **C**ommunity des ISB

Identity und Access Management

IAM-Pilotprojekte

IAM-Projekte sind IT-Infrastrukturprojekte

→ Realisierung im Rahmen E-Government ISB/ffO B2.06

Herausforderungen:

- Rechtliche Rahmenbedingungen (Nutzen eID, UID, …)
- Aufbau von rechtlich beglaubigten Register und Repositories, zentral und/oder dezentral.
- Bestimmen föderierter Domänen (Bund, Kantone, Gemeinden) mit den notwendigen Identity Providers und den Attribute Services.
- Entscheidungs-Gremien (eGov: ffO B2.06?)

Relativ problemlos:

- IT-Standards (International: Open Source, Microsoft, IBM, SAP, …)
- Technische Implementierung

Danke für ihre Unterstützung

?