



Generalversammlung eCH, 7. März 2008, Fribourg

Fachgruppe IAM (Identity & Access Management)

Fachgruppenleitung: Hans Häni    AFI Kanton Thurgau  
Markus Itin    KITT Kanton Zürich

**IAM auf dem Weg zum eCH-Standard**



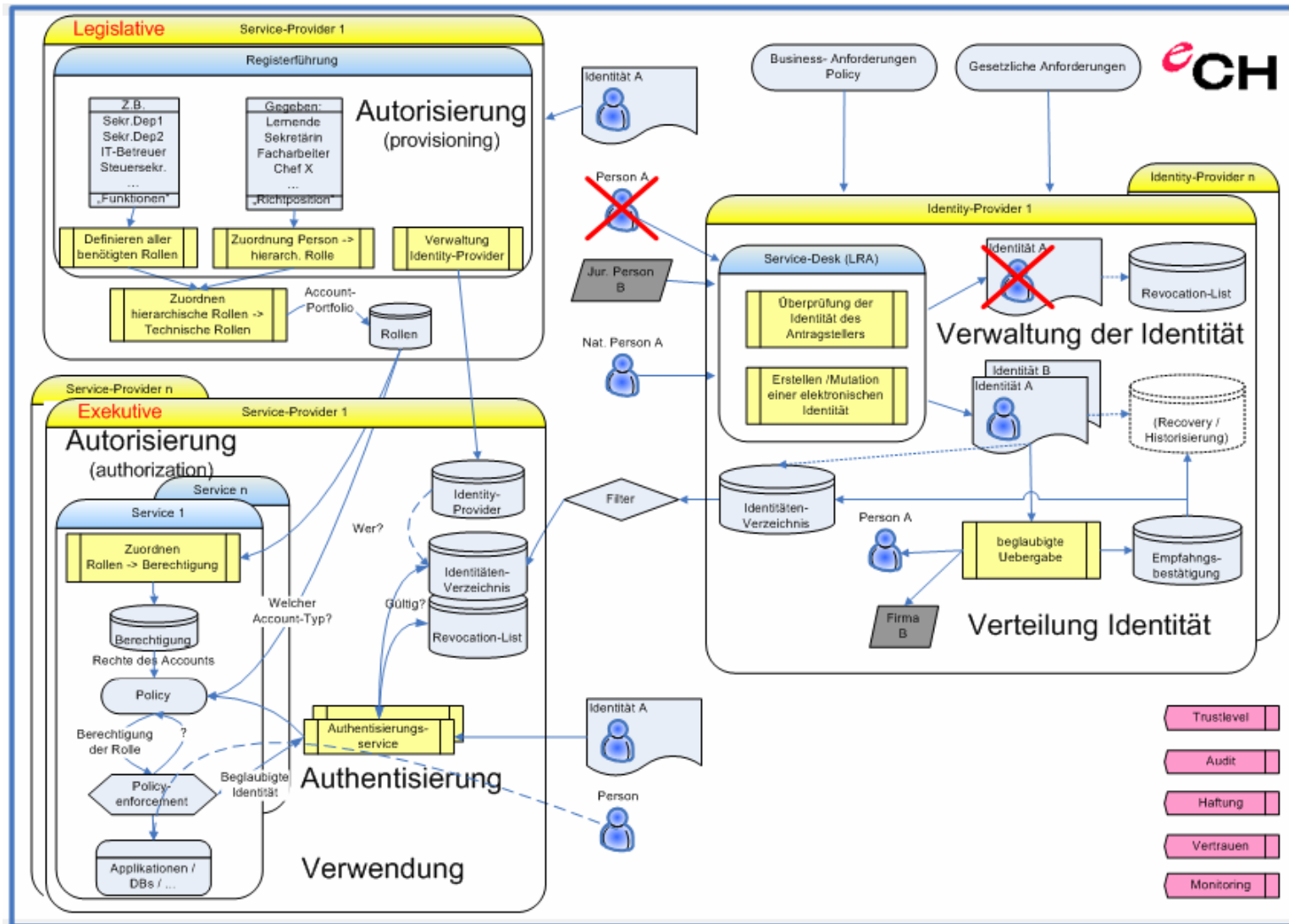
## IAM auf dem Weg zum Standard

- Erarbeitete Resultate und Erkenntnisse
- Stand heute, nächste Schritte
- Input aus Projekten, Hauptansatz
- Roadmap
- Fragen

## Erarbeitete Resultate

- April 2007: Referenzmodell des FG-Teams „IAM-Research“  
(als Dokument im eCH-Internetauftritt unter FG IAM)

## IAM Referenzmodell



## Erarbeitete Resultate und Erkenntnisse

- Y06/07: FG-Team „IAM-Scope“ erarbeitet Ansätze zu „WAS“ und „WIE“ in eCH-IAM Best Practice und Standards festzulegen sind
- Haupterkenntnisse daraus sind:
  - IAM ist in Form von Prozessen zu beschreiben
  - Auf welchem „Trustlevel“ jemand Zutritt haben muss ist nicht so von Bedeutung
  - Die Autorisierungsprozesse im Systemkontext und die IT-Architektur sind die Herausforderung
  - Es ist in erster Linie ein organisatorisches Thema und in zweiter Linie ein IT-Problem
  - Die relevanten internationalen IT-Standards sind weitgehend erarbeitet und in einer Konsolidierungsphase, i.B. unter Liberty Alliance
  - Es geht um „Compliance“ und „Governance“
  - Sept. 07: Der Standardisierungsprozess muss mit und anhand Key-eGov/eHealth-Projekte koordiniert erfolgen
  - Einbezug der Resultate aus diesen Key-Projekten
  - FG-Reorganisation: Nur noch ein IAM-Team



## Stand heute

- Reorganisation der FG IAM mit Einbezug neuer Mitglieder erfolgt
- Key-Projekte eruiert und mit Projekt-Schlüsselpersonen Kontakt aufgenommen (i.B. IAM-Projekte ZH und SG, Behördenverzeichnis, Gesundheitsberuferegister)
- Koordination mit eGov-Geschäftsstelle ISB und mit Koordinationsstelle eHealth im BAG gestartet
- IAM-Prozesse affin zu eGovernment-Geschäftsarchitektur beschreiben (Referenzmodell M. Schaffroth/W. Müller)
- Relevante Prozess- und Architekturansätze sind erkannt und in Verifizierung
- Sind im Einklang mit internationalen Standards
  - Liberty Alliance:
    - IGF (Identity Governance Framework) = Federation
    - LIAF (Liberty Identity Assurance Framework)
  - OASIS: SAML, XACML, ...
  - WS-\* (WS-Security, WS-Trust, WS-MetadataExchange, WS-SecurityPolicy ... )
  - Microsoft: CardSpace, Identity Metasystem, Windows Live ID
  - IBM/MS/... : WS-Federation (SOAP, SAML)

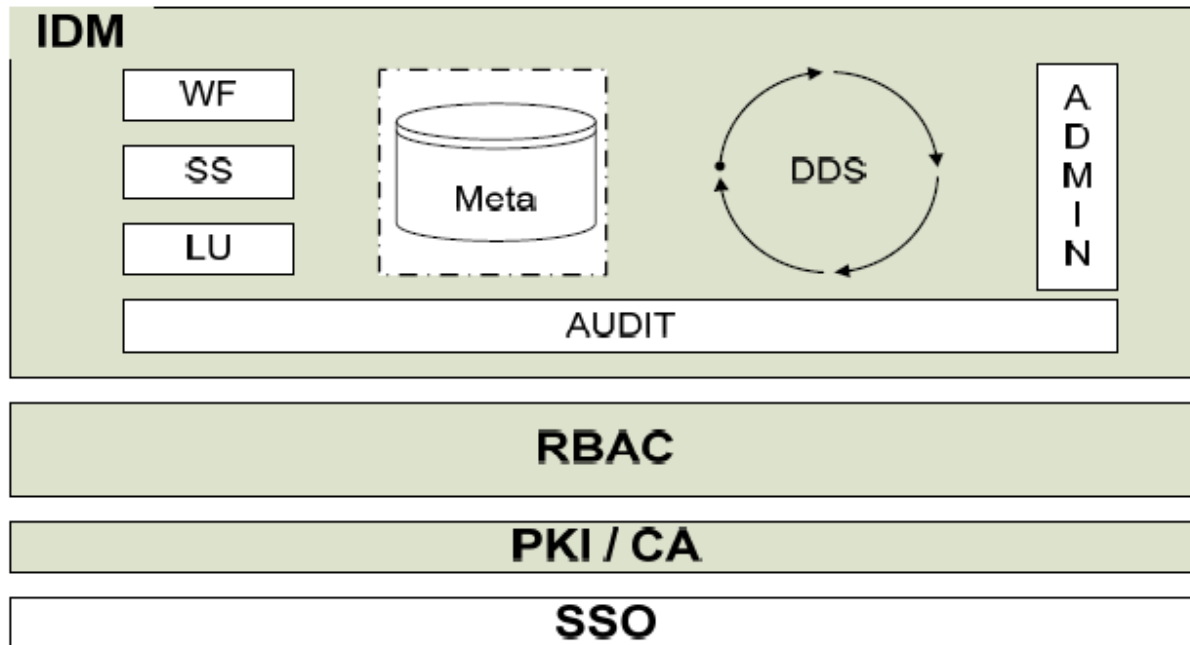


## Übernommenes aus Projekten

- Projekt IAM Kanton St.Gallen
- Projekt PKI-IAM Kanton Zürich
- Projekt RHG, Sedex BfS/ISB
- Vision/Konzept Event Bus Schweiz EBS
- Projekt Reference E-Gov BK
- eGov-Geschäftsmodell ISB (eCH 00..)
- SOA als IAM-IT-Architektur (MCM-Taxonomie, Uni St.Gallen)



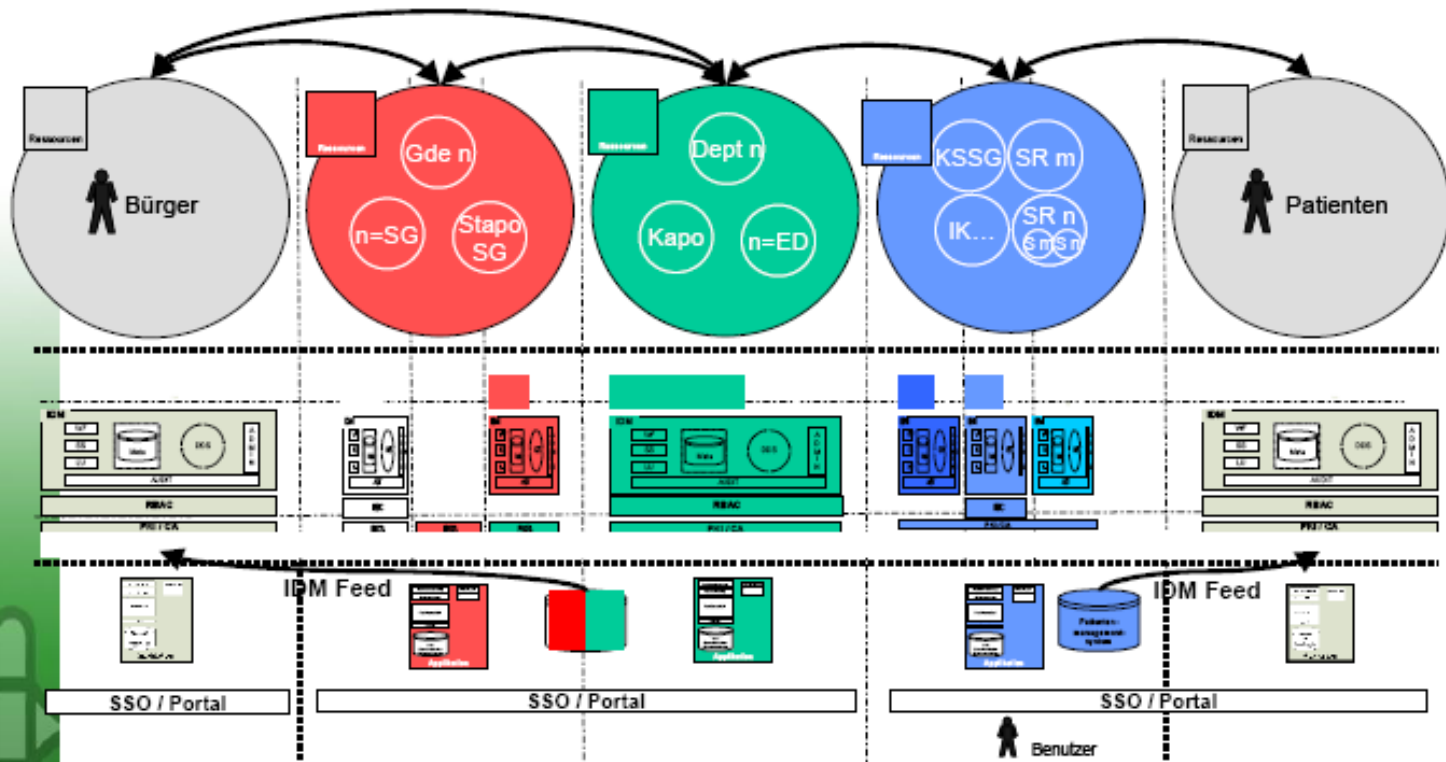
## Begriffe, Einordnung, Mechanik: Technische IDM Bausteine





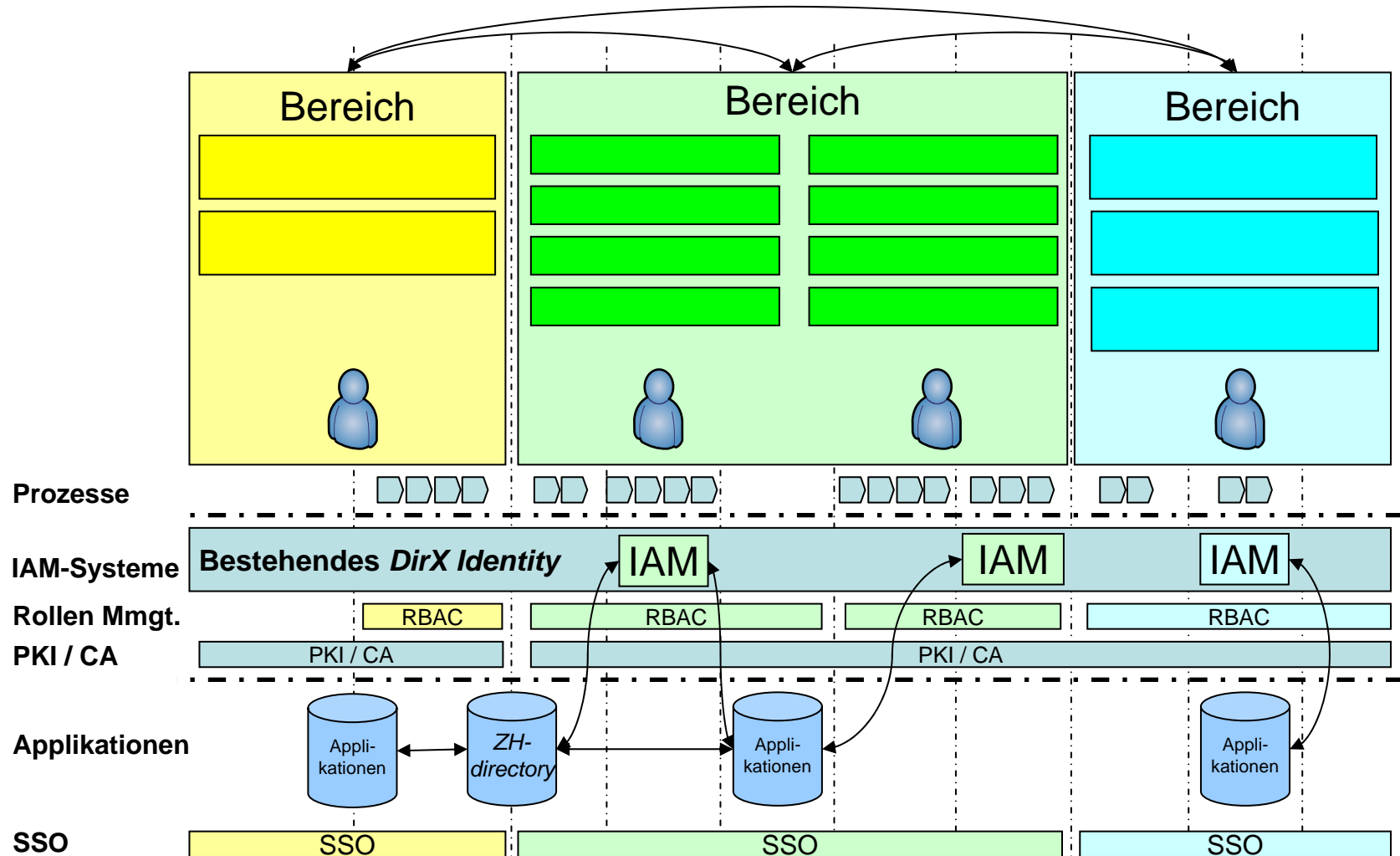


## Szenario: Federation



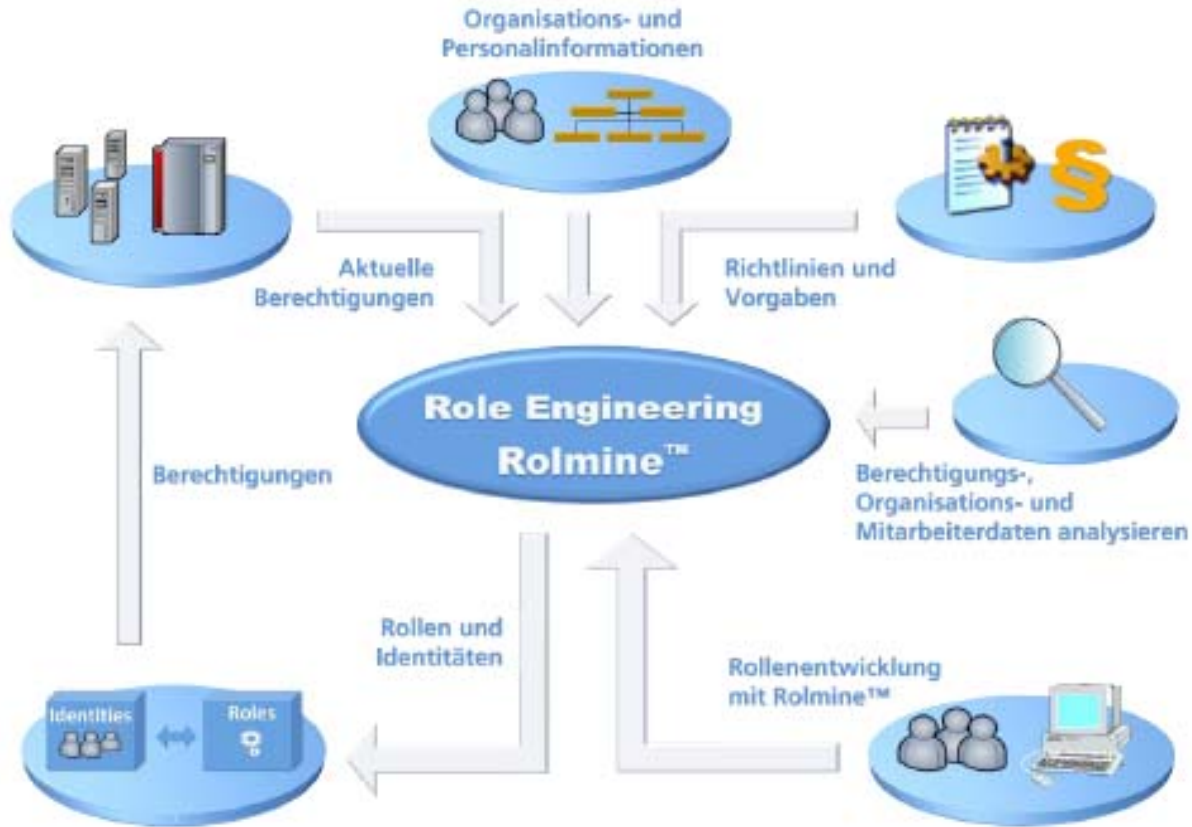


Lösungsvorschlag Kt. ZH  
Verbindender Ansatz mit Federation



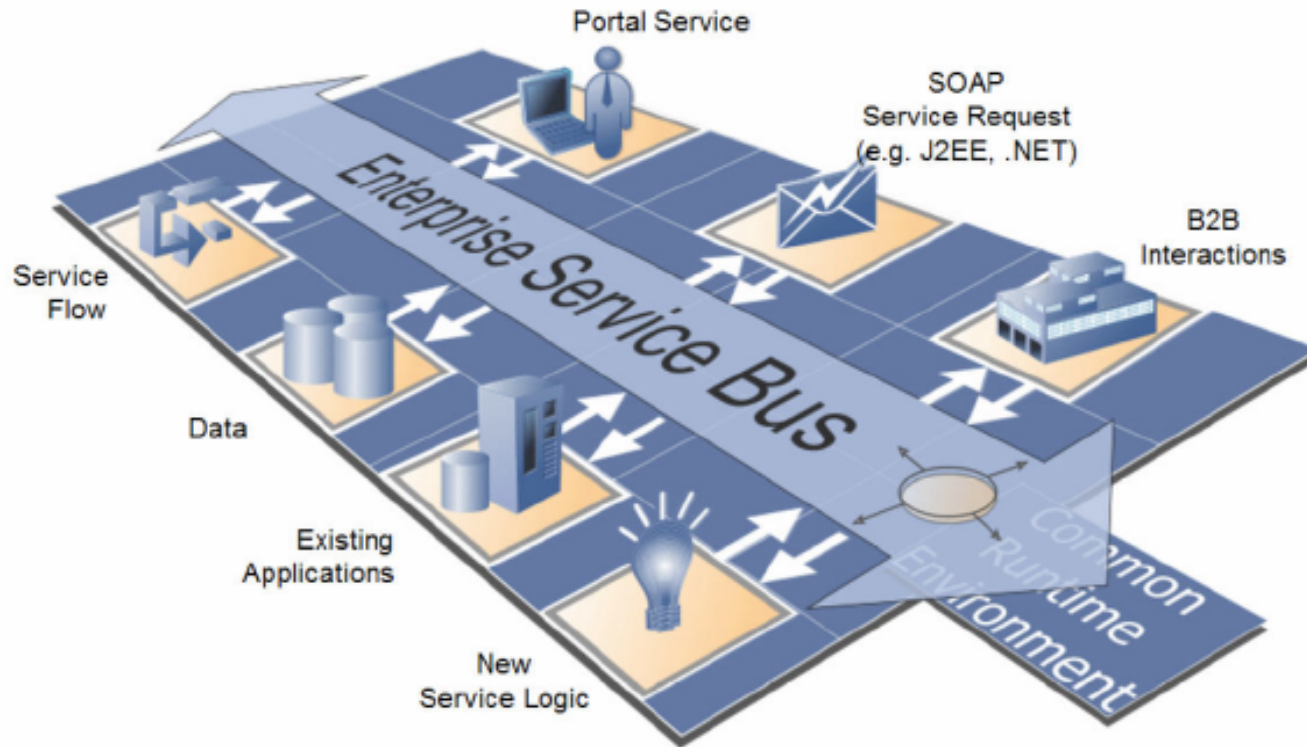


## Rollen-Management



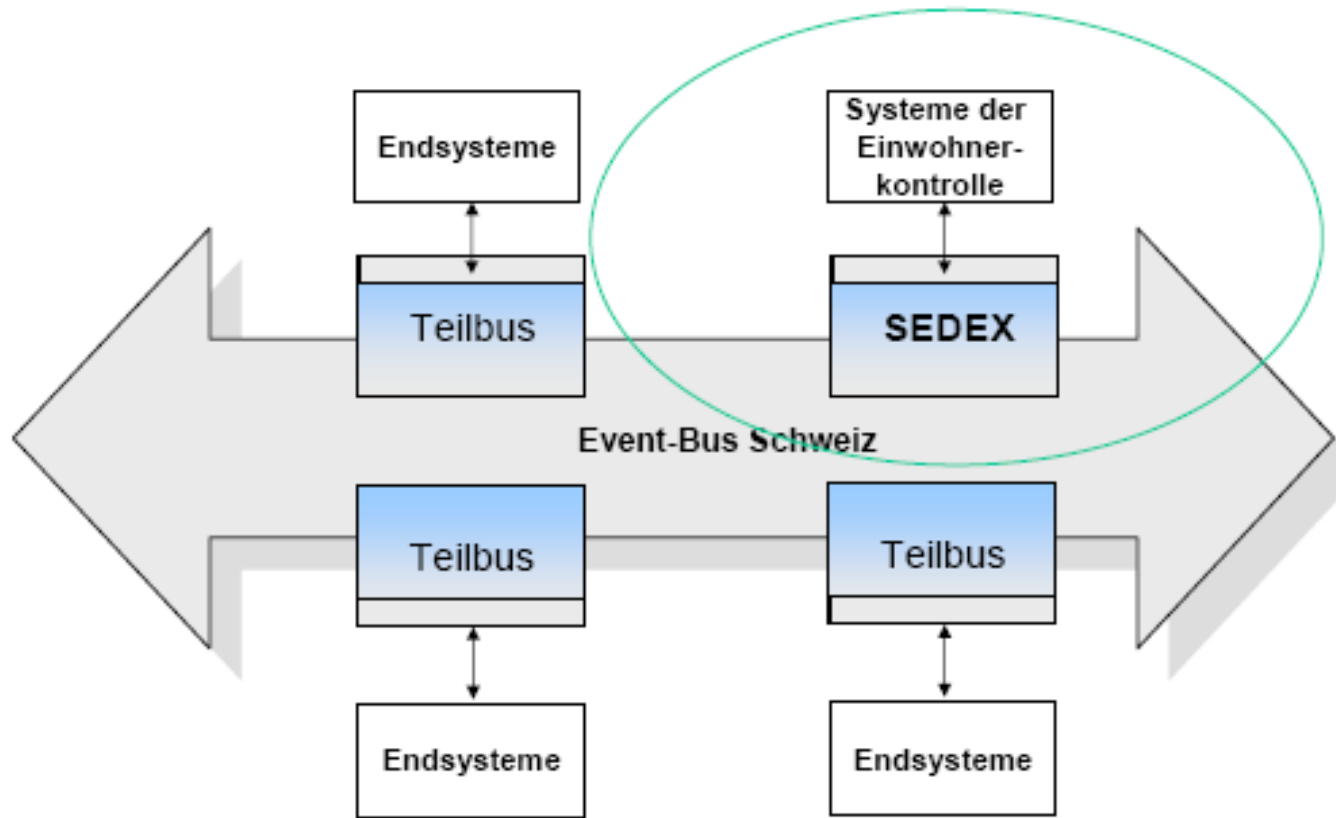


## Event Bus Schweiz



\* Patterns: Implementing an SOA Using an Enterprise Service Bus, IBM Redbook, 2004

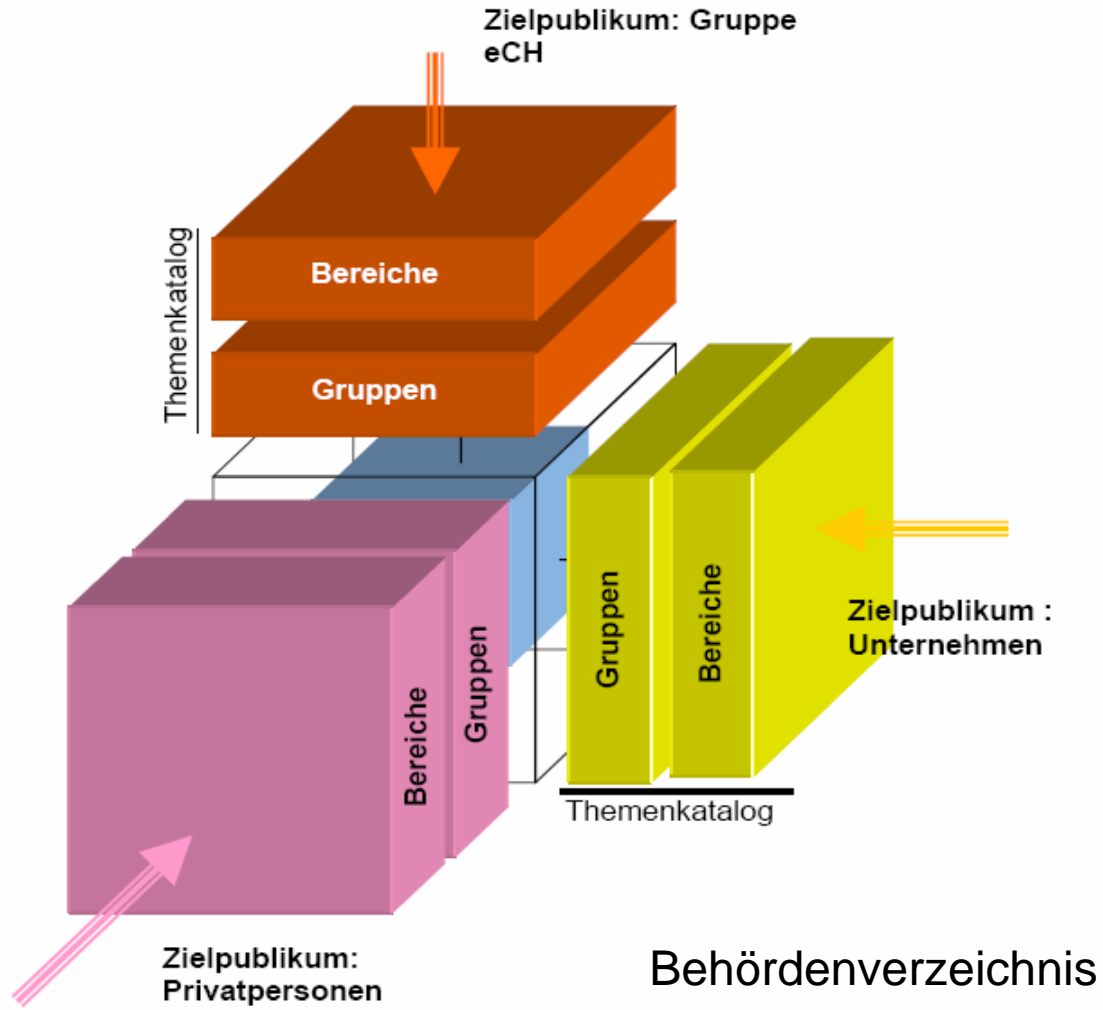
## SEDEX als erster Teilbus des Event-Bus Schweiz



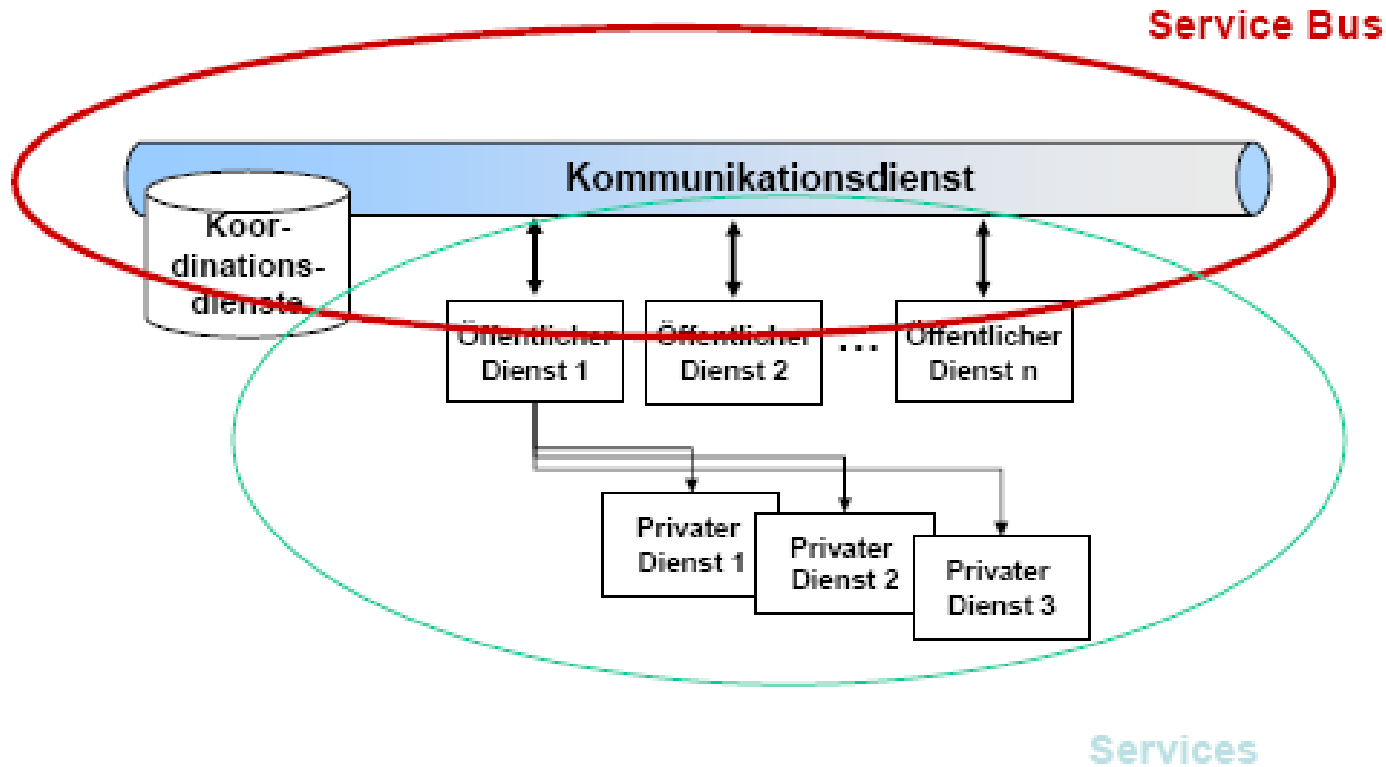
\* Willy Müller, Case Study: Event Bus Schweiz, Netzguide e-Government, 2006



## Projekt „Reference E-Gov“



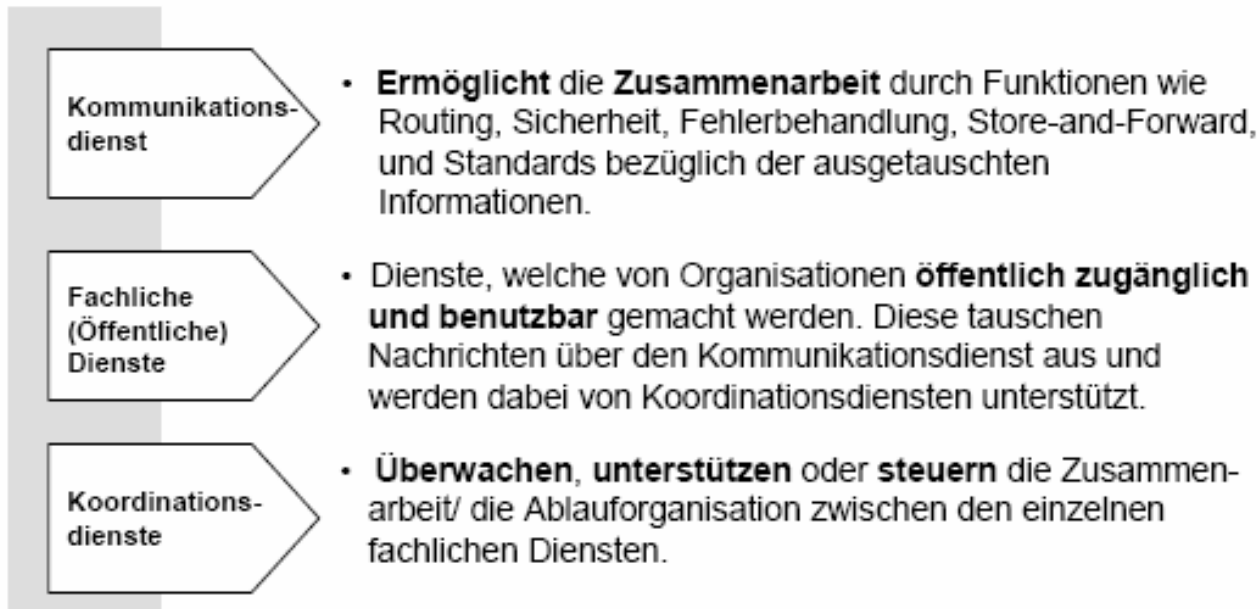
## MCM SOA-Taxonomie (1/2)



Aus eGov-Symposium Nov.07: Prof. Dr. B.F.. Schmid, UNI St.Gallen



## MCM SOA-Taxonomie (2/2)



Aus eGov-Symposium Nov.07: Prof. Dr. B.F. Schmid, UNI St.Gallen



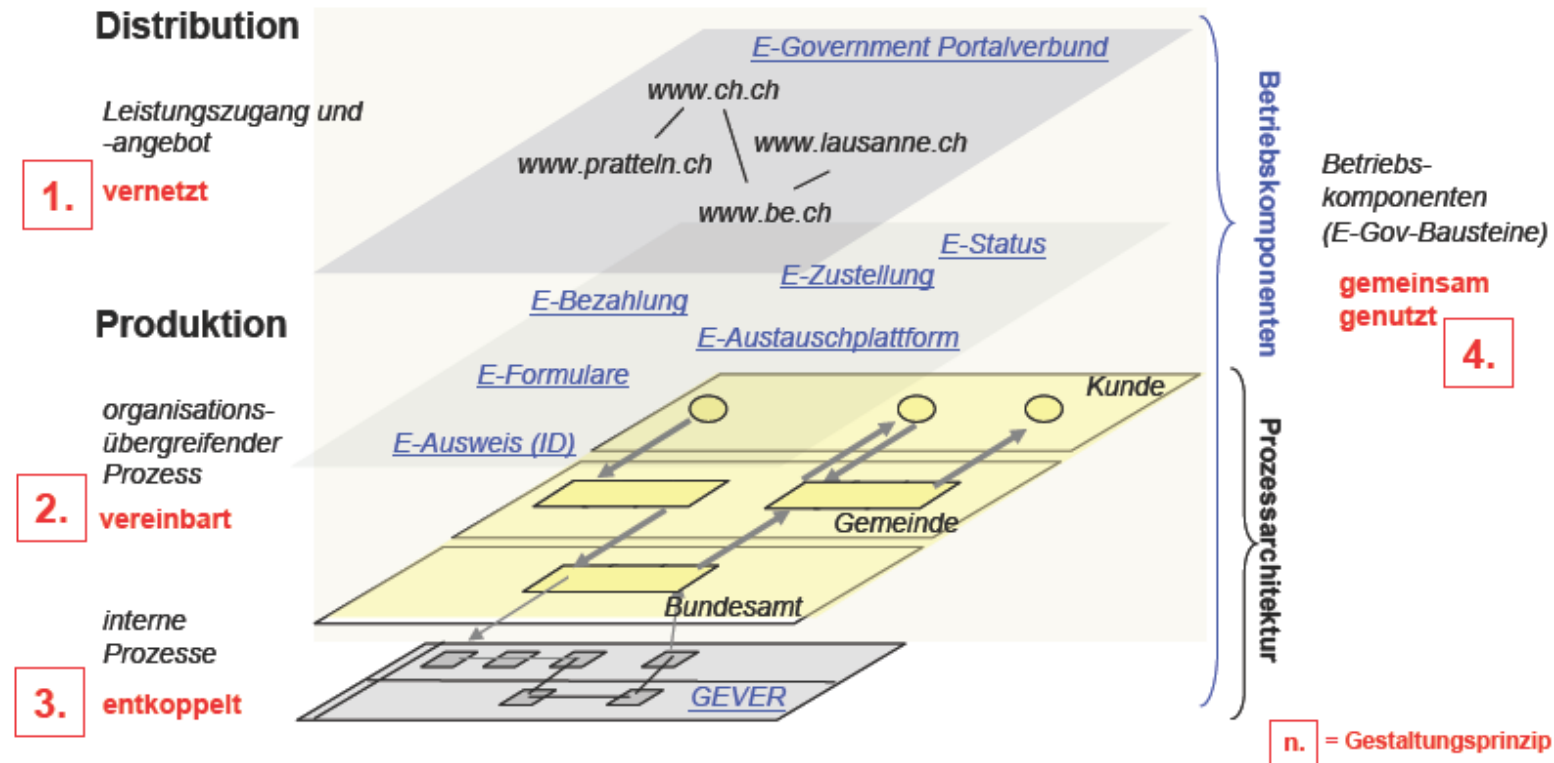


## Hauptansatz für Best Practice / Standard

- IAM-Prozesse als eGovernment-Geschäftsarchitektur (Referenzmodell M. Schaffroth/W. Müller)
- IAM als Meta-Prozess
- IAM-IT-Architektur = SOA (Service Oriented Architecture)
- Use Case aus Liberty Alliance, IGF



## Referenzmodell der Geschäftsarchitektur verbindet vier Gestaltungselemente und -prinzipien\*



\*vgl. dazu das Konzept des „operating model“ nach Ross/Weill/Robertson: Enterprise Architecture as Strategy (2006)



## IAM als Meta-Prozesse

(Liberty Alliance: Federation, IBM/MS: WS-Federation)

### Prozessorganisation (Legislative)

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

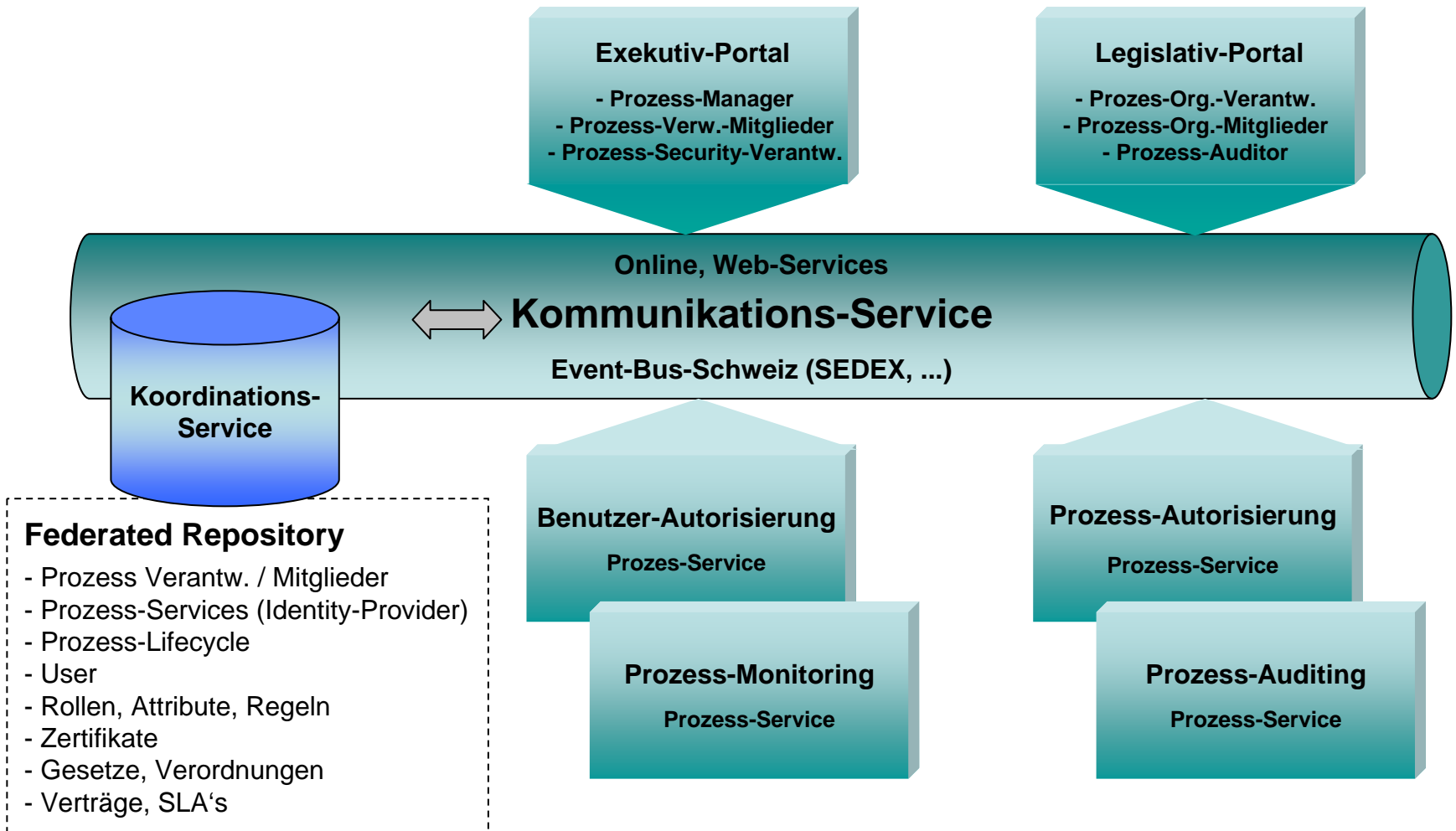
### Prozessmanagement (Exekutive)

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

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

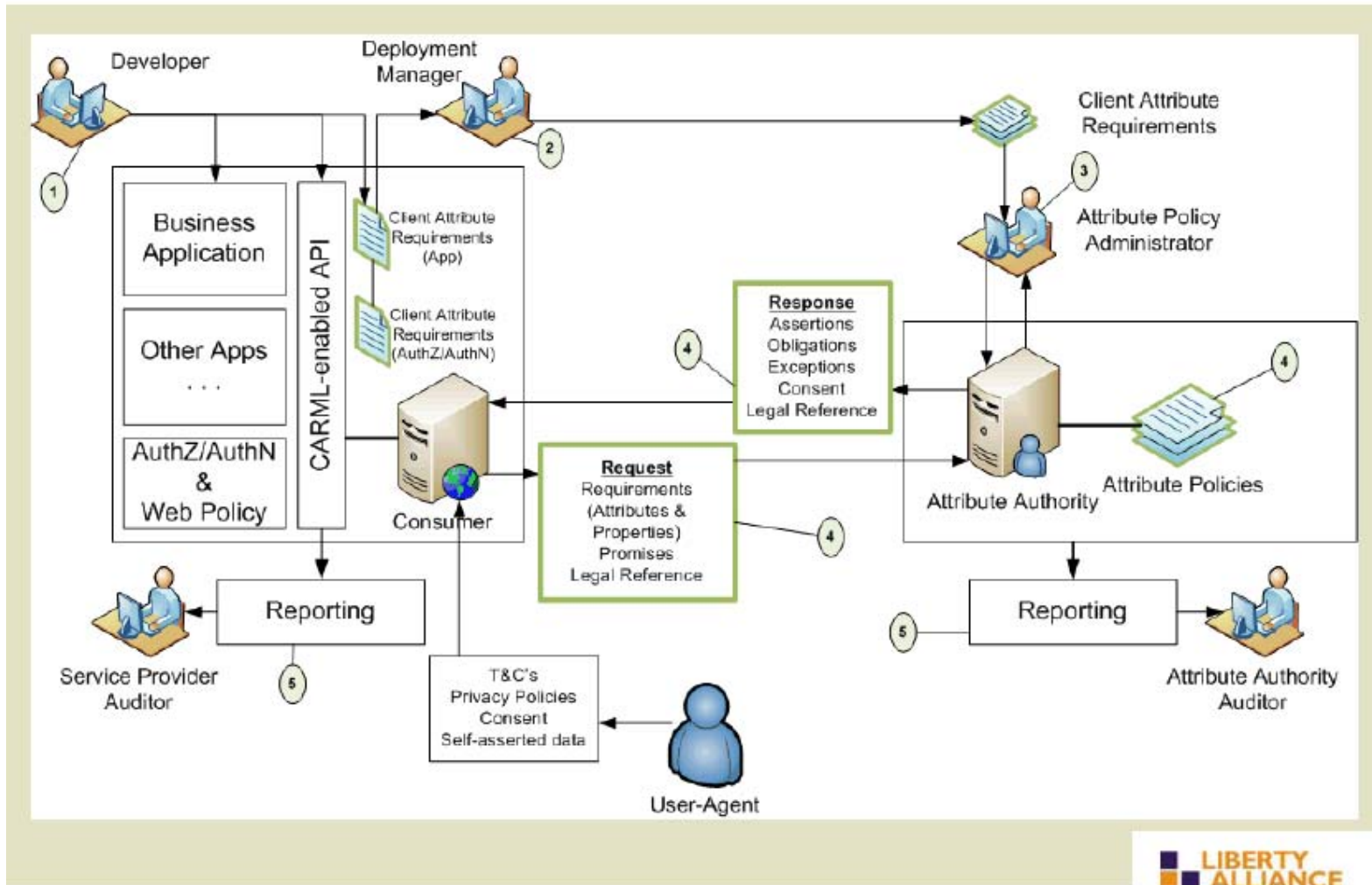
- |                      |   |
|----------------------|---|
| - Prozess-Portal     | Zugang im Berechtigungskontext                    |
| - Prozess-Services   | Koordinations-, Kommunikations- und Portaldienste |
| - Prozess-SLA        | Gesetze, Verträge, Serviceleistungen              |
| - Prozess-Monitoring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

## IAM-IT-Architektur = SOA





## Use Case aus Liberty Alliance, IGF





## Nächste Schritte und Ausblick

- Zusammenarbeit mit eGov-Geschäftsstelle und eHealth-Koordinationsstelle institutionalisieren
- Kontakt mit Projekt-Schlüsselpersonen von Key-Projekten vertiefen und Ansätze zu Best Practice und Standards weiter verifizieren
- Koordination und Konsolidierung mit anderen eCH-Standards
- Weiter im Einklang mit internationalen Standards bewegen



## IAM Roadmap

- März 08: Koordination mit Geschäftsstelle eGovernment im ISB und deren Umsetzungsorganisation „Vorhaben IAM“, sowie mit der Koordinationsstelle eHealth im BAG
- bis Herbst 08:
  - Best Practice und eCH-Standard als IAM-Prozesse eGov-Geschäftsmodell und Architektur auf Basis SOA erarbeiten und beschreiben (Prozess-Referenzmodell M. Schaffroth/W. Müller)
  - Laufendes Verifizieren der Resultate durch Workshops mit Projektteams laufender Key-eGov/eHealth-Projekte
- Herbst 08: Erarbeitetes in Vernehmlassung geben
- bis Ende 08: Best Practice-Vorgehen durch ein Vorgehens/Maturitätsmodell aufzeigen



**Fragen?**