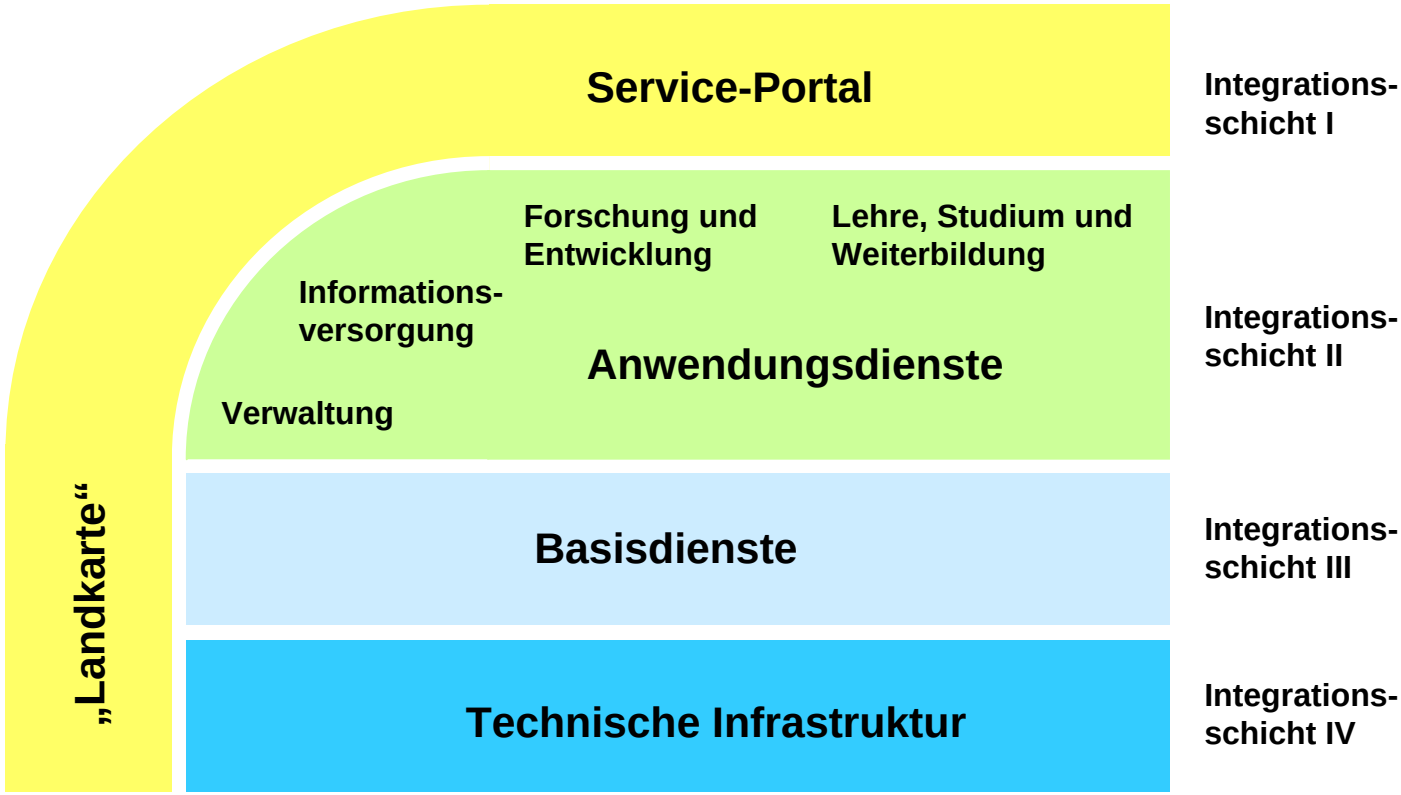
Karlsruhe Institute of Technology

# Sichere Web-Services in einem föderierten Umfeld

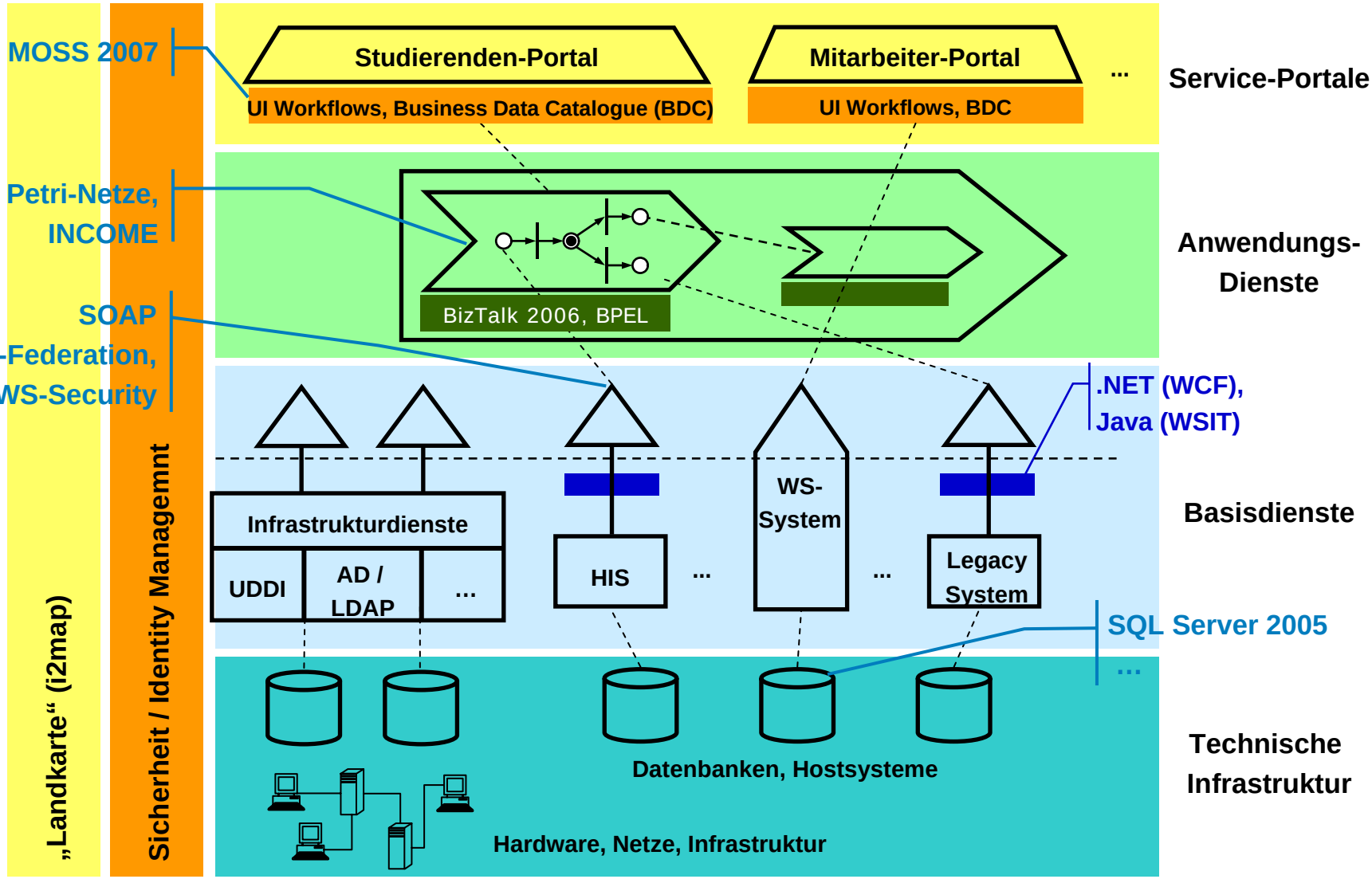
## ZKI Arbeitskreis Verzeichnisdienste – ZEDAT FU Berlin

**Axel Maurer**

# integrierte Service-Orientierte Architektur - iSOA



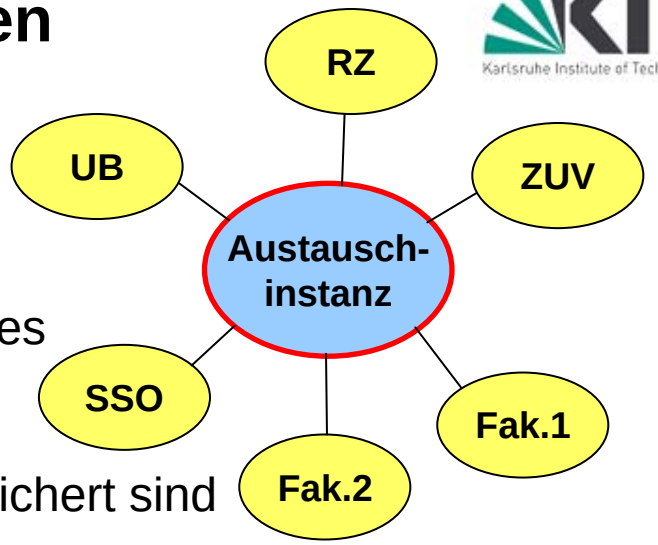
# KIM Architektur - Technologien & Plattformen



# KIM-IDM: Grundprinzipien

- **Einfachheit**
- **Weitestgehende Nutzerkontrolle, -steuerung**
- **Datenschutz im Entwurf**
- **Konzeption, Realisierung und Richtlinienbildung Hand in Hand**

# IDM: Umsetzung der Grundprinzipien



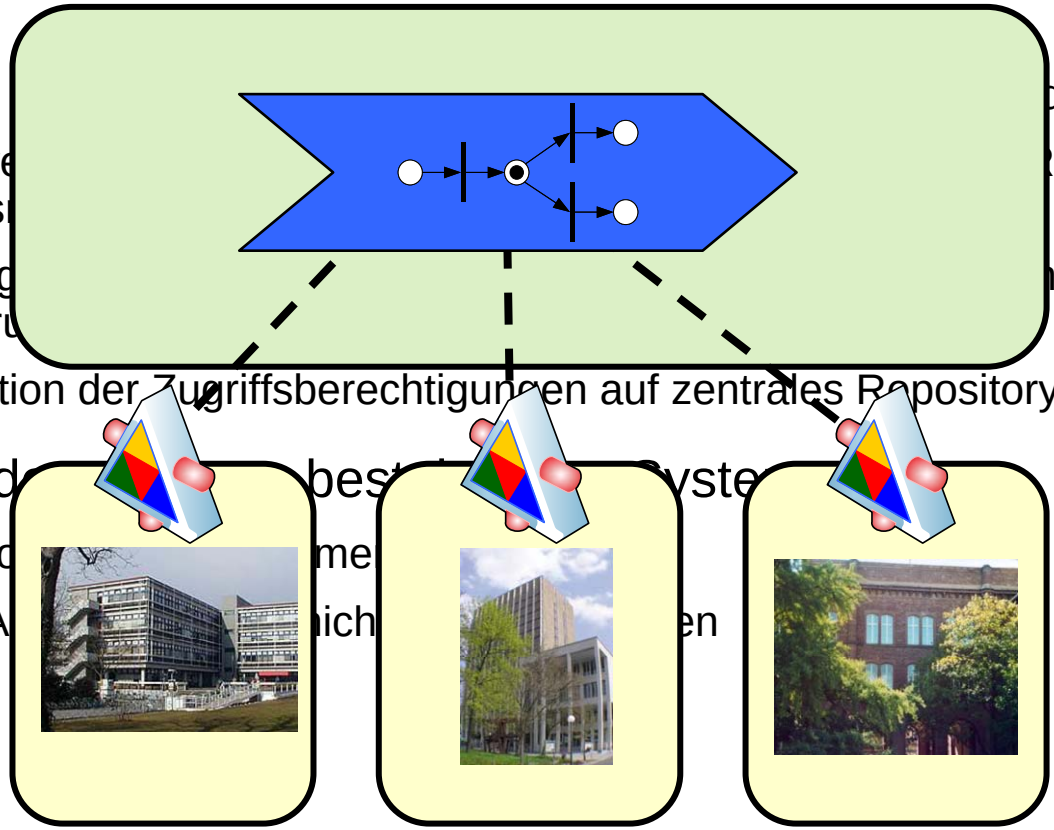

- Einrichtungen der Universität als Satelliten
  - eigenständige Datenhaltung
  - Austausch der Daten nur bei Zustimmung des Einzelnen, bzw. bei gesetzlichen Vorgaben
  - jeglicher Austausch wird dokumentiert: ⇒ mehr Transparenz, wo welche Daten gespeichert sind
- Konsistente Daten über alle Satelliten
  - kongruente Daten müssen synchronisiert werden
  - nicht kongruente Daten werden in den Satelliten gepflegt
- Authentifikation
  - SSO über alle Satelliten hinweg (steuerbar durch Benutzer)
- Datenschutz
  - Grundsatz der Datensparsamkeit (§4 LDSG)
  - Zugriff nur auf die der Berechtigung unterliegenden Daten (§9 LDSG Abs.3)
  - Selbstbestimmungsrecht (§5 LDSG)
  - Zweckbindung (§15 LDSG)

# Dienstorientiertes Identitätsmanagement

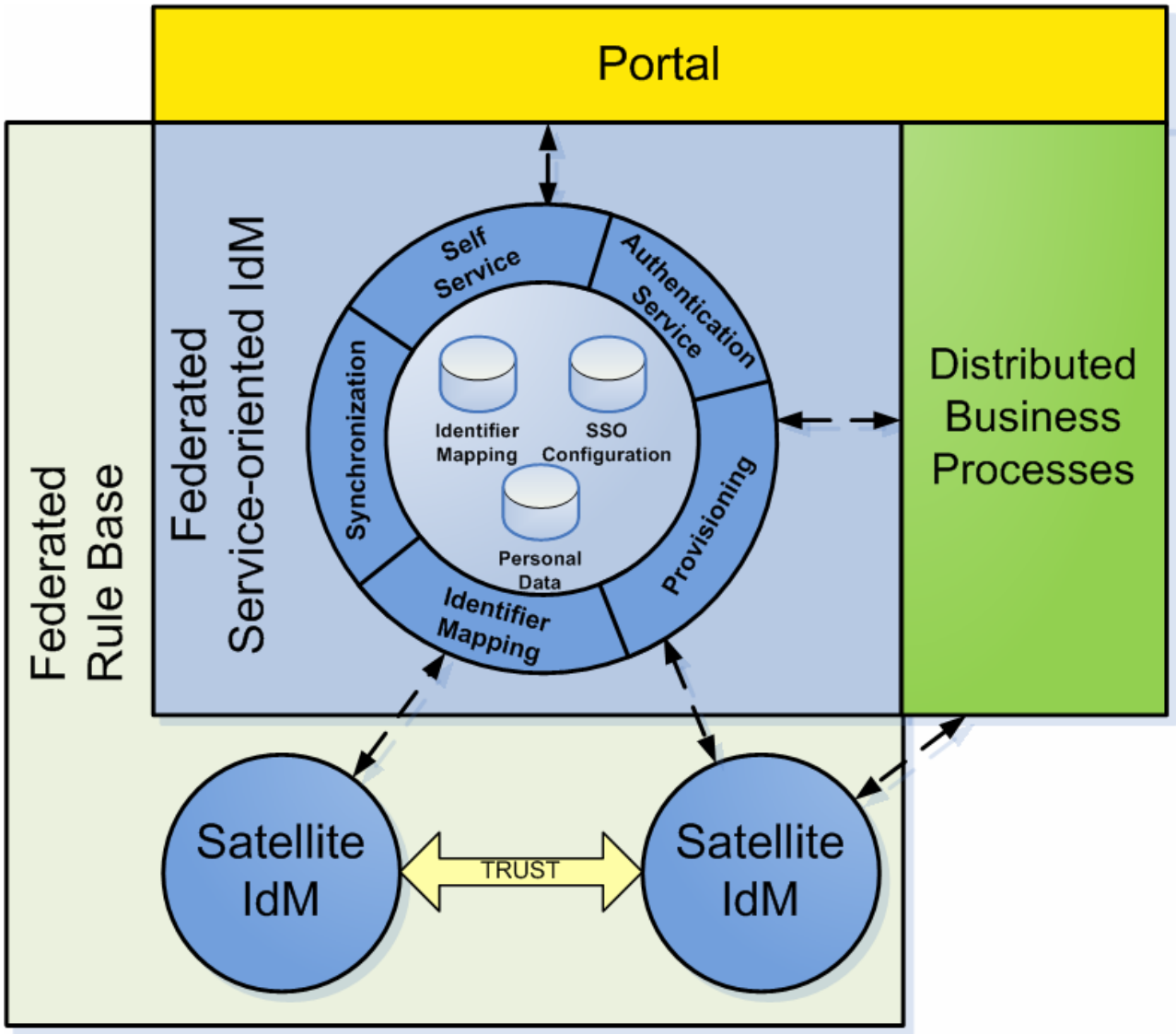
- Was ist dienstorientiertes Identitätsmanagement?

  „Ein dienstorientiertes Identitätsmanagement stellt Anwendungen identitätsbezogene Daten und Dienste über dezentrale Dienstschnittstellen zur Verfügung.“

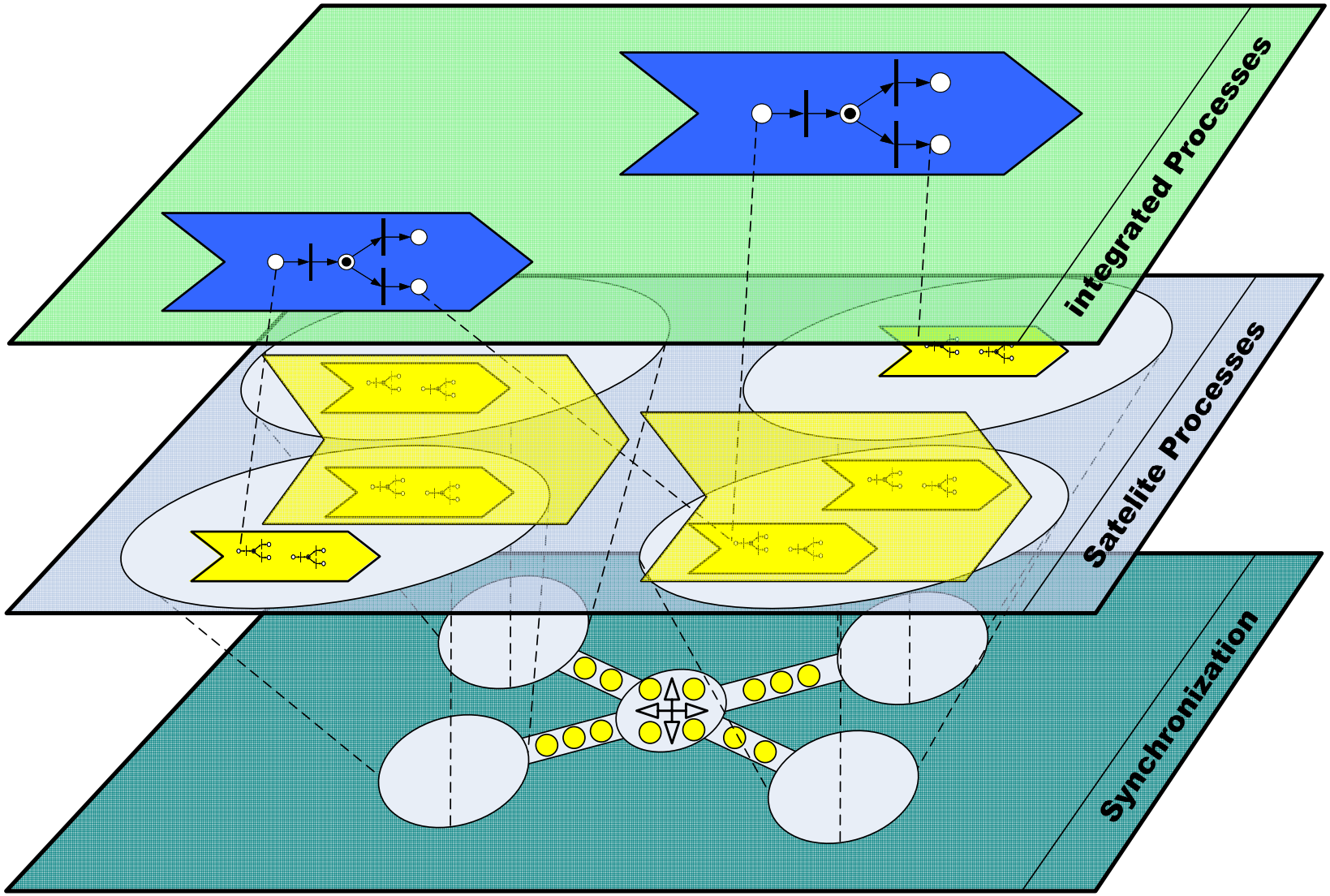
- Grundzüge
  - Daten bleiben
  - Universitätswe
    über Identitäts
  - Durch Nutzung
    Verzeichnisstru
  - Keine Replikation der Zugriffsberechtigungen auf zentrales Repository notwendig
- Minimale Änd
  - Fortbestand vo
  - Existierende A



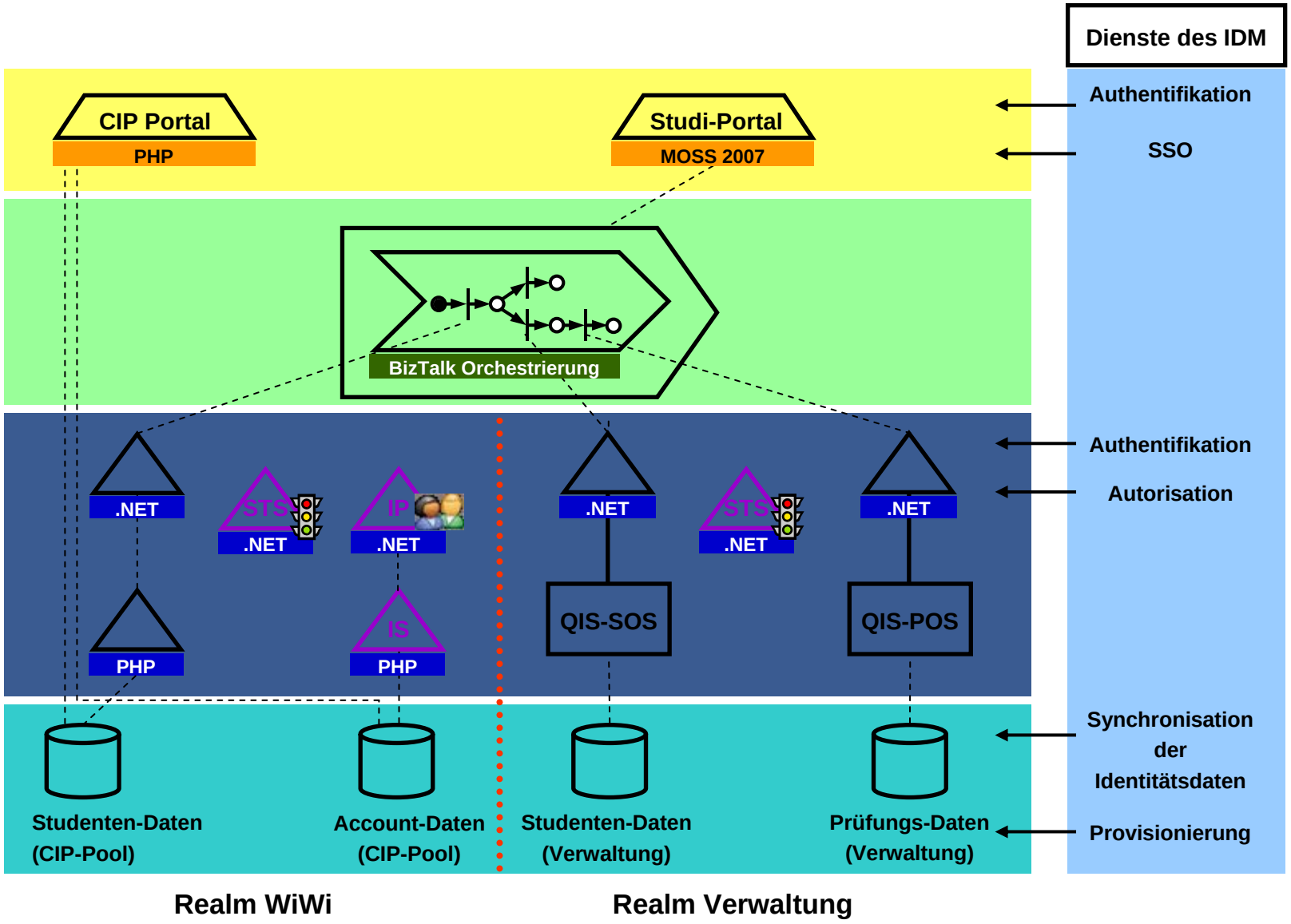
# Überblick KIM-IDM Konzept



# Architektur

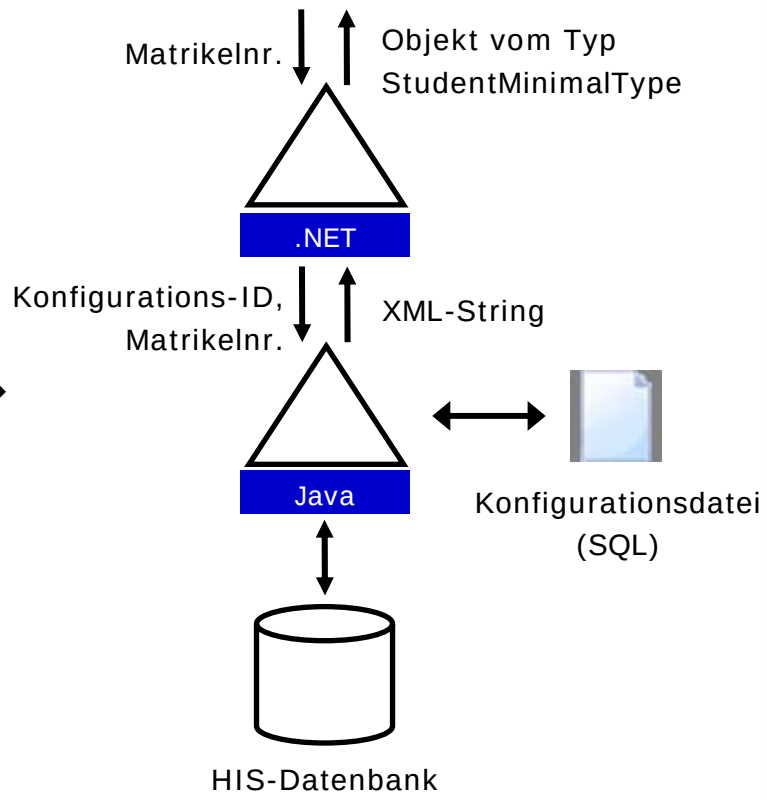


# Einordnung Identitätsmanagement in KIM

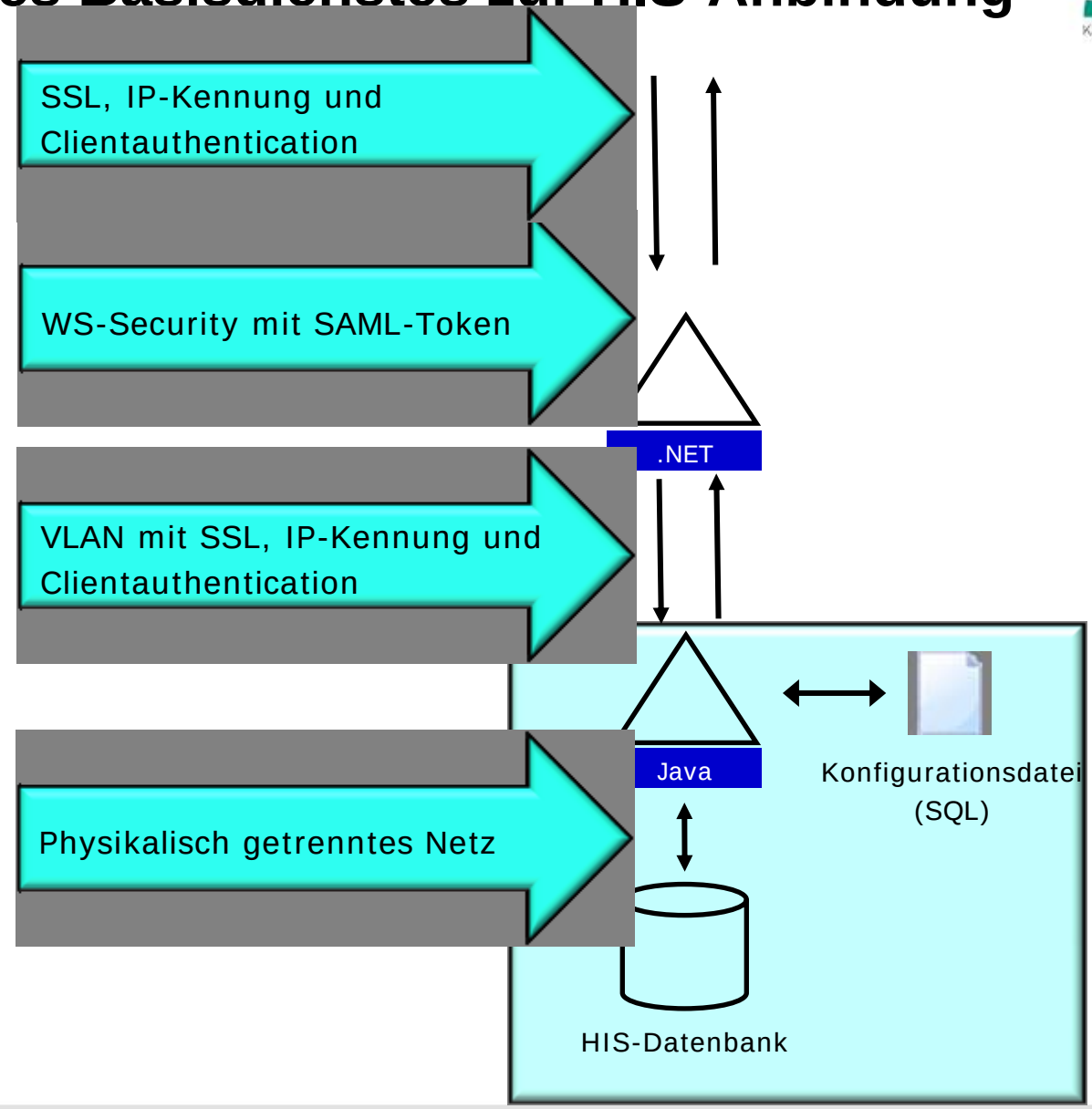


# Basisdienst zur HIS-Anbindung

- Daten sind über SOAP Schnittstelle des XML Publishing Moduls von HIS abfragbar
- .NET Wrapper Web Service ist für Datentransformation und Kapselung der Sicherheit zuständig
- Nächstes Ziel: HIS Web Service(s) liefern korrektes Schema und integrieren Sicherheit → .NET Wrapper entfällt

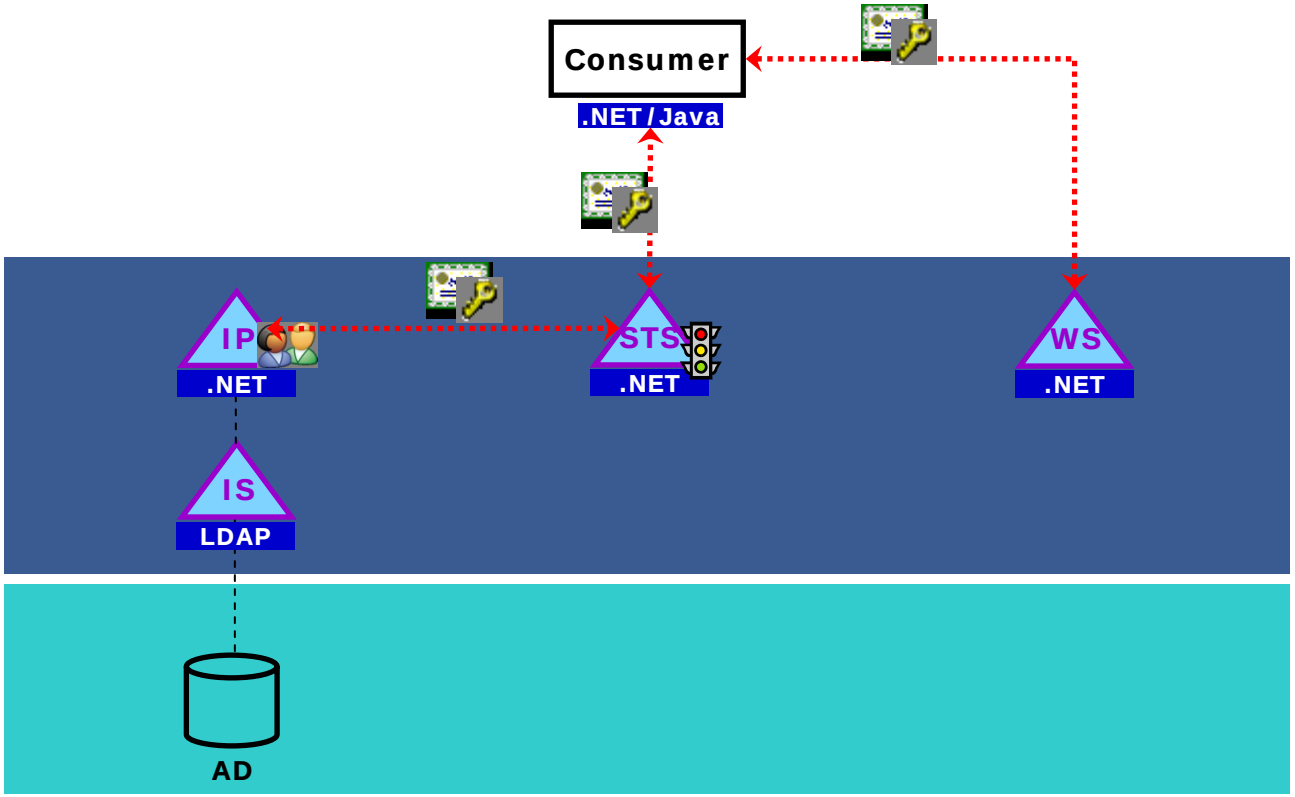


# Sicherung des Basisdienstes zur HIS-Anbindung



# Szenario WS Sicherung

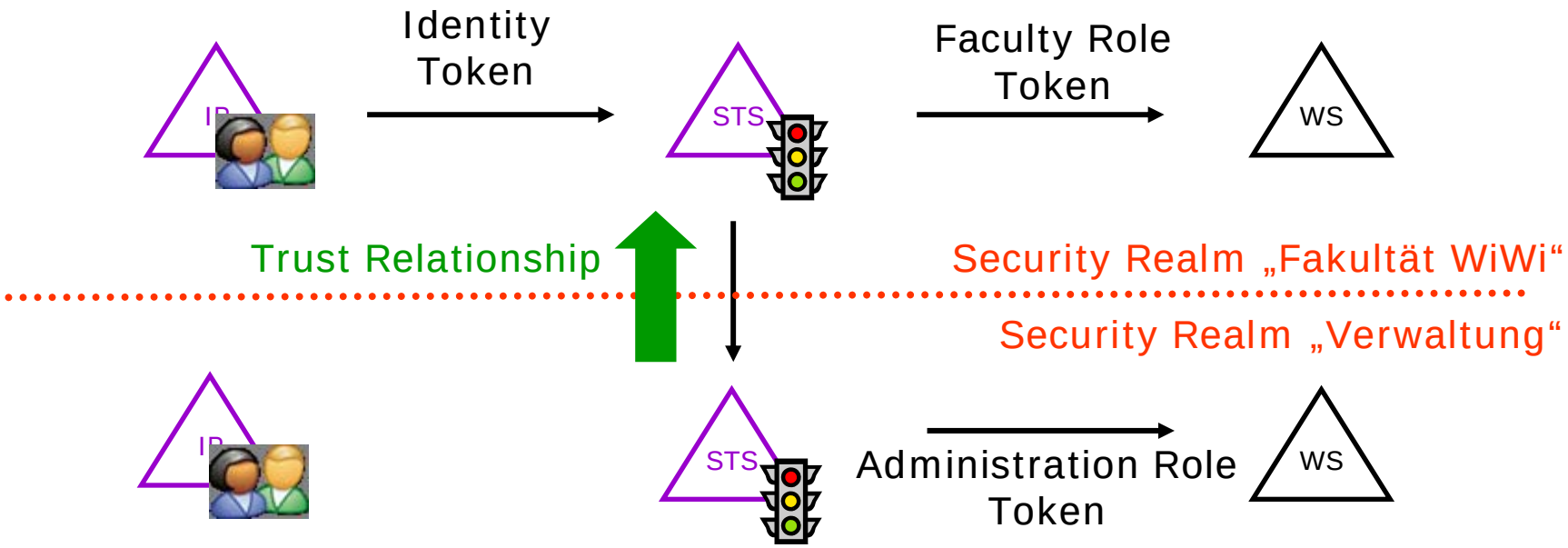
- Absicherung eines Basisdienstes innerhalb eines Security Realms
  - Für den Aufruf aus einem generischen Client: Teil des Active Requestor Profiles aus WS-Federation Spezifikation wird umgesetzt



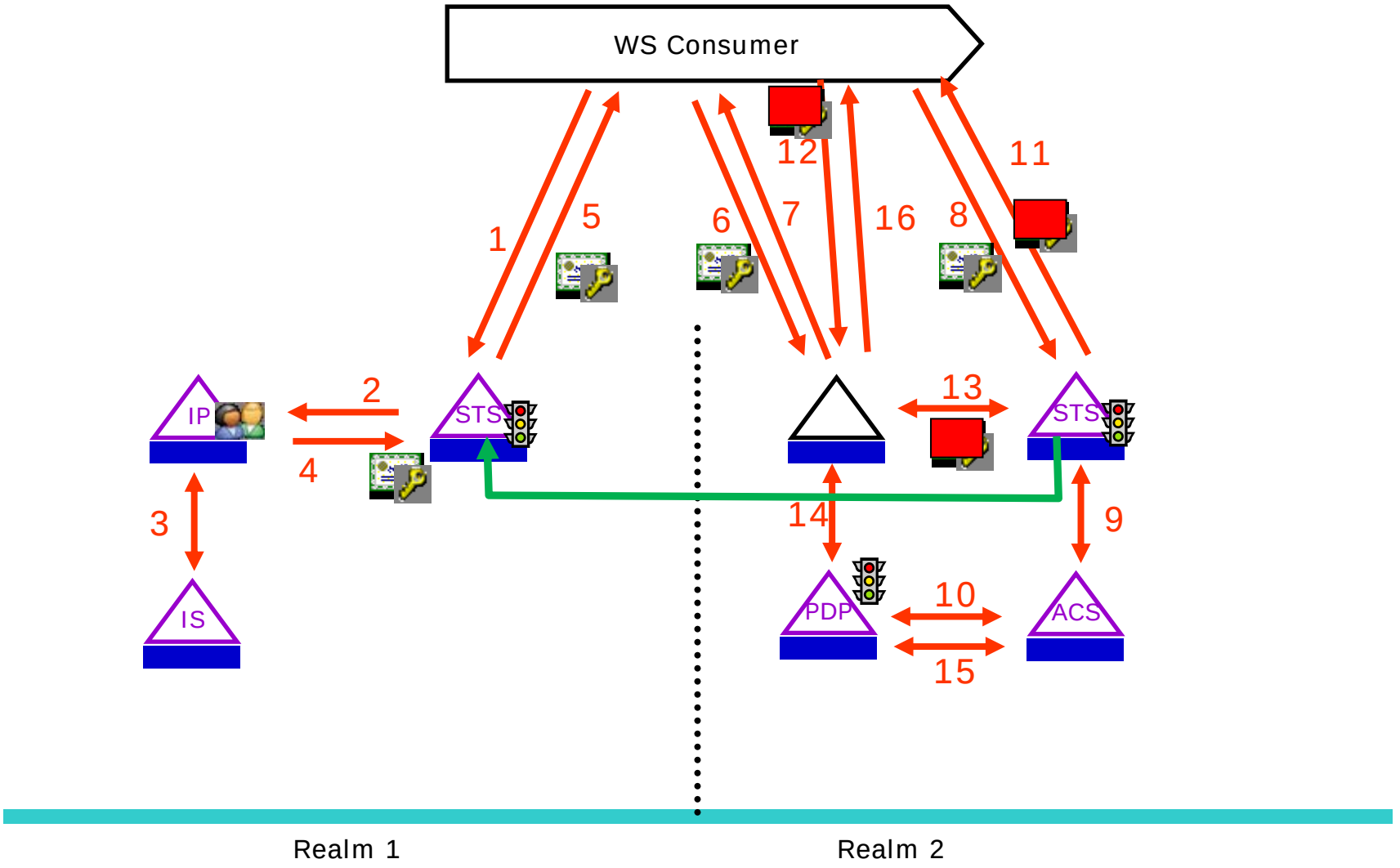
# Probleme des derzeitigen Verfahrens im föderierten Umfeld

- Clientzertifikate müssen bei jedem Consumer gepflegt werden
- IP-Adressänderungen sowohl auf Seiten der Consumer als auch der Provider müssen gepflegt werden
- Keine Unterstützung eines föderierten Umfeldes, d.h. alle Benutzer müssen lokal vorhanden sein und gepflegt werden
- Keine Kenntnis über die den Service nutzende Person, da in der Regel mit Consumer-bezogenen Accounts gearbeitet wird
- Keine nachhaltige Prüfung der Service-Consumer

# Security Concept



# Föderation – Szenario



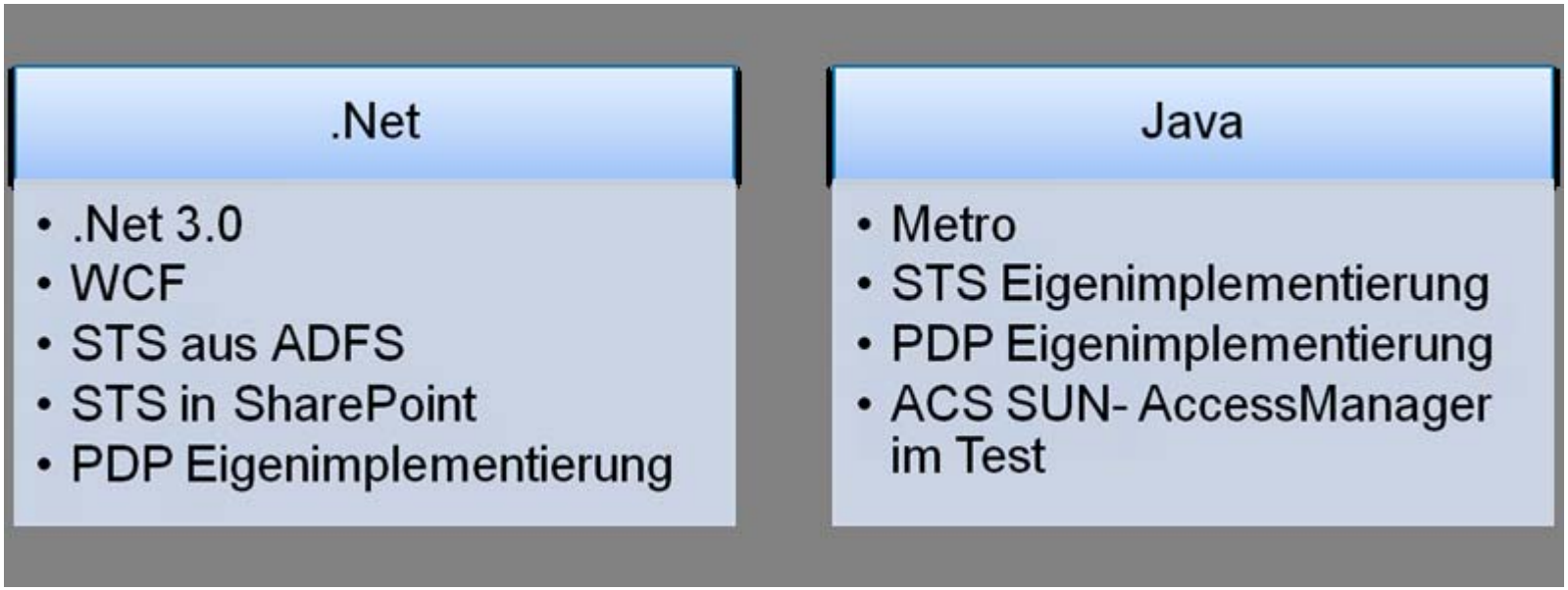



KIM

Universität Karlsruhe (TH)
Forschungsuniversität • gegründet 1825

# Implementierungsumfeld

- Realisiert in Java und .Net




- Anforderungen an Consumerservice:
  1. Implementierung von WS-Security
  2. Implementierung von WS-SecurityPolicy alternativ die Konfiguration der Adresse des Partner-STS

# Vorteile des neuen Verfahrens im föderierten Umfeld

- Zertifikatsaustausch über WS-Trust
- Offener SSL-Zugang
- Authentifizierungsinformation direkt vom vertrauten STS in der Regel angebunden an das IDM
- Aktuelle Informationen aus dem IDM des Partners
- Direkte konfigurierbare Autorisierungsinformation

# Vielen Dank
# für Ihre Aufmerksamkeit!