V26

Anforderungen an Zertifikate und Rechtemanagement

Göttingen, 28.03.2007

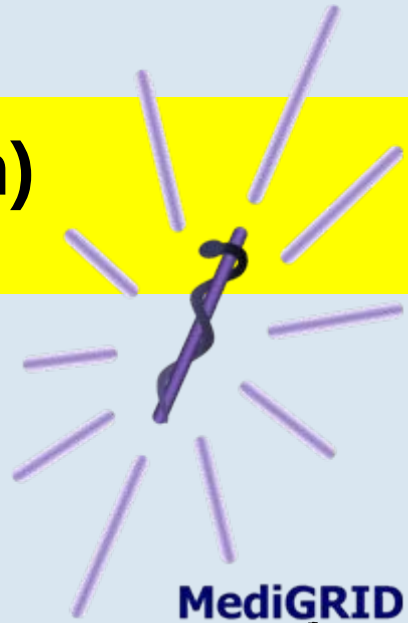
Ulrich Sax

MediGRID

Bundesministerium
für Bildung
und Forschung

Anforderungen an Zertifikate und Rechtemanagement

1. Zertifikate (im Gesundheitswesen)
2. Feingranulare Zugriffsrechte
3. Ausblick



Gewährleistung der Vertraulichkeit

- Integrität und Authentizität von patientenbezogenen Daten bedarf elektronischer Signaturverfahren
- Es wird unterschieden zwischen
  - ➜ **Einfachen, fortgeschrittenen, qualifizierten und akkreditierten Signaturen.**
- Im Signaturgesetz sind nur qualifizierte elektronische Signaturen ausgeführt bezüglich technischer und organisatorischer Rahmenbedingungen.
- Nur qualifizierte und akkreditierte elektronische Signaturen sind der handschriftlichen Unterschrift weitestgehend gleichgestellt.
- Integrität und Authentizität der Daten muss über den gesetzlichen Aufbewahrungszeitraum von 30 Jahren (BGB §199) gewährleistet sein (Problem: Verlust an Beweiswert)

Authentication Policy Guidelines

- Wherever possible
  - No more than one CA per country
  - Aim for widest possible cover
- PMA does not provide identity assertions
  - Certificates issued meet or exceed the guidelines
- Identity for Grid/eScience Authentication *only*
  - No support of data encryption or non-repudiation
  - No support for financial transactions
  - No liability!

Prüfverfahren für eGK und HBA

PKI im Gesundheitswesen

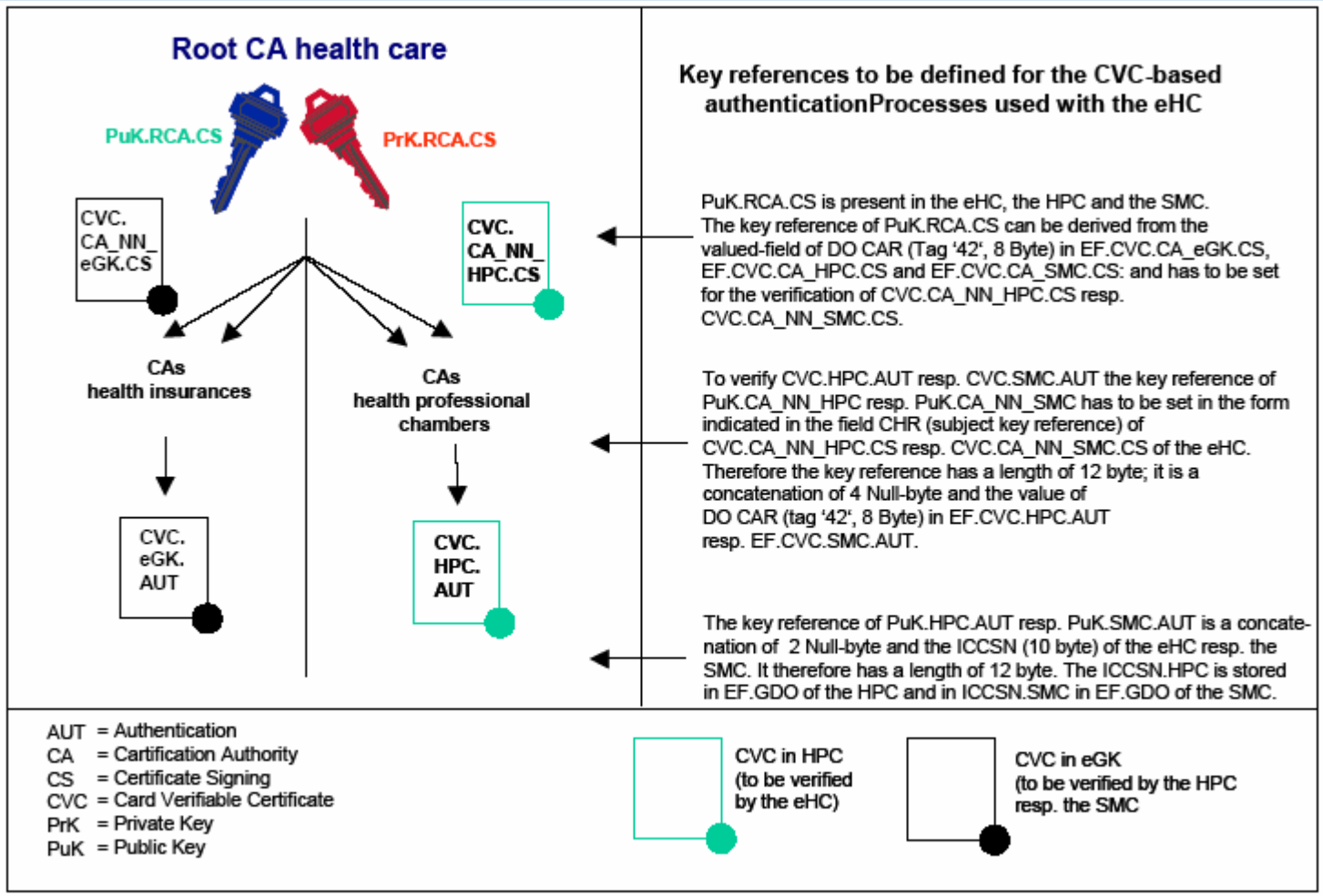
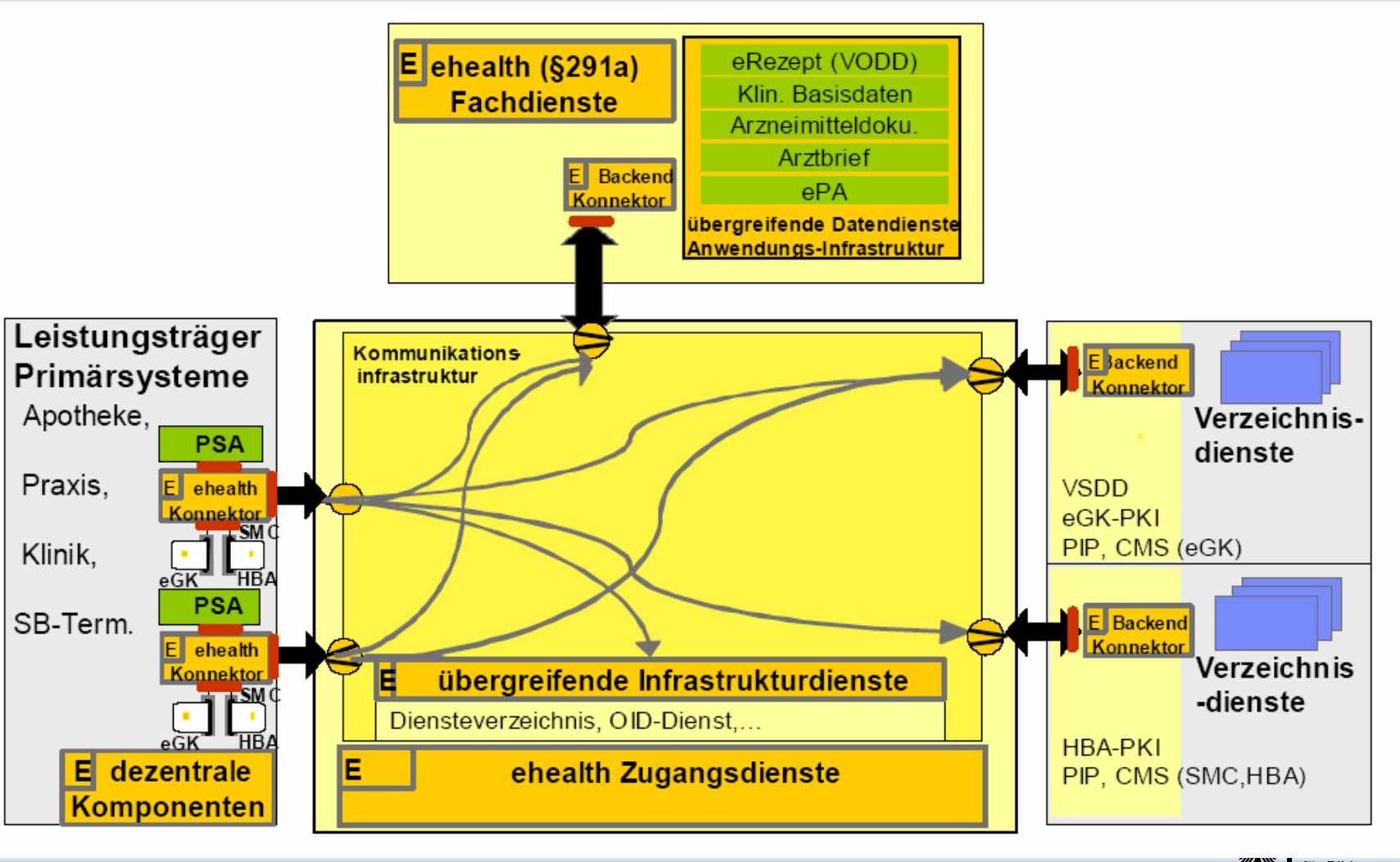


Figure 4 - Verification of CV-Certificates

Quelle: http://www.bmg.bund.de/nn_667298/SharedDocs/Gesetzestexte/Gesundheitskarte/spec-engl-part2,templateId=raw,property=publicationFile.pdf/spec-engl-part2.pdf

Komponenten der Telematikinfrastruktur



Quelle: http://www.gematik.de/download-spezifikationen.aspx

Zertifikate im deutschen Gesundheitswesen

Heute: flächendeckende PKI im Gesundheitswesen wird aufgebaut

- ➜ Einführung der elektronischen Heilberufeausweise und der elektronischen Gesundheitskarte (www.gematik.de) auf Niveau qualifizierter / akkreditierter Zertifikate **verzögert sich**

Voraussetzungen für **Phase I**:

- ➜ Grundlegende Infrastruktur (AAI)
- ➜ Audit trails (!)
- ➜ Beobachtung der HBA und eGK-Projekte im Hinblick auf Phase II

Voraussetzungen für **Phase II**:

- ➜ Feingranlulare Zugriffsrechte
- ➜ **ggf**. Integration der HBA und eGK-Infrastruktur **nach Vorliegen**
- ➜ Berücksichtigung andere PKI-Projekte (eCard Österreich etc.)

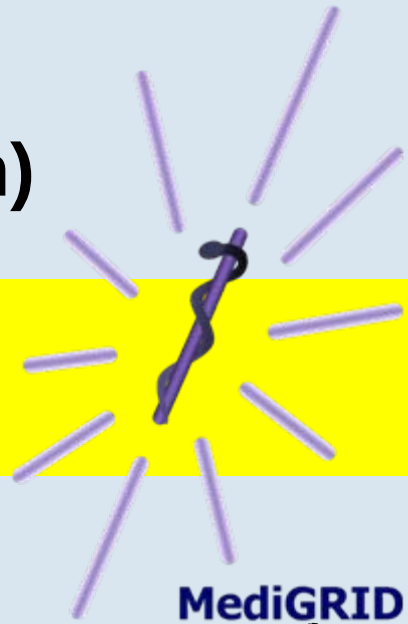
Voraussetzungen für **Phase II**: Trackability

Anforderungen an Zertifikate und Rechtemanagement

1. Zertifikate (im Gesundheitswesen)

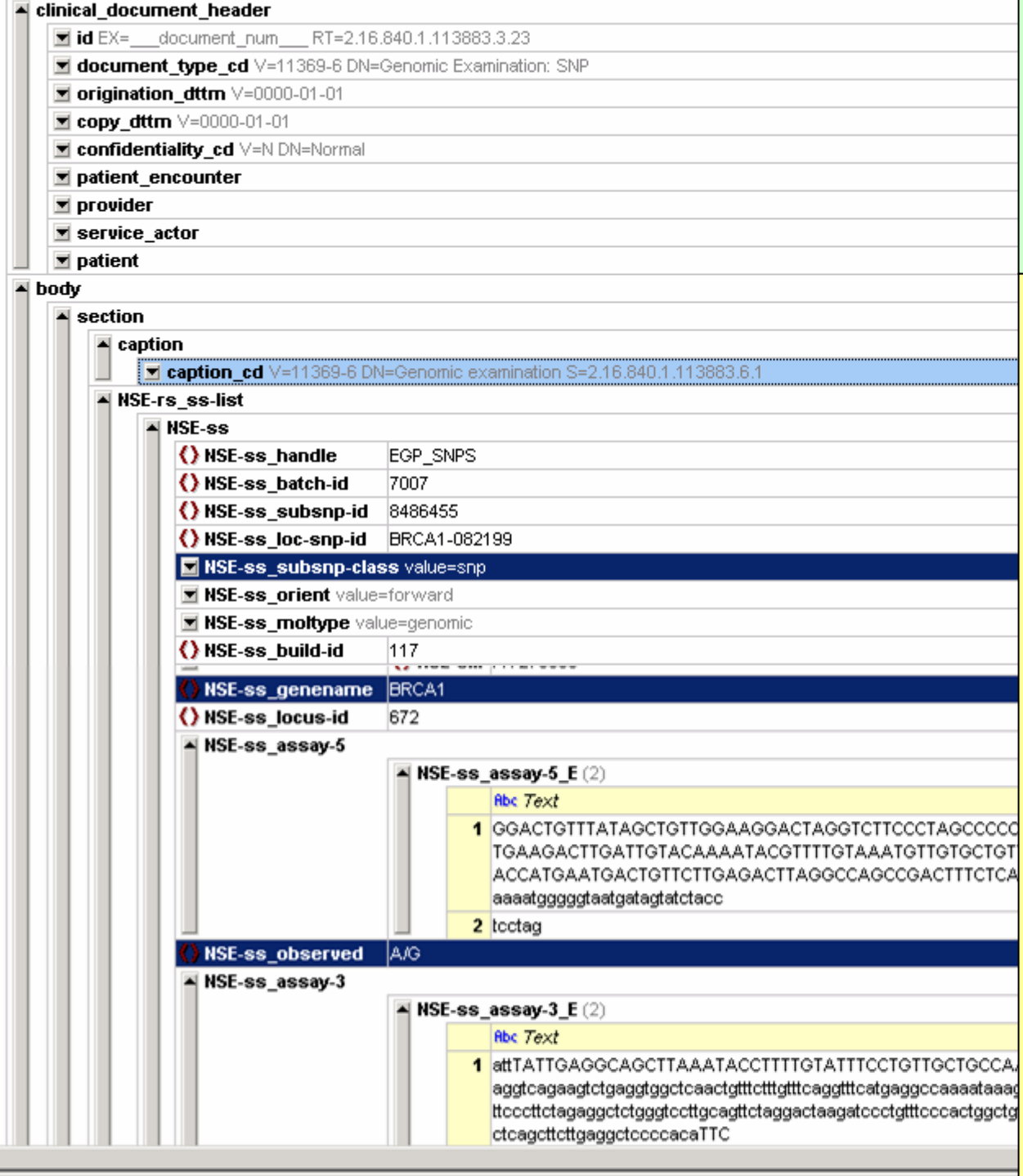
2. Feingranulare Zugriffsrechte

3. Ausblick



„Enhanced Security“ AP InGrid/MediGRID/DGI

- Audit: a posteriori Logs. Data provenance und data annotation (Prozessschritte).
- Trackability: a priori Kenntnisse bzw. Richtlinien wo Datentransport, Transaktionen, Berechnungen und Speicherung von personen- bzw. patientenbezogenen Daten stattfinden.
- feingranulare Zugriffsrechte: Zugriffsrechte und Zugriffskontrolle sollen nicht nur auf Fileebene erfolgen, sondern auch innerhalb eines Formulars bzw. Datensatzes.
- Vertraulichkeit: parallel den Anforderungen bei den Zugriffsrechten muss auch Vertraulichkeit entsprechend feingranular erfolgen können.
- Trust und Trust Delegation: nicht nur für Software-Instanzen, sondern auch auf Ebene von Personen und Organisationen ist erforderlich.
- Safety: Physikalische Absicherung von Daten in Grid-Umgebungen und dynamischen Grid-Umgebungen (Policy-basad storage, Querbezug zu Daten- und Informationsmanagement)



Header

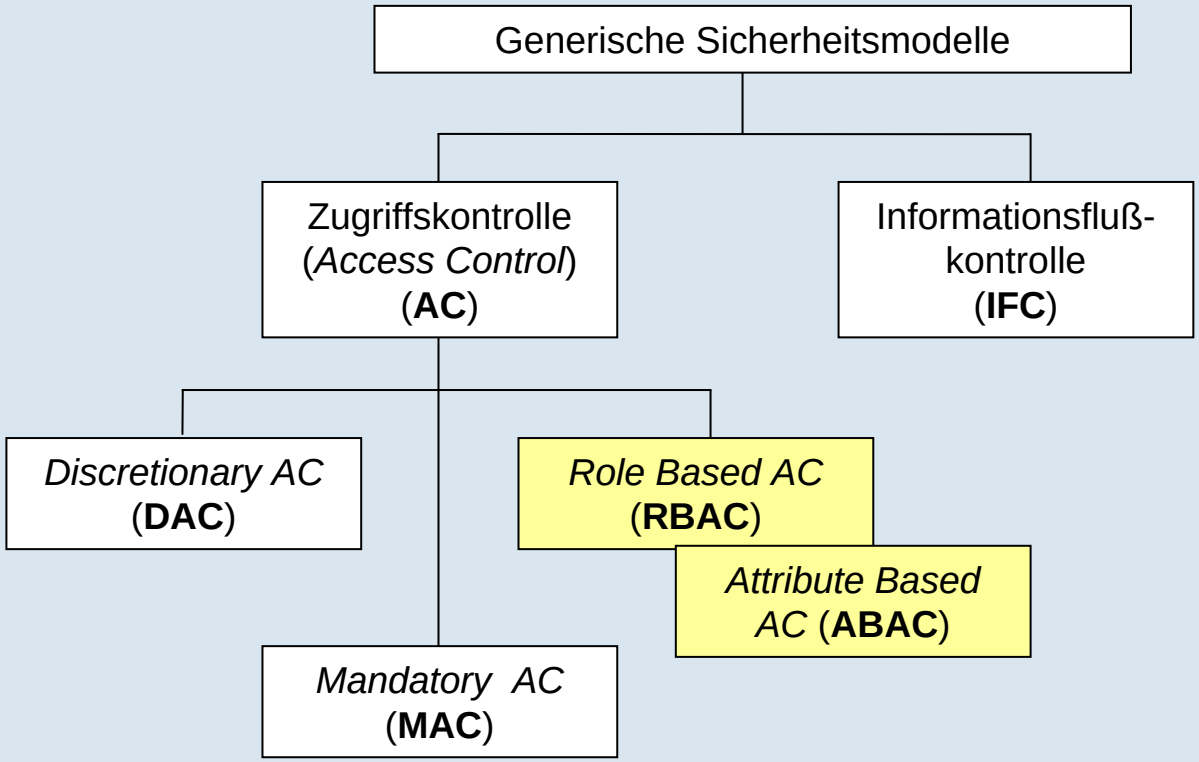
Body

SNP Test Beschreibung

Sequenzinformation

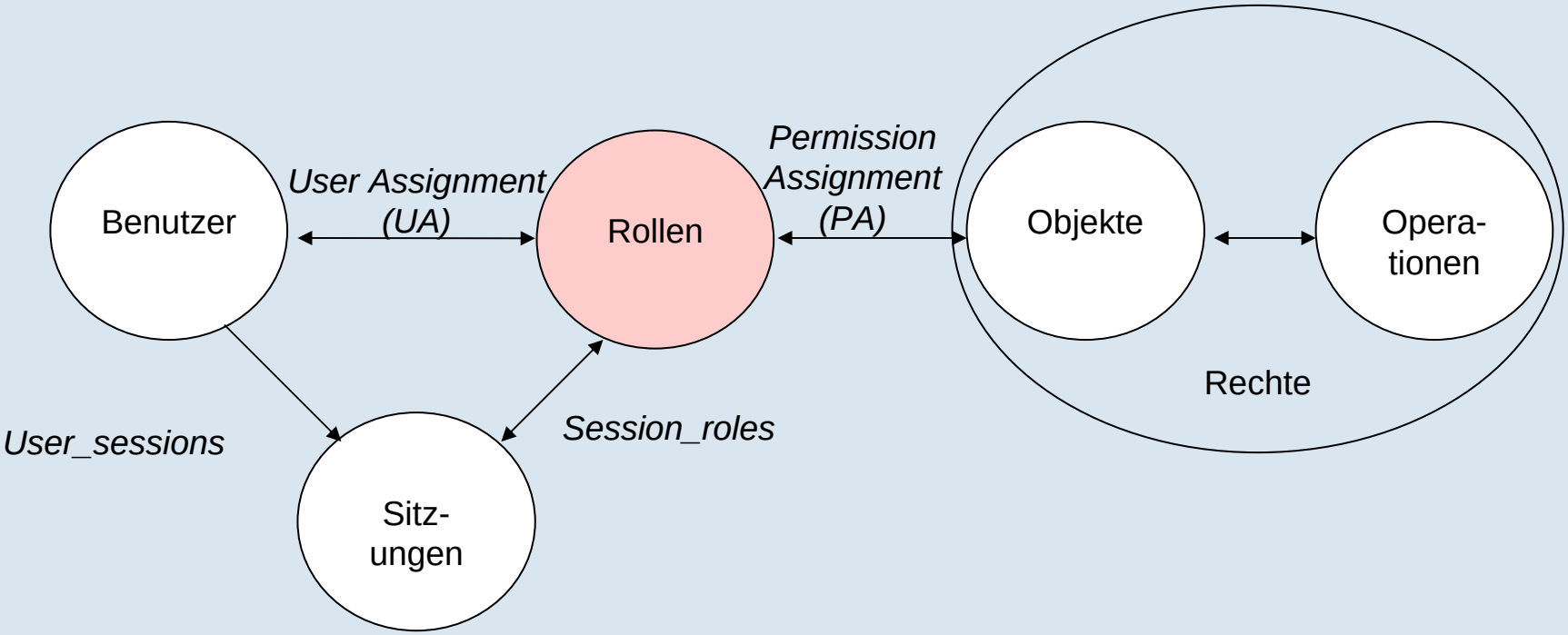
Interpretation

Architektur einer applikations-übergreifenden Berechtigungsverwaltung



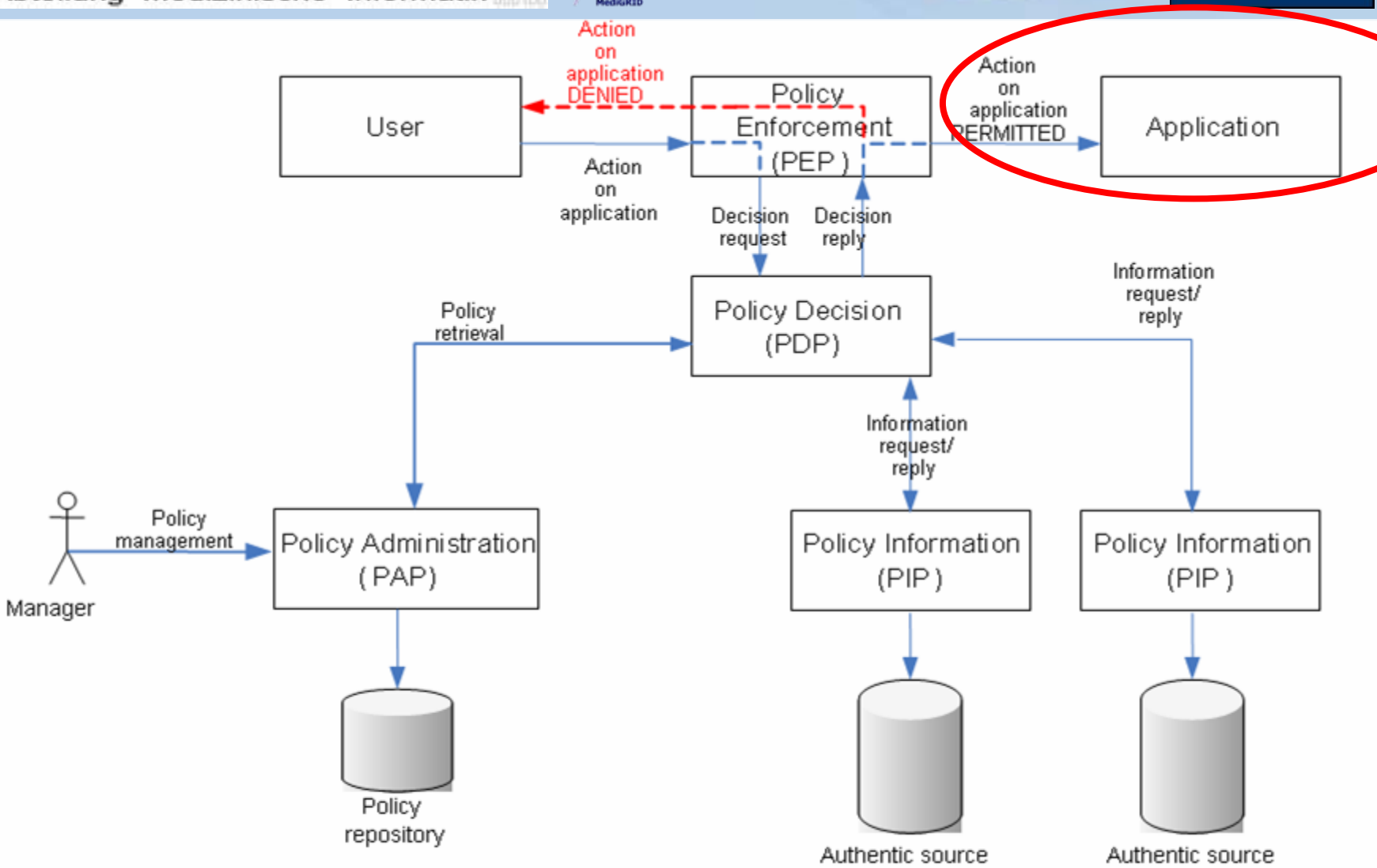
Architektur einer applikationsübergreifenden Berechtigungsverwaltung

Role Based Access Control (RBAC)



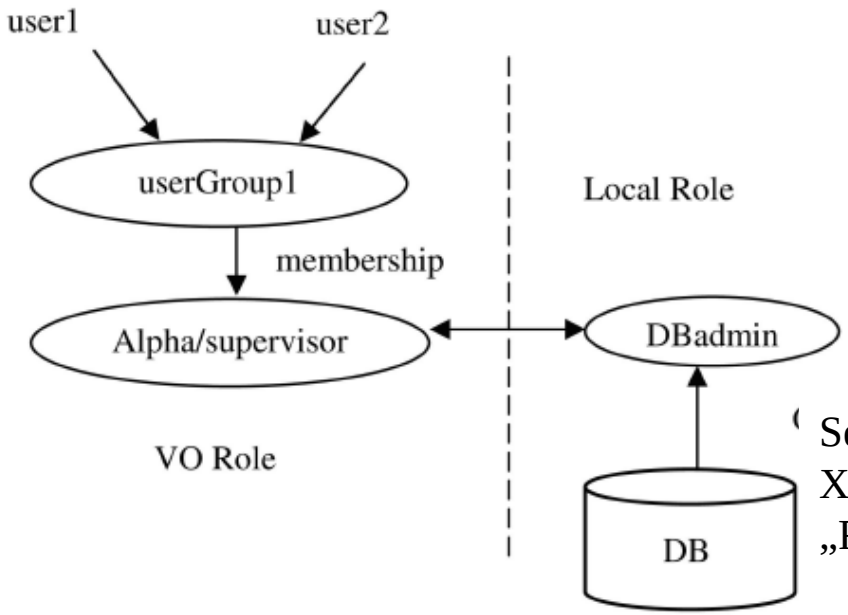
Quelle: [Sandhu 1996]

Policy enforcment model



Role Mapping

Public key authorization and delegation mechanisms provided by the Grid Security Infrastructure (GSI)



Select „**Procedure**“ from XML_Referral_Letter where „Referrer=„XYZ“

Fig. 3. Specifying VO roles using CAS.

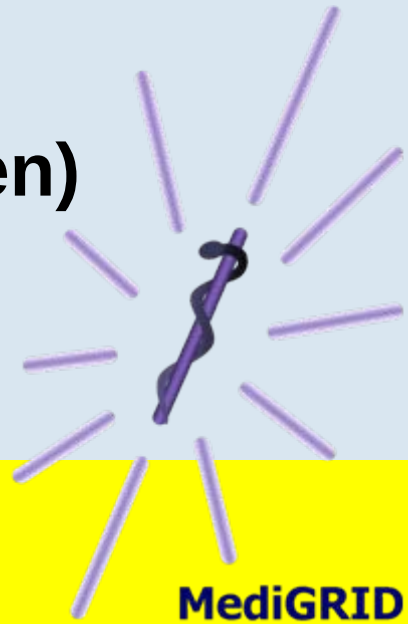
Quelle: Pereira et al IEEE Dependable and Secure Computing 2006

Anforderungen an Zertifikate und Rechtemanagement

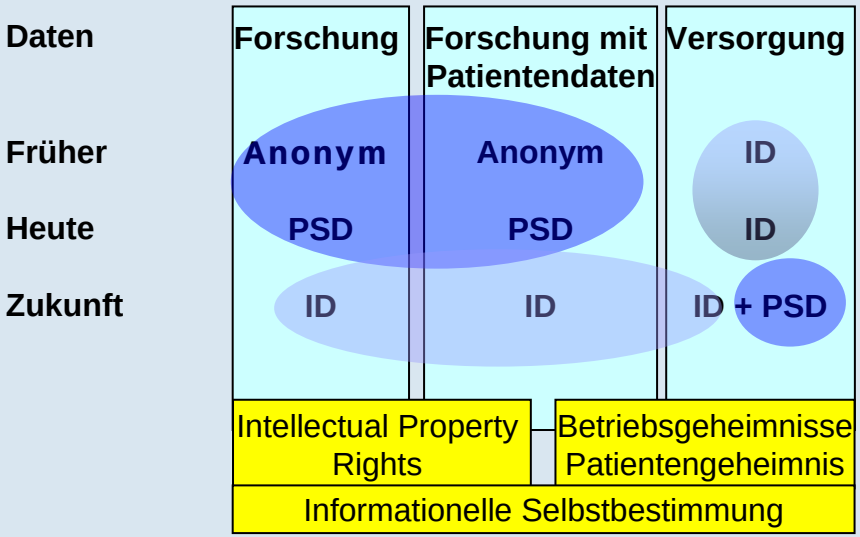
1. Zertifikate (im Gesundheitswesen)

2. Feingranulare Zugriffsrechte

3. Ausblick



Ausblick: Enhanced Security



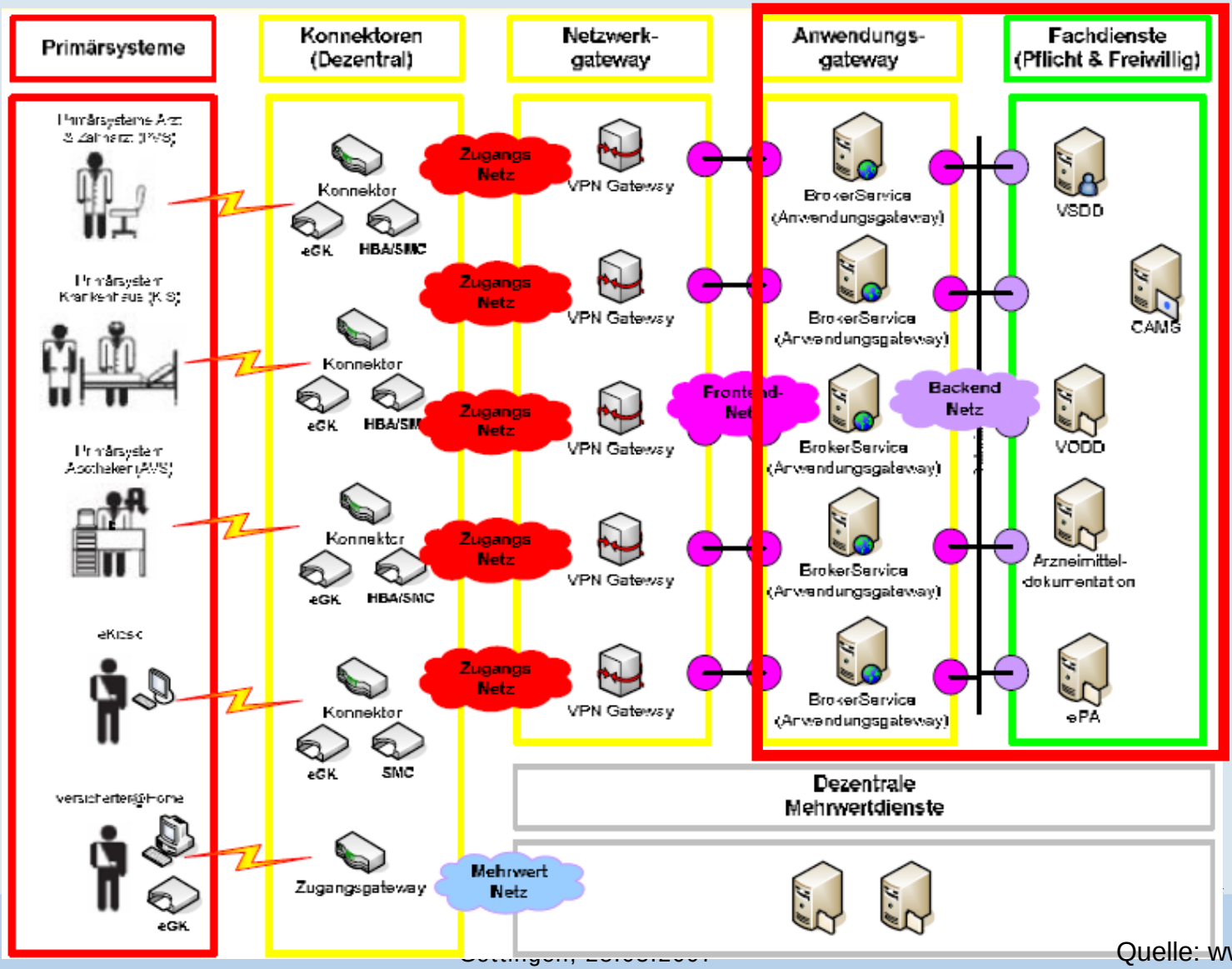
ID: identifizierende Daten

PSD: pseudonymisierte Daten

Very Enhanced Security

- **z.B. Splitting von Datensätzen in nicht identifizierbare Teilstücke**
- **Technische Realisierung in vorhandene Grid-Technologien (Global Grid Forum GGF) angepasst werden**
- **Weiterentwicklung der generischen Datenschutzkonzepte für schwer de-identifizierbare Datenätze**

Infrastruktur eGK und HBA



Quelle: www.gematik.de

Ausblick auf EHR Grid Services

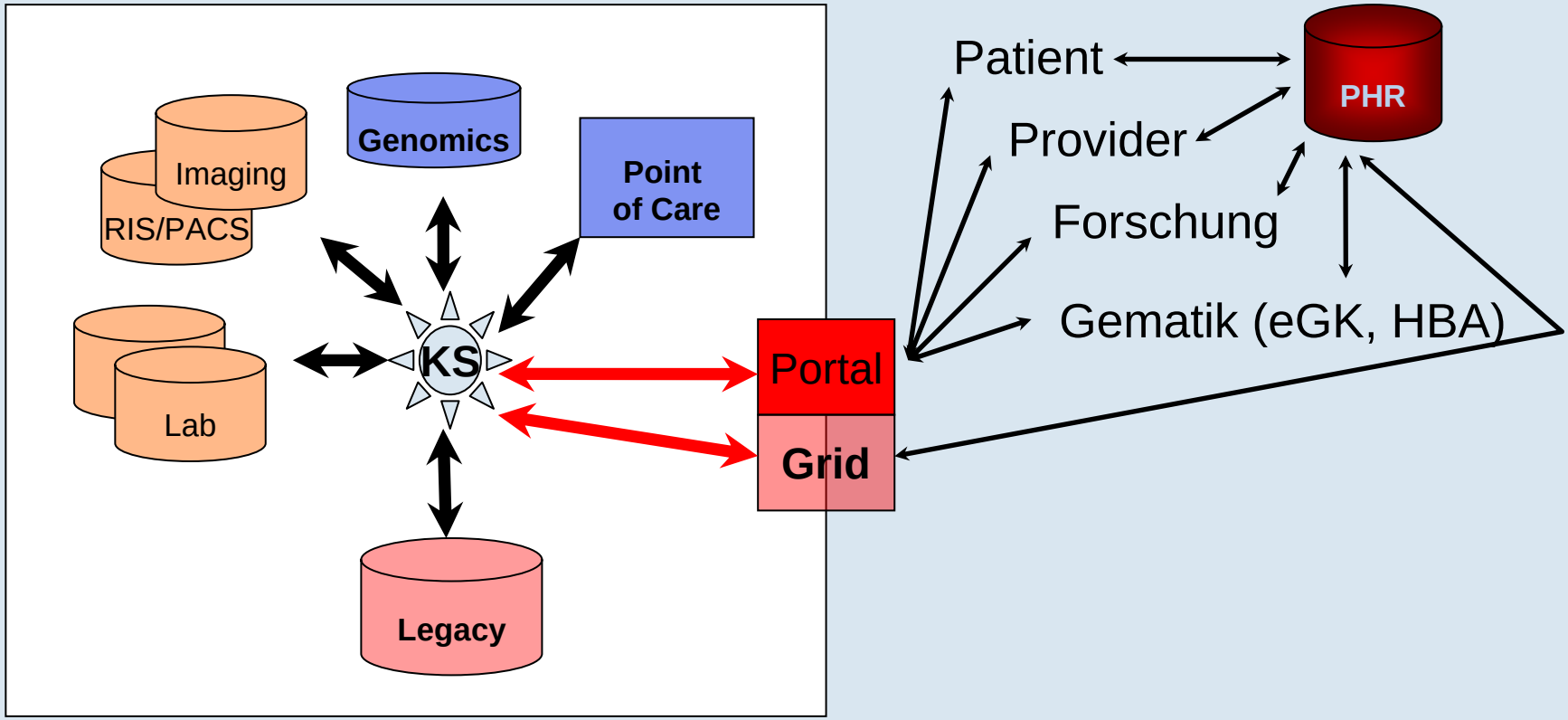
Storage
- ➜ Massendatenverwaltung (Rohdaten)
- ➜ incl. Verschlüsselung und
- ➜ Replikatverwaltung

Retrieval
- ➜ Vergleich mit ähnlichen Fällen
- ➜ Kontrollierte Freigabe für Forschung
- ➜ Kontrollierte Freigabe für Versorgung

Präsentation
- ➜ Rendering, Segmentierung etc. bei Bildverarbeitung
- ➜ Korrelationsmechanismen als Grid-Services

Sicherheit
- ➜ AAI (eGK, HBA), Pseudonymisierung, Verschlüsselung
- ➜ Audit, Tracking

Ausblick: Krankenhaus-IT



Zusammenfassung

Zertifikate

- ➜ In Phase 1: DFN-AAI einsetzbar (fortgeschrittene Z.)
- ➜ In Phase 2+: Übergang zu HBA (qual. Akkr. SigG-Niveau)

Feingranulare Zugriffsrechte

- ➜ Rollen- bzw. Attributbasiert
- ➜ Datenbanken
- ➜ strukturierte Dokumente

Ausblick: EPA Grid Services

- ➜ Storage
- ➜ Retrieval
- ➜ Präsentation
- ➜ Sicherheit

V26

Anforderungen an Zertifikate und Rechtemanagement

Göttingen, 28.03.2007

Ulrich Sax

MediGRID

Bundesministerium
für Bildung
und Forschung