eFA
elektronische FallAkte
Wir verbinden Menschen und Informationen

Pseudonymisierung bei der elektronischen Fallakte

15. Dezember 2008
TMF-Workshop »ID-Management«

Initiative »elektronische Fallakte«

Zielstellung

- Etablierung einer interoperablen Lösung für den effizienten, einrichtungs- und sektorübergreifenden Austausch von medizinischen Daten
  - medizinisch-fachliche Szenarien
  - (datenschutz-)rechtlicher Rahmen
  - technische Lösungskomponenten

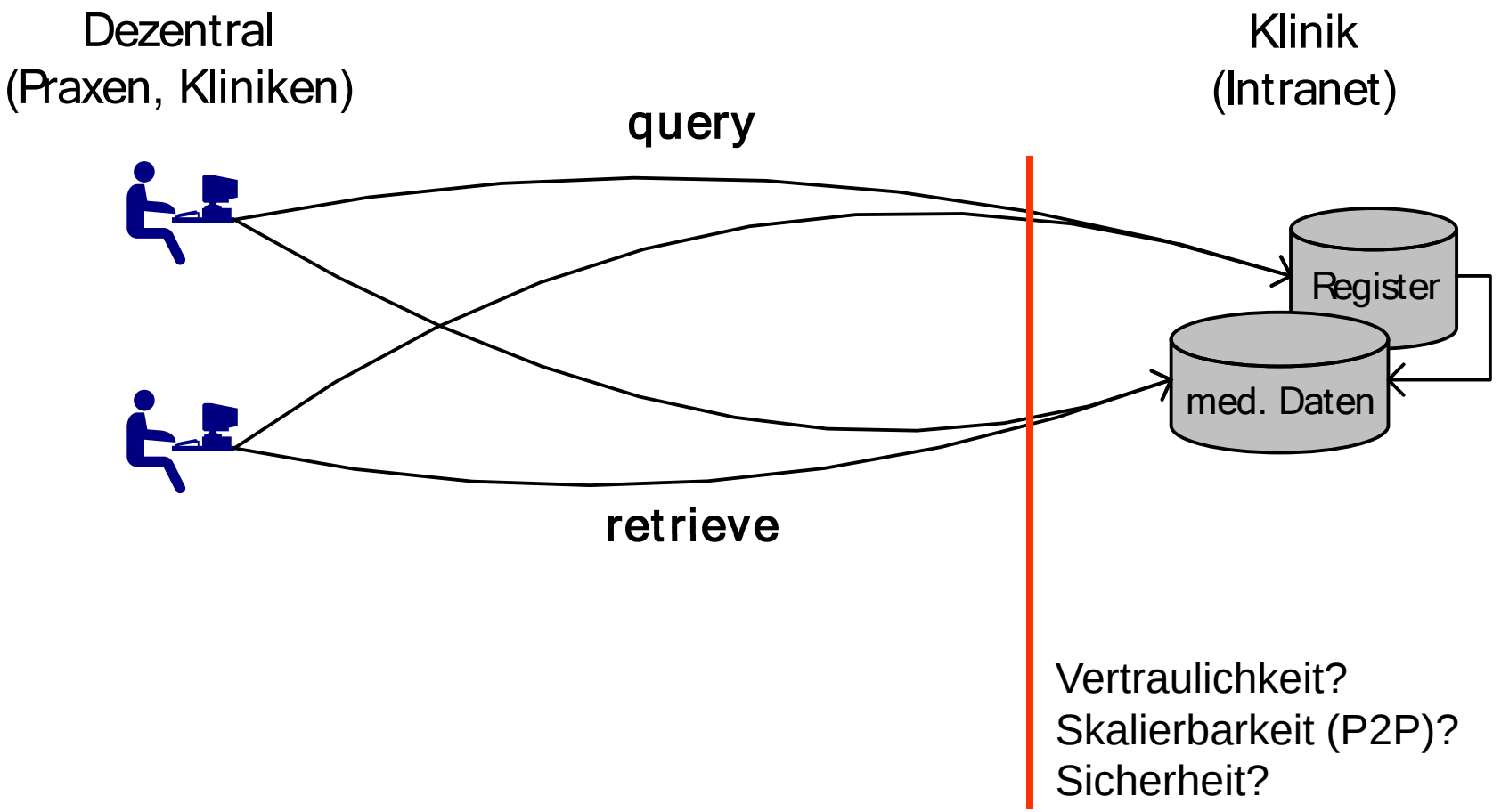
Kooperation und Konkurrenz

- Kooperation statt Konkurrenz bei der Schaffung von Rahmenbedingungen für eine Verbesserung der medizinischen Versorgung
- Wettbewerb über medizinische Leistungsfähigkeit in Versorgungsnetzen und nicht über technologischen »Lock-In«

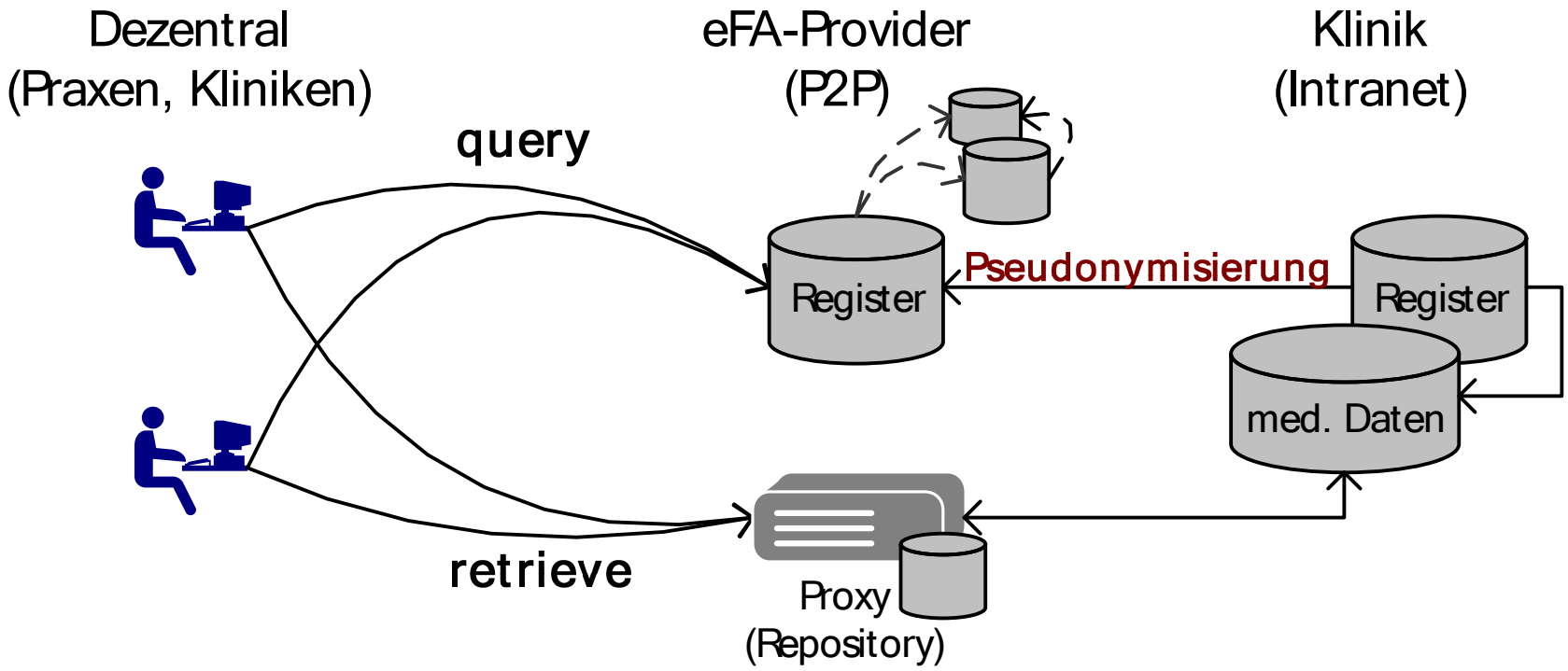
Offenheit

- Alle Spezifikationen sind öffentlich und frei umsetzbar.

Bereitstellung von med. Daten



eFA Provider



Merkmale des Patienten

	Dezentral verwaltet / erzeugt		Zentral verwaltet / erzeugt
	One-time	repeatable	
Widerrufbar	Private Key (Challenge-Response)	Signed Secret Objekt auf Träger Pseudonym	Zertifikat, Kartennummer Username (virtuelle Identität) Pseudonym
Lebenslang gültig		Biometrische Merkmale	Name, Alter, etc. Rentenversicherungsnummer

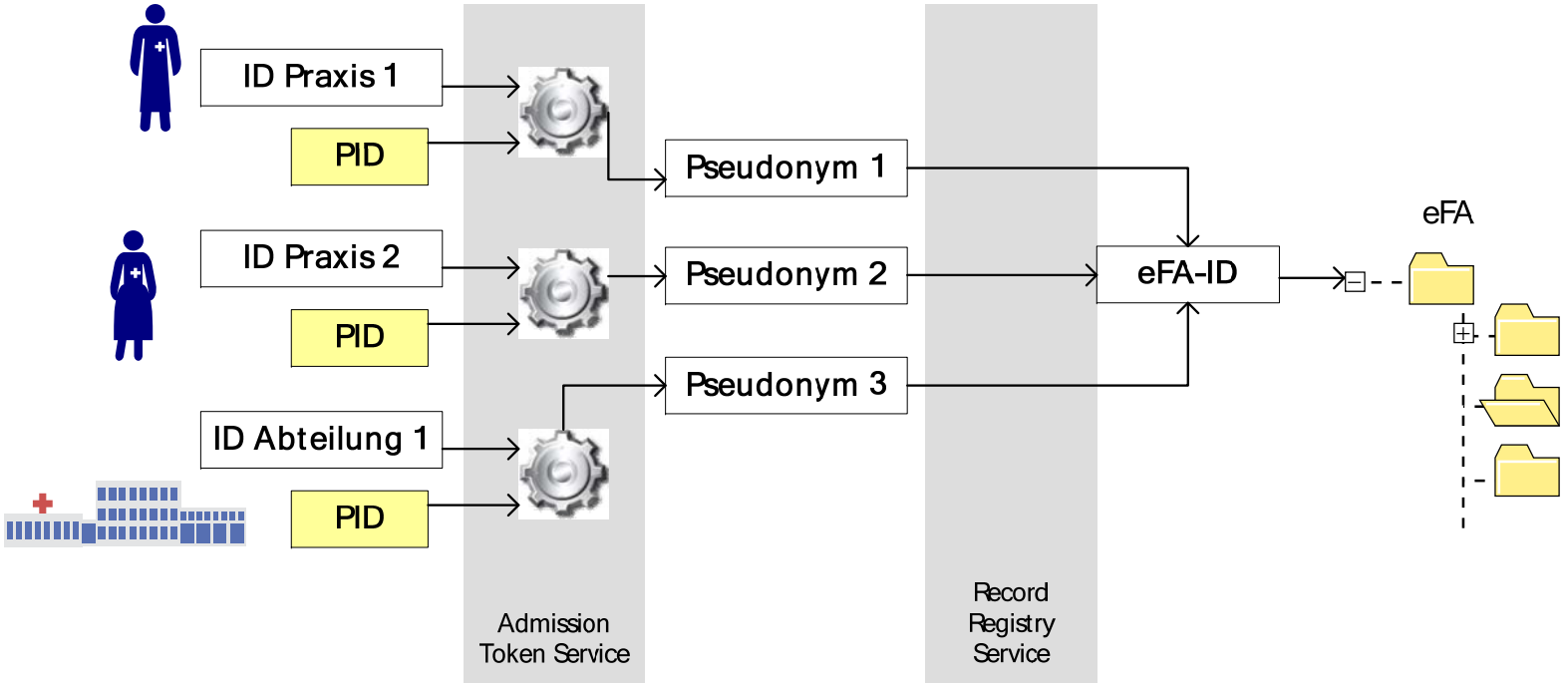
Patient identifizieren: Öffentliches Merkmal (idealerweise langlebig und mit durch Patienten gesteuertem Lebenszyklus)

Patient authentifizieren: Dezentrales Merkmal (idealerweise One-Time)

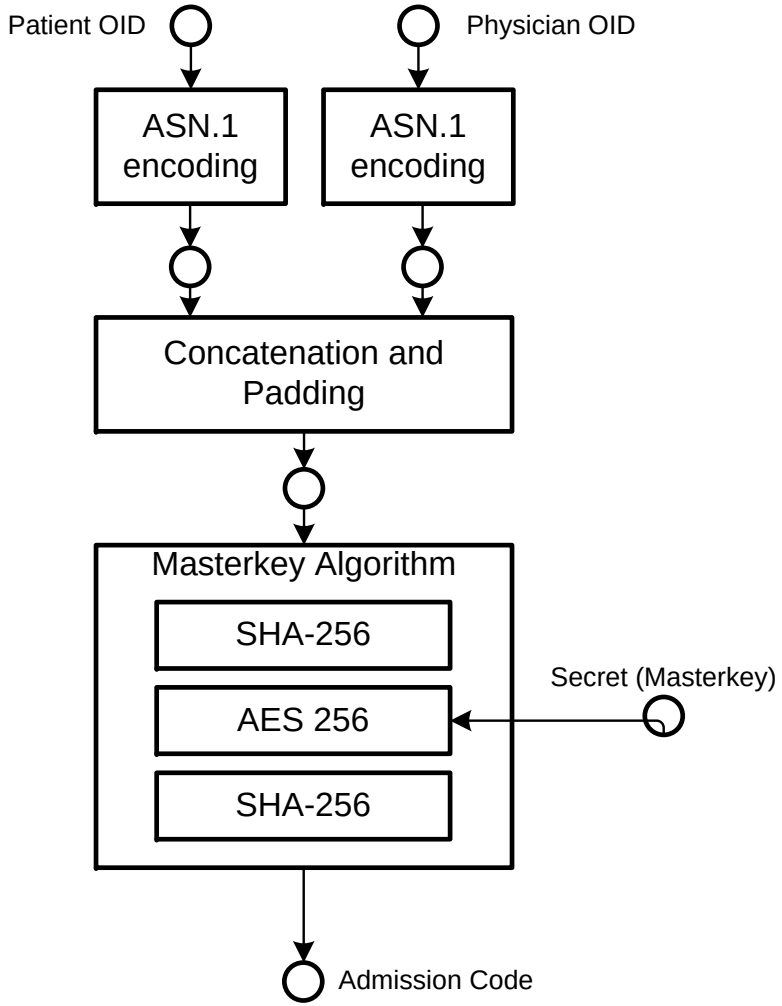
Datenzuordnung: Öffentliches Merkmal (Widerrufbar)

Ordnungskriterien der eFA

- Alle Fallakten verwenden als einziges Ordnungkriterium die eFA-ID. Diese ist eine semantik-freie OID ohne Patientenbezug.
- Die Zuordnung von Fallakten zu Patienten erfolgt über Pseudonyme
- Der AdmissionToken Service ist zustandslos und verwaltet keine Daten



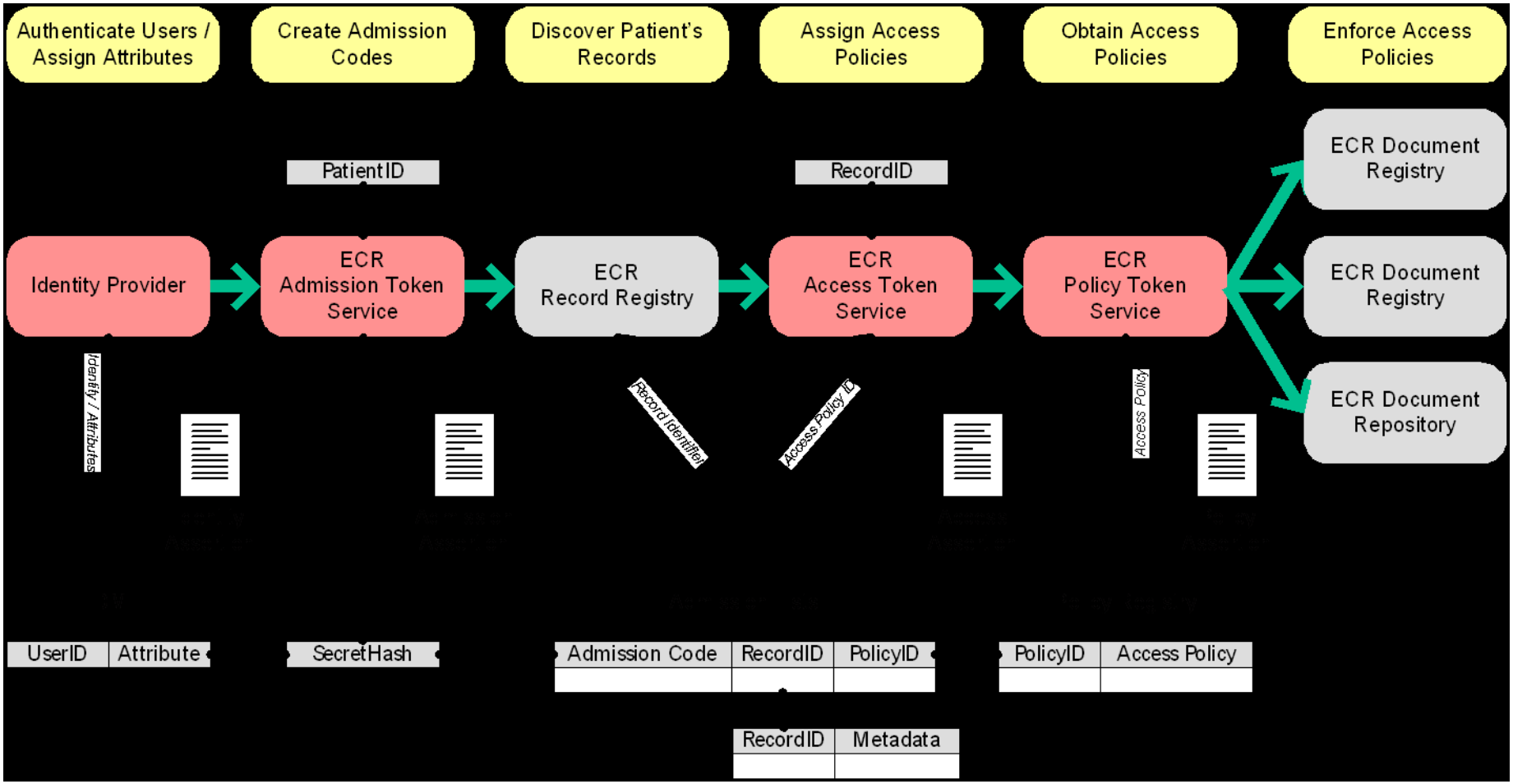
Pseudonym-Berechnung



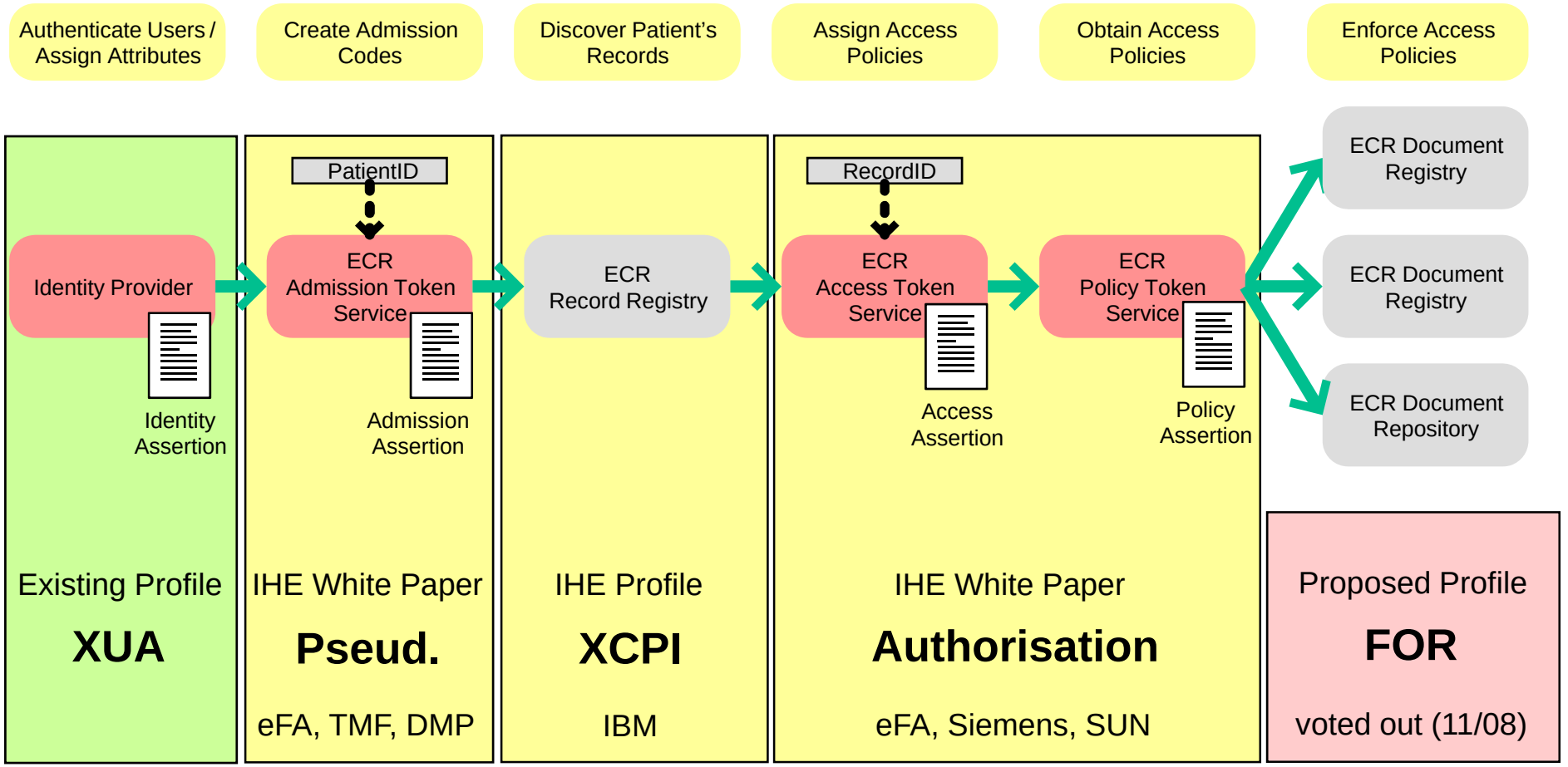
Merkmale der eFA-Pseudonyme

- unterschiedliche Pseudonyme für verschiedene Anwendungen möglich (z. B. um Verknüpfungen zu verhindern)
- Ein Zugangscode pro Kombination aus Anwendung, Patient und Berechtigtem
  - nur eine Suchanfrage: “Liste alle Fallakten des Patienten X zu denen ich zugriffsberechtigt bin!”
  - keine Änderung der Schadenshöhe im Mißbrauchsfall gegenüber der aktuellen Offline-Situation (aber bessere Nachweisbarkeit!)
- Das Verfahren ist geeignet, einfache DAC-Szenarien sicher abzubilden
  - Zugangserlaubnis für Individuen, Rollen, Gruppen
  - Trennung von Zugangs- und Zugriffssicherung (eFA: Admission Codes + XACML Policies)

Abläufe der eFA-Sicherheitsarchitektur



Abläufe der eFA-Sicherheitsarchitektur



Themen für das IHE White Paper

- Identity Protection, Pseudonymisation, and Anonymisation
- Pseudonymisation Models (Use Cases)
- Building Blocks
- Implementation and Deployment
- Security Considerations
- Outline of a Privacy Framework
- Application of Pseudonymisation on Content Profiles from PCC and QRPH

- Grundlagen
  - ISO TC 215: Privacy Protection through Pseudonymisation in eHealth.
  - TMF: IT Infrastructure for Clinical Research
  - OASIS WSFED technical committee
  - eCR Admission Token Service

eFA

elektronische FallAkte

Wir verbinden Menschen und Informationen

http://www.fallakte.de

- Welche Population ist im Anwendungsfall / Projekt betroffen?
- Wie wird eine eindeutige Identifikation sichergestellt? Oder werden Homonym- und Synonymfehler toleriert?
- Welche Pseudonyme oder nichtsprechenden Ordnungsmerkmale werden verwendet? (Aufbau/Struktur)
- Aus welchen Daten werden diese Pseudonyme erzeugt?
  Wird eine eindeutige ID zugrunde gelegt oder werden (dann notgedrungen fehlerbehaftete) persönliche Daten in die Pseudonymerzeugung eingespeist?
- Wie werden Pseudonyme erzeugt?
  - Zuordnungsliste?
  - Kryptographische Transformation?
  - Andere Methoden?
- Wo und von wem werden Pseudonyme erzeugt? z. B. Datentreuhänder, dezentral, ...?
- Welche Szenarien zur Depseudonymisierung sind vorgesehen?
  - Wie wird dann verfahren?
  - Wer ist involviert?
  - Wer kann Pseudonyme auflösen? (d. h. wer hat die dazu nötigen Informationen?)
- Gibt es weitere zum Patienten/Probanden beziehbaren IDs/Pseudonyme, z.B. auch für Laborproben, und wie ist deren Beziehung untereinander?
- Wie ist die Datenhaltung der organisiert und verteilt? (medizinische Daten, nicht-medizinische Daten, was liegt im offenen Personenbezug und was im Bezug zu dem bzw. den Pseudonym(en) vor)
- Gab es spezifische Anforderungen der Datenschutzbehörden und/oder Ethikkommissionen für das jeweilige Projekt, die die betreffende Pseudonymisierungslösung beeinflusst haben? Liegt ein Datenschutzkonzept und ein Votum einer Datenschutzbehörde vor zum betreffenden Anwendungsfall / Projekt vor?