

SOA & Security: Elektronische Fallakten

Dr. Jörg Caumanns, Oliver Boehm
Fraunhofer ISST Berlin

Frankfurt/Main, 12.03.08
Workshop: SOA & Security

Elektronische Fallakten: Hintergrund

- Januar 2006** Asklepios, Rhön-Klinikum, Sana Kliniken und Deutsche Krankenhausgesellschaft beauftragen das Fraunhofer ISST mit der "Spezifikation einer Architektur zum sicheren Austausch von Patientendaten"
- Juli 2006** Freigabe der Version 1.0
- November 2006** Beitritt von 7 weiteren Kliniken zum Konsortium
- Februar 2007** Einbindung der Industrie zum Abgleich der Spezifikationen mit bestehenden Produkten
- Mai 2007** Erste Pilotumsetzungen in Zuweiserportalen
- Dezember 2007** Freigabe der Version 1.2
- Februar 2008** Erste Umsetzung der Version 1.2 durch Siemens

eFA Konsortium und »Industrial Board«

Industry Partners

Medical Systems
(esp. Hospital Information Systems)

Siemens med
Agfa Healthcare
DOCexpert
Meierhofer AG
iSoft
Tieto Enator
Philips
ISPro
ICW

Infrastructure Components
(esp. Security and Identity Management)

SUN Oracle IBM
Microsoft T-Systems Cisco GMD
Intel Siemens SAP

Marabu

Hospitals

Rhön Clinics
(~60 Hospitals)

Asklepios Clinics
(~100 Hospitals)

Sana Clinics
(~50 Hospitals)

Helios Clinics (~60 Hospitals)
Munich Muncpal Clinics
Berlin Muncpal Clinics (vivantes)
Berlin Univ. Hospital (Charité)
Tübingen Univ. Hospital
Aachen Univ. Hospital
Dortmund Muncpal Clinics



Jan 2006

Nov 2006

May 2007

Anforderungen an die Architektur

Dezentralität - Vermeidung zentraler Dienste

- Übernahme von Authentisierungen und Autorisierungen (SSO, One-Stop-Shop)

Sicherheit - Beachtung der gesetzlichen Vorgaben des Datenschutz

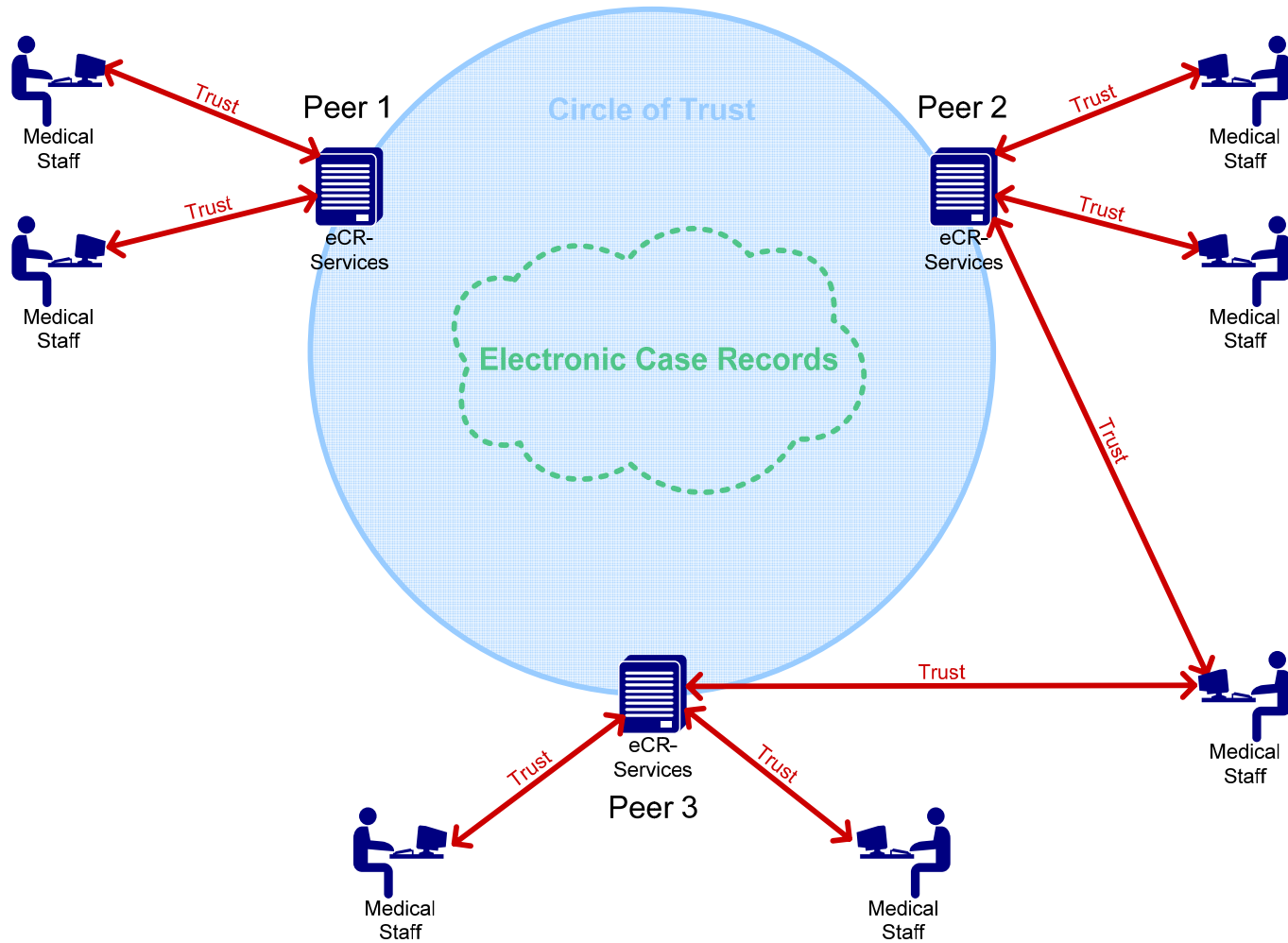
- Skalierbares Sicherheitsniveau

Investitionsschutz - Nutzung zukünftig relevanter Standards

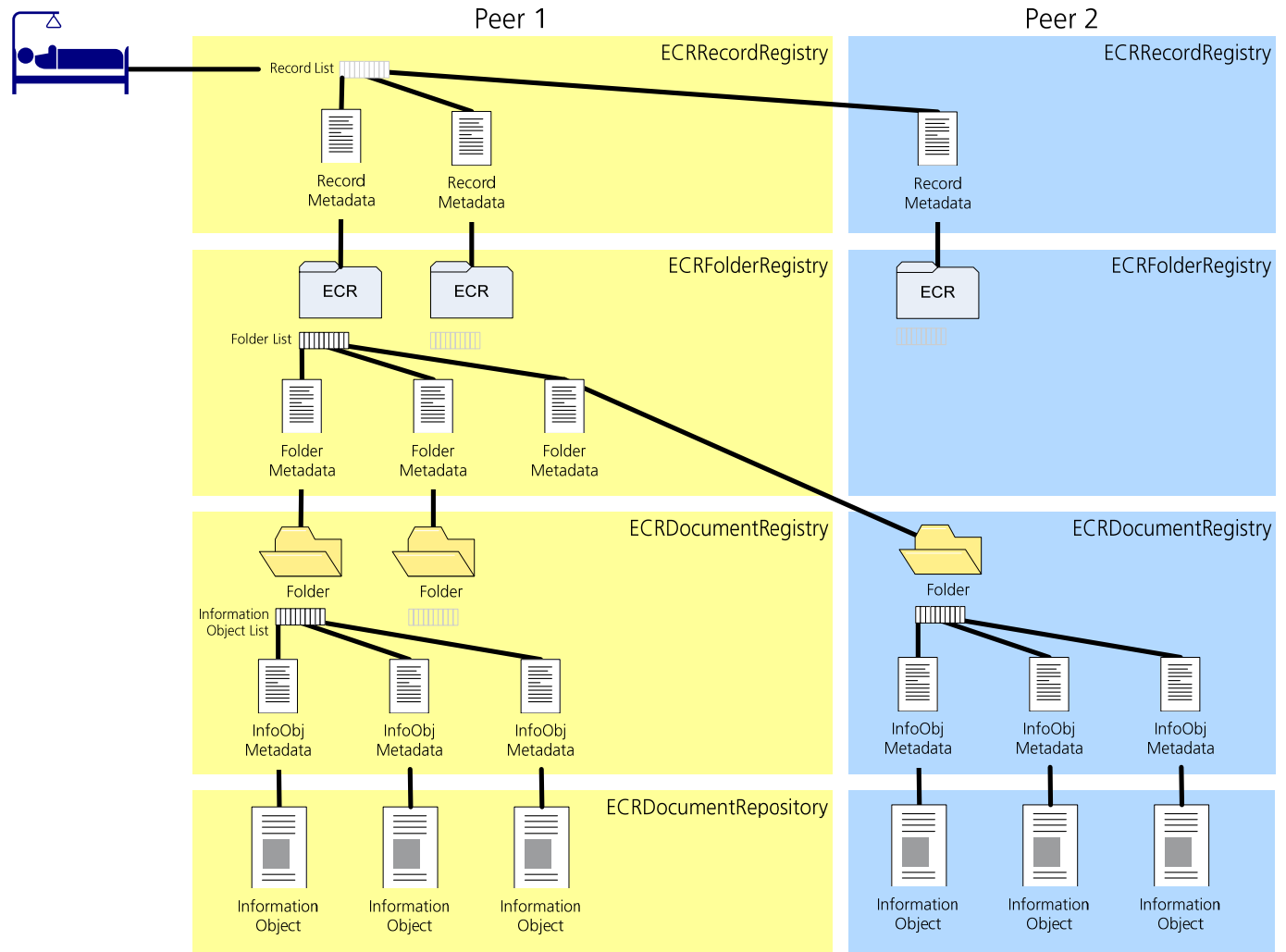
- Nachnutzbarkeit von Lösungsbausteinen durch andere Anwendungen

Administrierbarkeit - Vermeidung von Redundanzen in der Verwaltung medizinischer und administrativer Daten

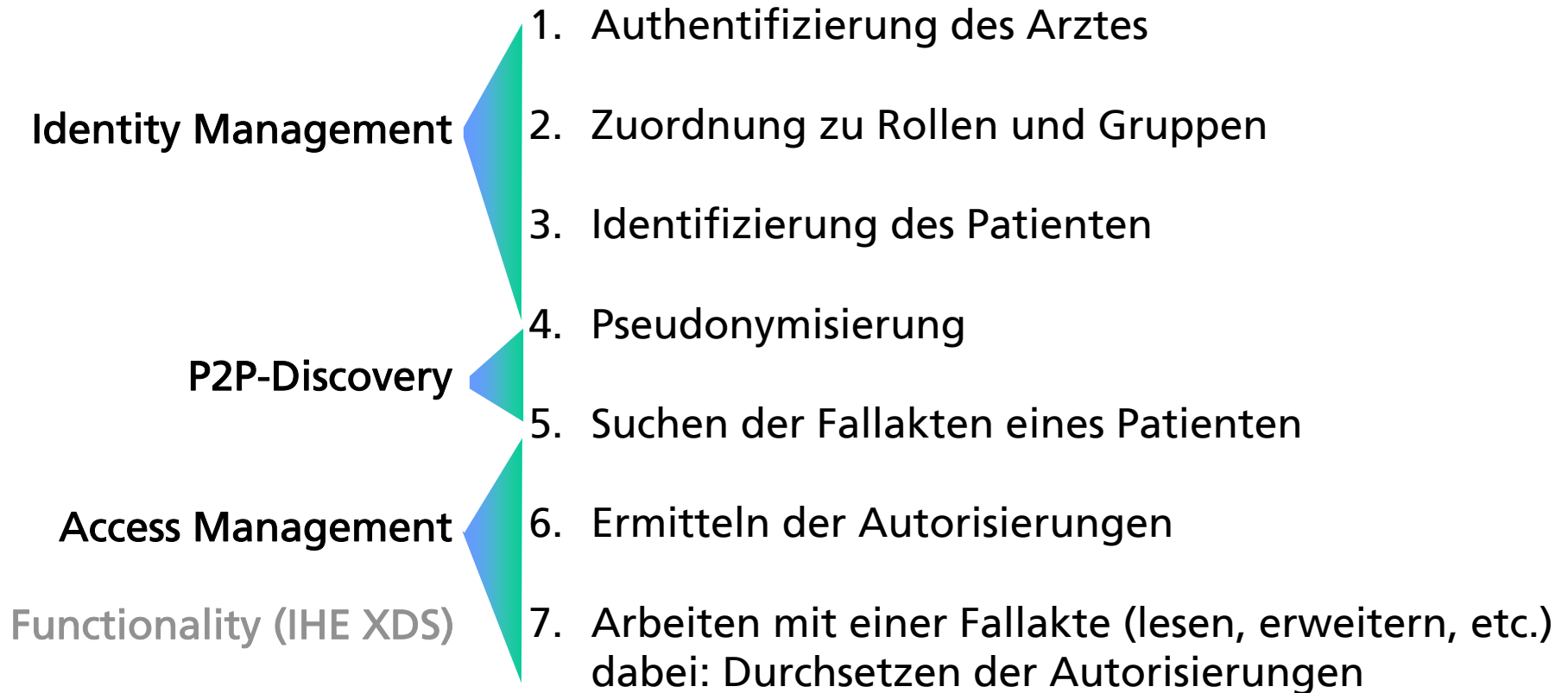
Circle of Trust



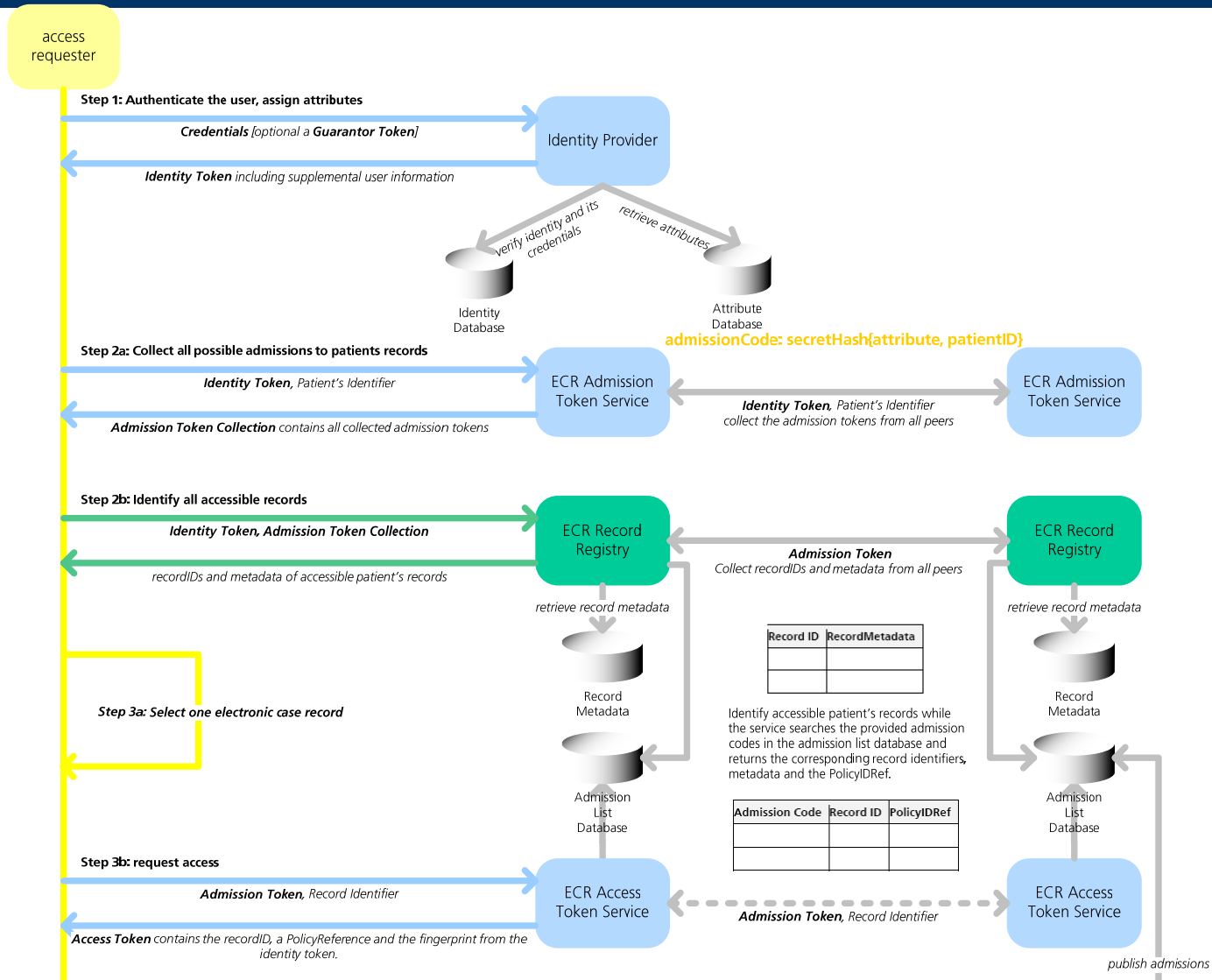
Anwendungsdienste



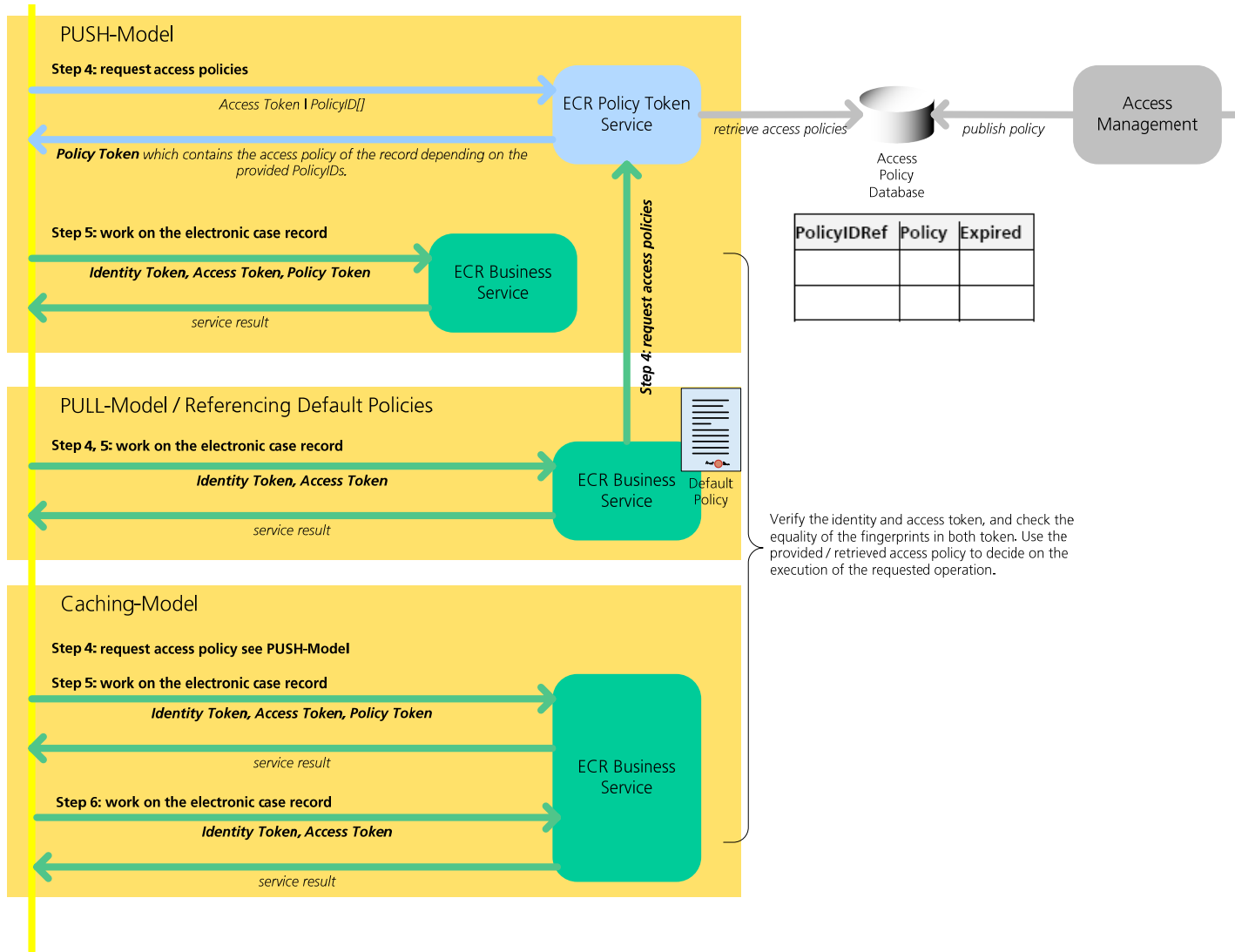
eCR Security: Ablaufschritte



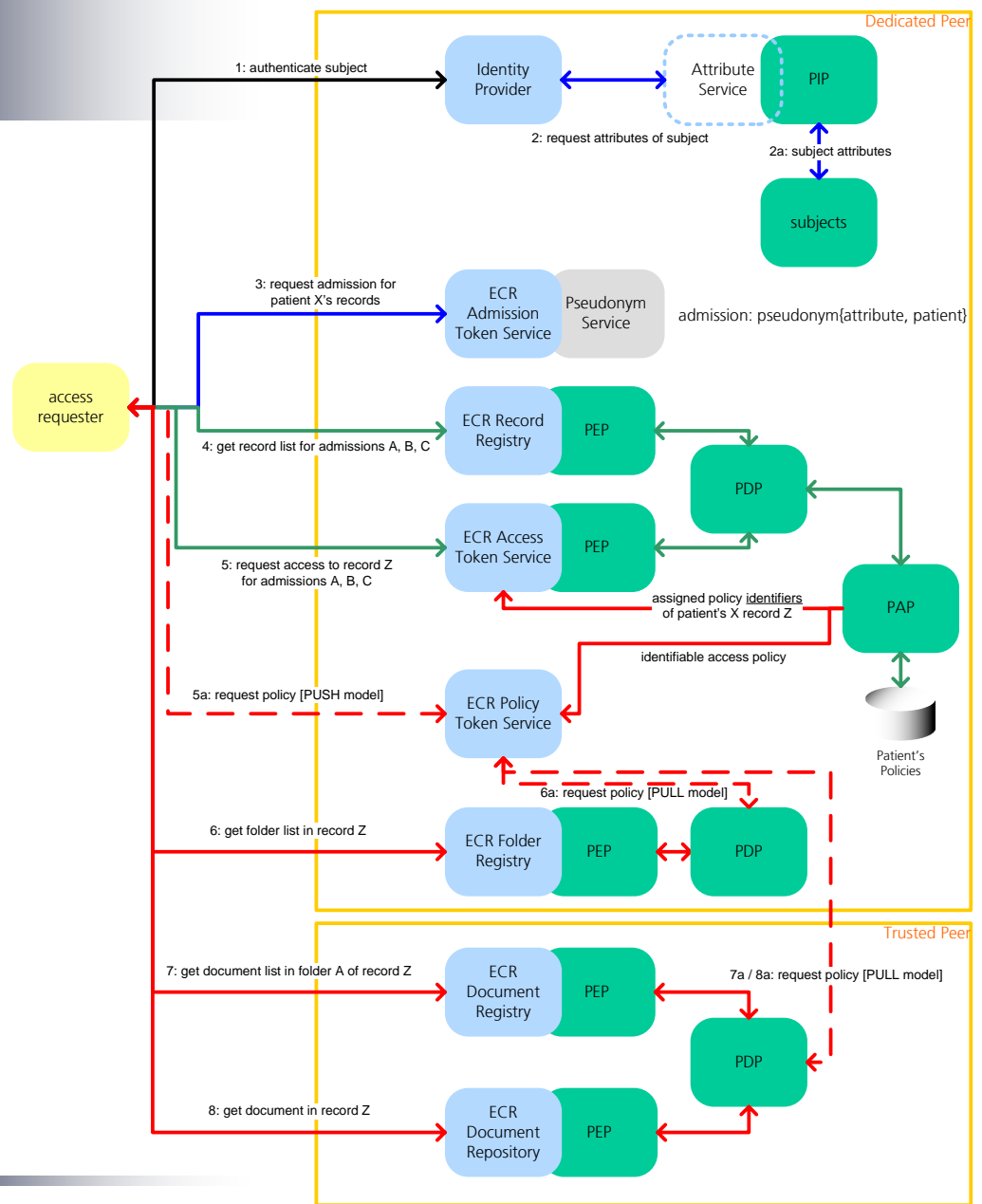
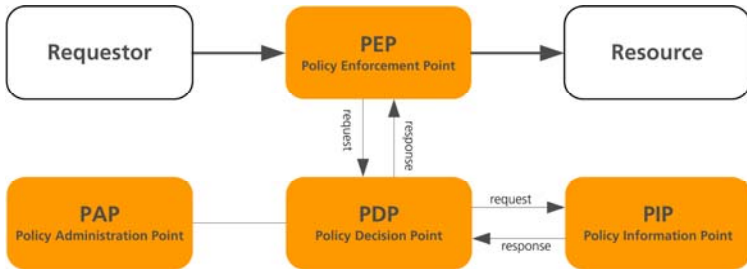
eCR Security Services



Policy Push vs. Policy Pull



Policy Enforcement



Realisierung von Sicherheit entlang der Ablaufschritte

Identity Management

Der Zugreifer ist identifiziert, authentifiziert und seine Rollen sind bekannt

-> **SAML Identity Assertion** (+ SAML Guarantor Assertion)

Ein Pseudonym liegt vor, in das die ID des Patienten und die Identitäten des Zugreifers eingeflossen sind

-> **SAML Admission Assertion**

P2P-Discovery

Die OID einer an das Pseudonym gebundenen Akte ist bekannt

Access Management

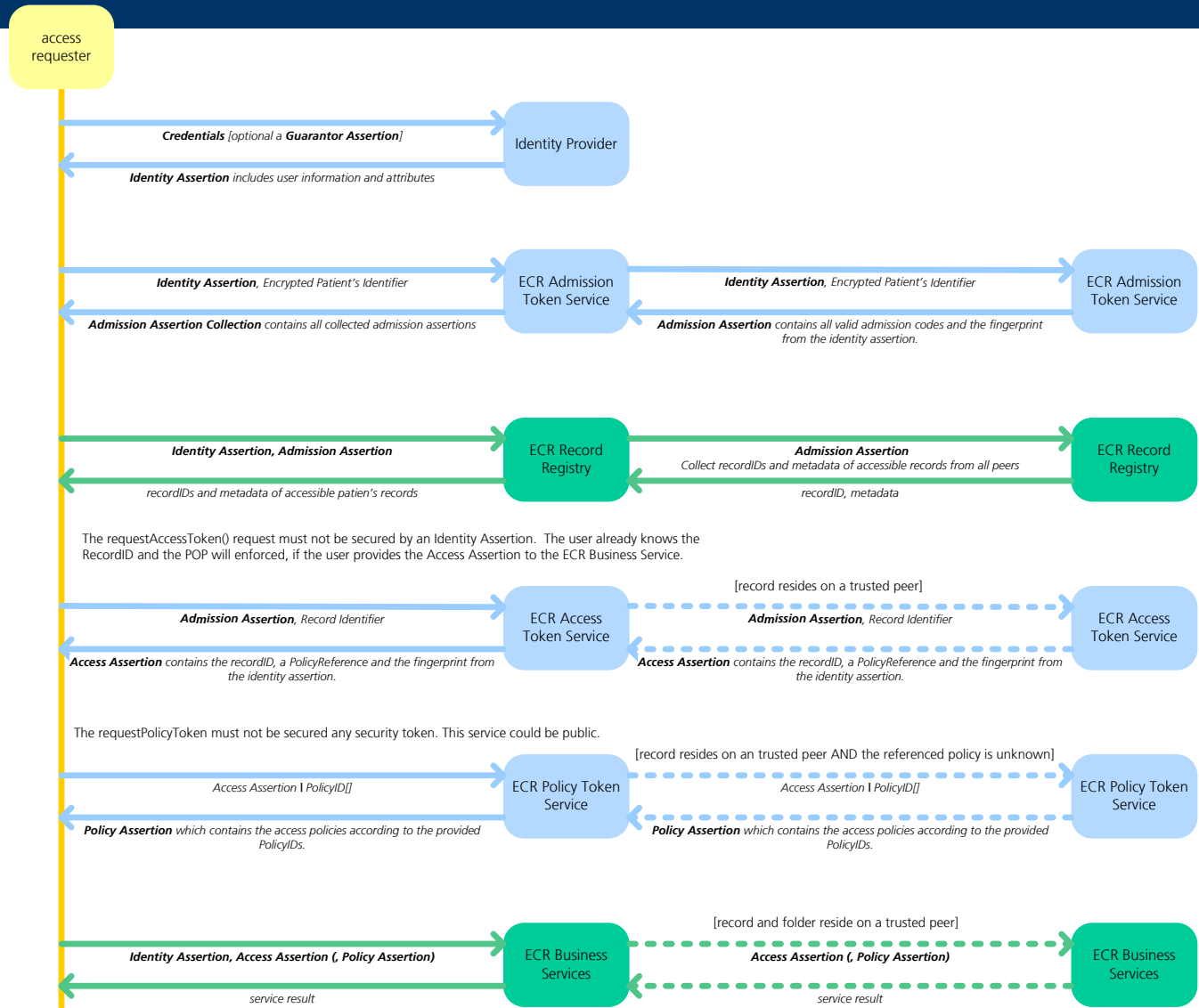
Es ist bekannt, wo die Berechtigungen des Zugreifers auf die Akte abgerufen werden können

-> **SAML Access Assertion**

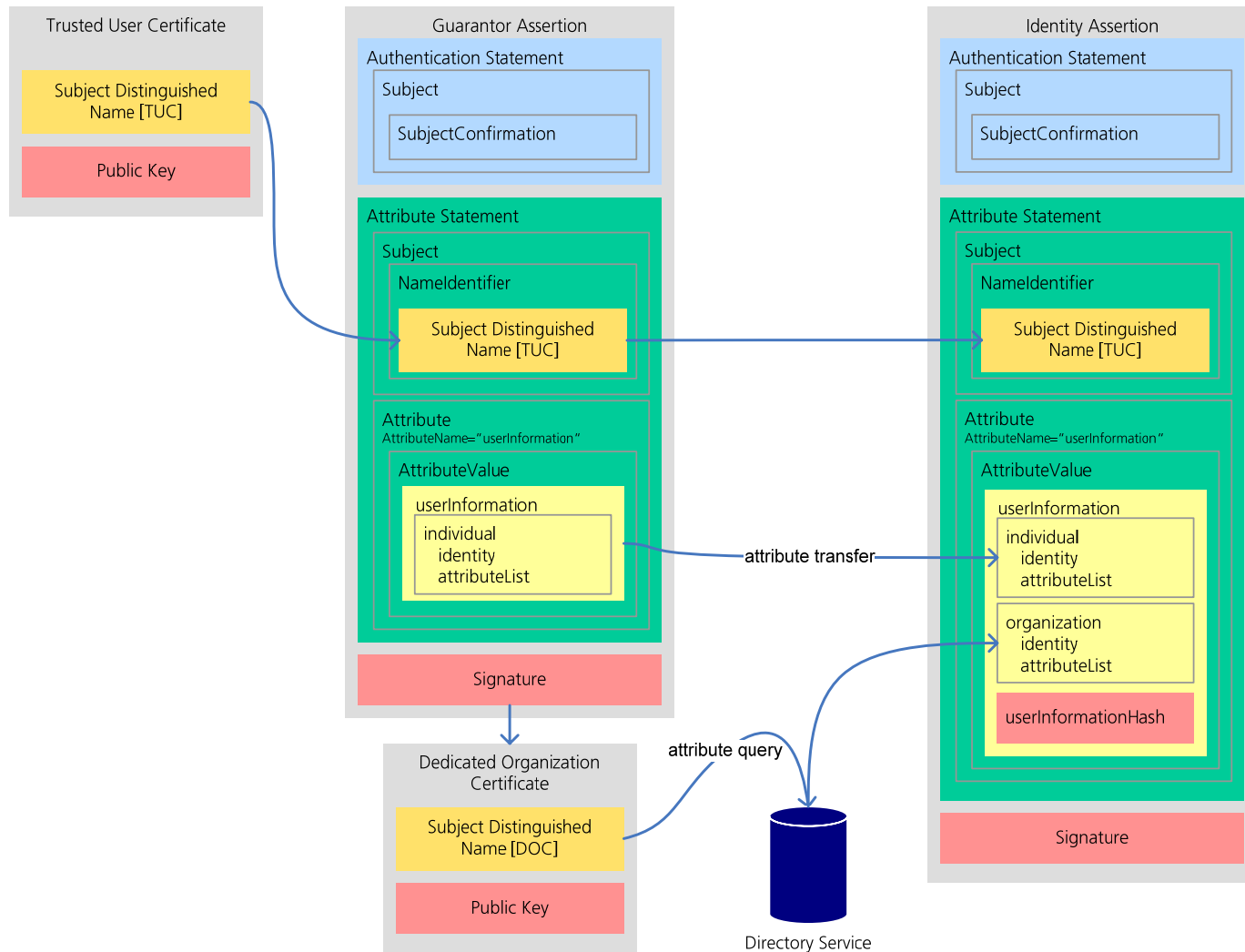
Die Berechtigungen des Zugreifers auf der Akte sind bekannt

-> **SAML Policy Assertion** (incl. XACML Policy)

Assertion Flow



Brokered Trust: Guarantor Assertions



SOAP Austausch von Nachrichten zwischen Clients und eFA-Diensten sowie zwischen eFA-Diensten

Web Service Description Language (WSDL) Beschreibung der als Web Services realisierten eFA Dienste

WS Security Sicherung der Kommunikationsstrecken

WS Policy
WS Security Policy Festlegung der einzusetzenden Sicherheitsmechanismen in der Kommunikation mit und zwischen eFA-Diensten

Security Assertion Markup Language (SAML) Kodierung von Authentisierungs- und Autorisierungsnachweisen

eXtensible Access Control Markup Lang. (XACML) Kodierung von Berechtigungen (Policies)

WS Trust Kommunikation eines Clients mit Sicherheitsdiensten der eFA

WS Secure Conversation Nachrichtenaustausch zwischen eFA-Diensten verschiedener Provider

WS Federation Language Basis der Verankerung des eFA Identity Providers in der Architektur

Dr. Jörg Caumanns

joerg.caumanns@isst.fhg.de

Oliver Boehm

oliver.boehm@isst.fhg.de

eFA-Website

<http://www.fallakte.de>

- Spezifikationen
- Veranstaltungshinweise
- Foliensätze