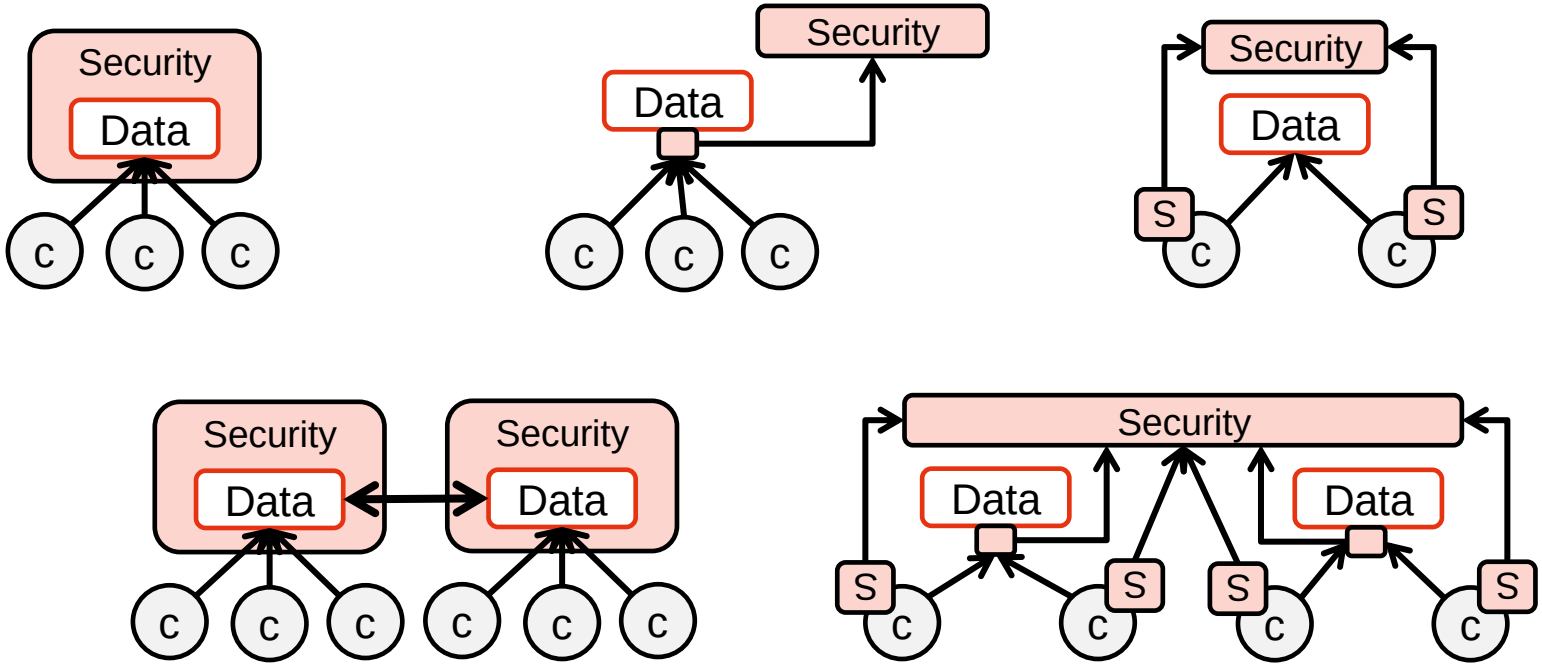
SECURITY DESIGN PATTERN FÜR EHEALTH-PLATTFORMEN

Dr. Jörg Caumanns
Fraunhofer FOKUS, Berlin

Fraunhofer FOKUS

BEISPIELE FÜR EHEALTH ARCHITEKTUREN



MOTIVATION

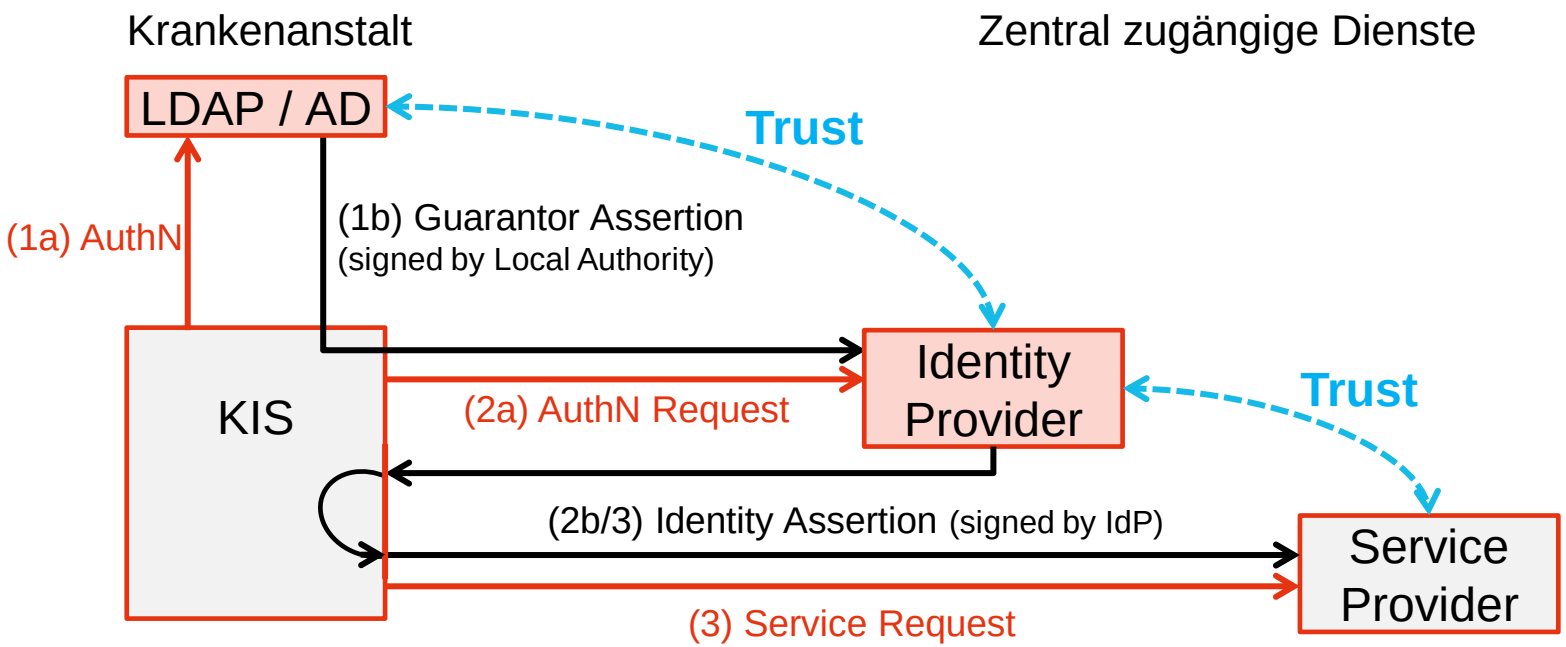
- Sicherheitsdienste zur Authentisierung und Autorisierung werden gerne am Zugang zum Server platziert, da dies viele Vorteile bringt
  - „Passt gut“ zu einer zentralen Verwaltung von Identitäten und Berechtigungen
  - Wirtschaftliche Umsetzung, da Sicherheitsdienste nur in wenigen Instanzen existieren und zentral administriert werden können
  - Singuläre „Source of Truth“ für die Pflege des Lebenszyklus von Identitäten, Credentials, Einwilligungen und Regulativen

- Hochgradig verteilte Systeme (z. B. P2P) werden in Bezug auf die Integration von Sicherheitsdiensten schnell komplex und anfällig
  - das Problem entsteht vor allem, wenn man verteilte Anwendungen mit auf Client-Server-Paradigmen ausgelegten Sicherheitsdiensten und Ablaufmustern kombiniert
  - **verteilte Systeme erfordern neue Muster für die Integration von Sicherheitsdiensten**

MUSTER 1: LOCAL AUTHORITY

Problem	Die Pflege von Nutzerattributen (z.B. administrative Rollen) über mehrere Organisationen hinweg ist teuer und der Datenbestand ist selten aktuell
Lösung	Ein vertrauenswürdiger Dienst innerhalb einer Einrichtung (Local Authority) spielt (dezentral) verwaltete Attribute im Rahmen der Authentisierung in die Plattform/Anwendung ein.
Umsetzung	Dezentral erstellte und signierte SAML Guarantor Assertion wird an einen zentralen Identity-Provider übergeben, der eine zentrale Vertrauensstellung hat und ggf. Erweiterungen oder Normierungen an der Assertion vornehmen kann. Der Identity Provider stellt auf Basis der Guarantor Assertion eine in der Domain/Anwendung nutzbare Identity Assertion aus.
Beispiele	EFA, ELGA, ePA-291a, epSOS

MUSTER 1: LOCAL AUTHORITY



Fraunhofer FOKUS

IdA = Identity Assertion
IdP = Identity Provider

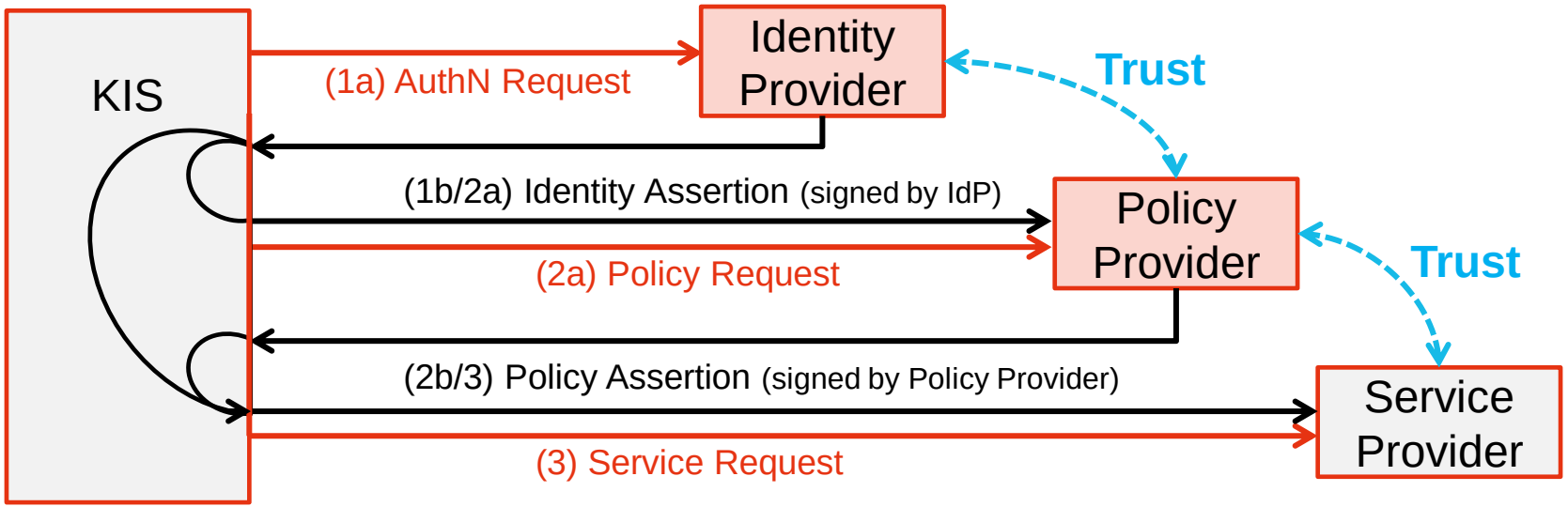
MUSTER 2: POLICY PUSH / ASSERTION CHAINING

Problem	In einem lose gekoppelten Berechtigungsmanagement kann ein Dienst die Policy des Nutzers nicht abrufen, da ihm Informationen fehlen (z.B. die „richtige“ ID von Patient oder Nutzer) oder da die Berechtigungen über mehrere Provider verteilt verwaltet werden.
Lösung	Der Consumer „besorgt“ sich die Information zu den Rechten des aktuellen Nutzer und fügt diese dem Dienstaufruf bei.
Umsetzung	Der Consumer ruft unter Beigabe einer IdA eine Policy Assertion vom Berechtigungssystem ab. Diese ist mit der IdA verknüpft und vom Berechtigungssystem signiert. Beim Dienstaufruf werden beide Assertions mitgegeben und die Policy vom Dienst durchgesetzt. Es wird faktisch ein Sicherheitskontext über Consumer und Provider gespannt.
Beispiele	EFA, (ELGA), ePA-291a

MUSTER 2: POLICY PUSH

Krankenanstalt

Zentral zugängige Dienste



Fraunhofer FOKUS

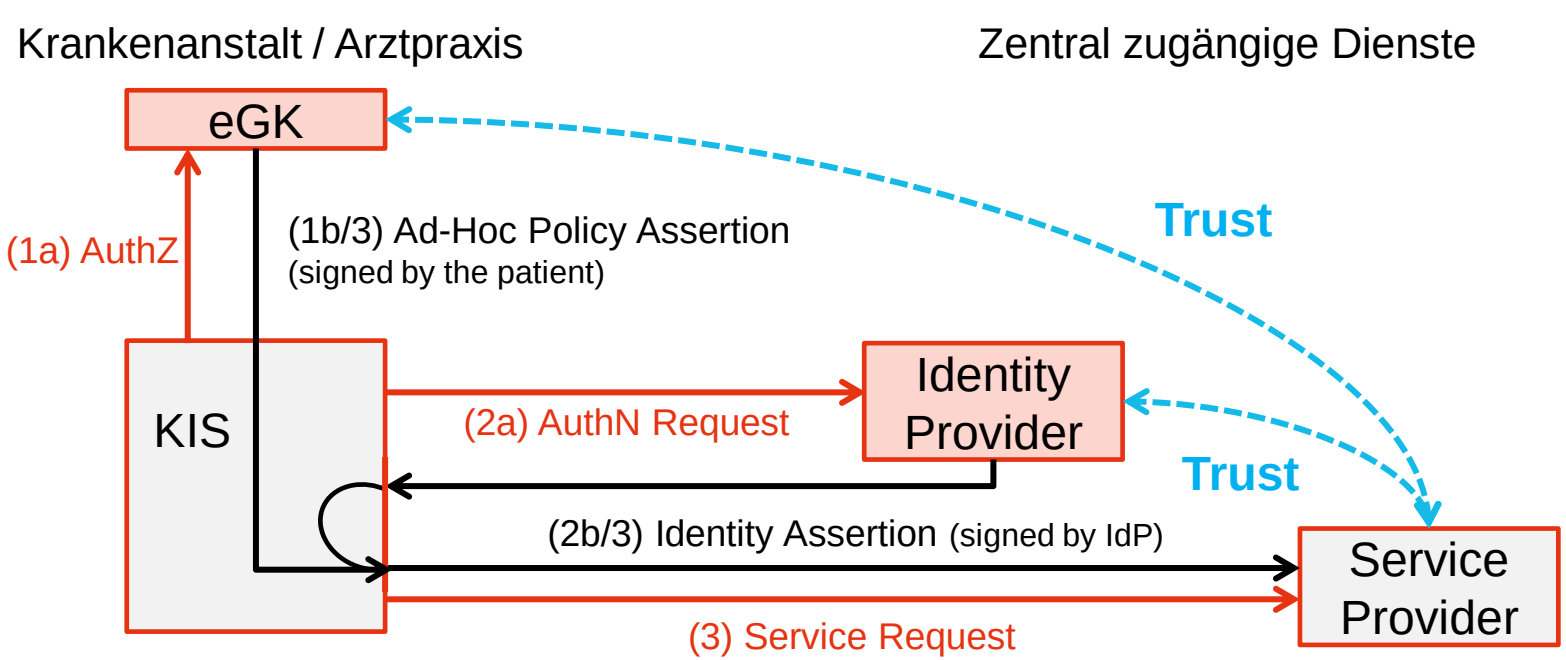
IdA = Identity Assertion

IdP = Identity Provider

MUSTER 3: AD-HOC POLICIES

Problem	Das Erfordernis eines Zugriffs auf eine Gesundheitsakte entsteht oft erst, wenn der Patient beim Arzt ist. Dann ist es aber nicht mehr möglich, eine entsprechende Berechtigung zentral zu registrieren.
Lösung	Eine Zugriffspolicy wird beim Arzt bedarfsgerecht erzeugt und vom Patienten freigegeben. Auf Basis der Policy stellt die Akte die gewünschten Daten bereit.
Umsetzung	Im Arztsystem wird eine XACML Policy erzeugt und per SmartCard vom Patienten signiert. Die Policy wird zusammen mit dem Request an die Anwendung geschickt und dort im Kontext des Requests ausgewertet. Die Policy verbleibt im System des Artes und kann innerhalb ihrer Gültigkeit mehrfach verwendet werden.
Beispiele	ePA-291a

MUSTER 3: AD-HOC POLICIES



Fraunhofer FOKUS

IdA = Identity Assertion
IdP = Identity Provider

FAZIT

- Identitäten müssen nicht zwingend zentral verwaltet werden.
  - Eine dezentrale Verwaltung kann gerade dann sinnvoll sein, wenn sich Attribute häufig ändern (z. B. Mitarbeiter in einer Krankenanstalt)
- Authentisierung muss nicht zwingend zentral passieren.
  - In der Praxis erleichtert man sich Vieles, wenn Personen dezentral und Organisationen zentral authentifiziert werden.
- Berechtigungen müssen nicht zwingend zentral gepflegt werden.
  - Gerade Szenarien, in denen Arzt und Patient zur selben Zeit am selben Ort sind, lassen sich gut mit Ad-Hoc-Autorisierungen ohne zentrales Berechtigungssystem abdecken.

GENUTZTE BEISPIELE

ELGA	http://www.elga.gv.at/
EFA	http://www.fallakte.de
	http://wiki.hl7.de/index.php?title=cdaefa:EFA_Spezifikation_v2.0
ePA-291a	https://www.epa291a.de/doku.php
epSOS	http://www.epsos.eu
IHE ITI	White Paper „Access Control“

KONTAKT

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
www.fokus.fraunhofer.de

Dr. Jörg Caumanns
Leiter Kompetenzzentrum E-HEALTH
joerg.caumanns@fokus.fraunhofer.de
Tel. +49 (0)30 3463-7581