

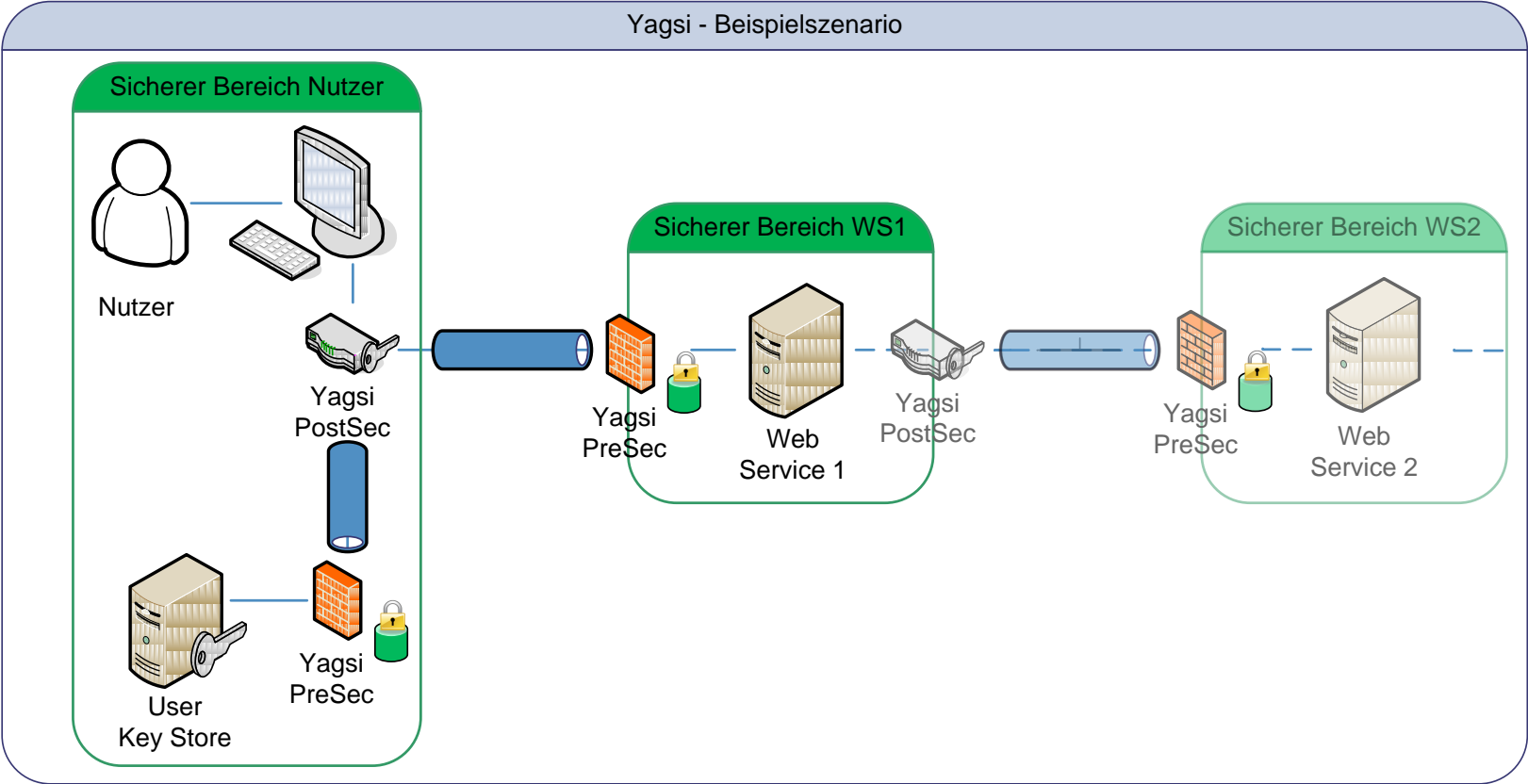
# Yagsi – Sicherheit für Webservices im Gesundheitswesen

Andreas Hoheisel, Oleg Khovalko

November 2010



# Übersicht



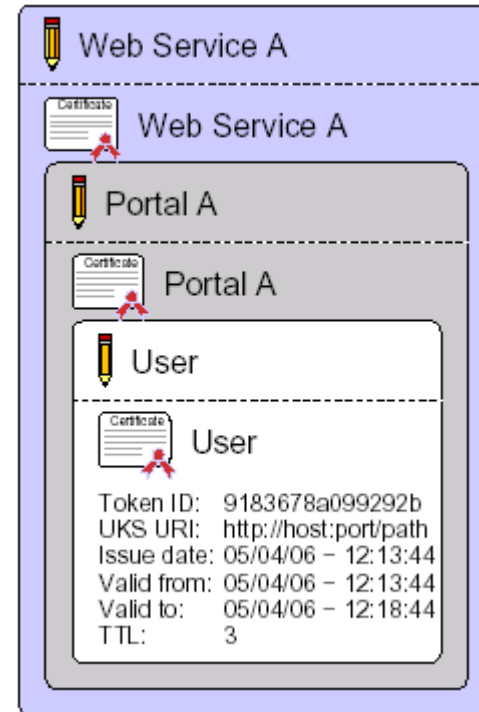
# Yagsi: Sicherheit für Web-Services im Gesundheitswesen

## Ziele / Visionen

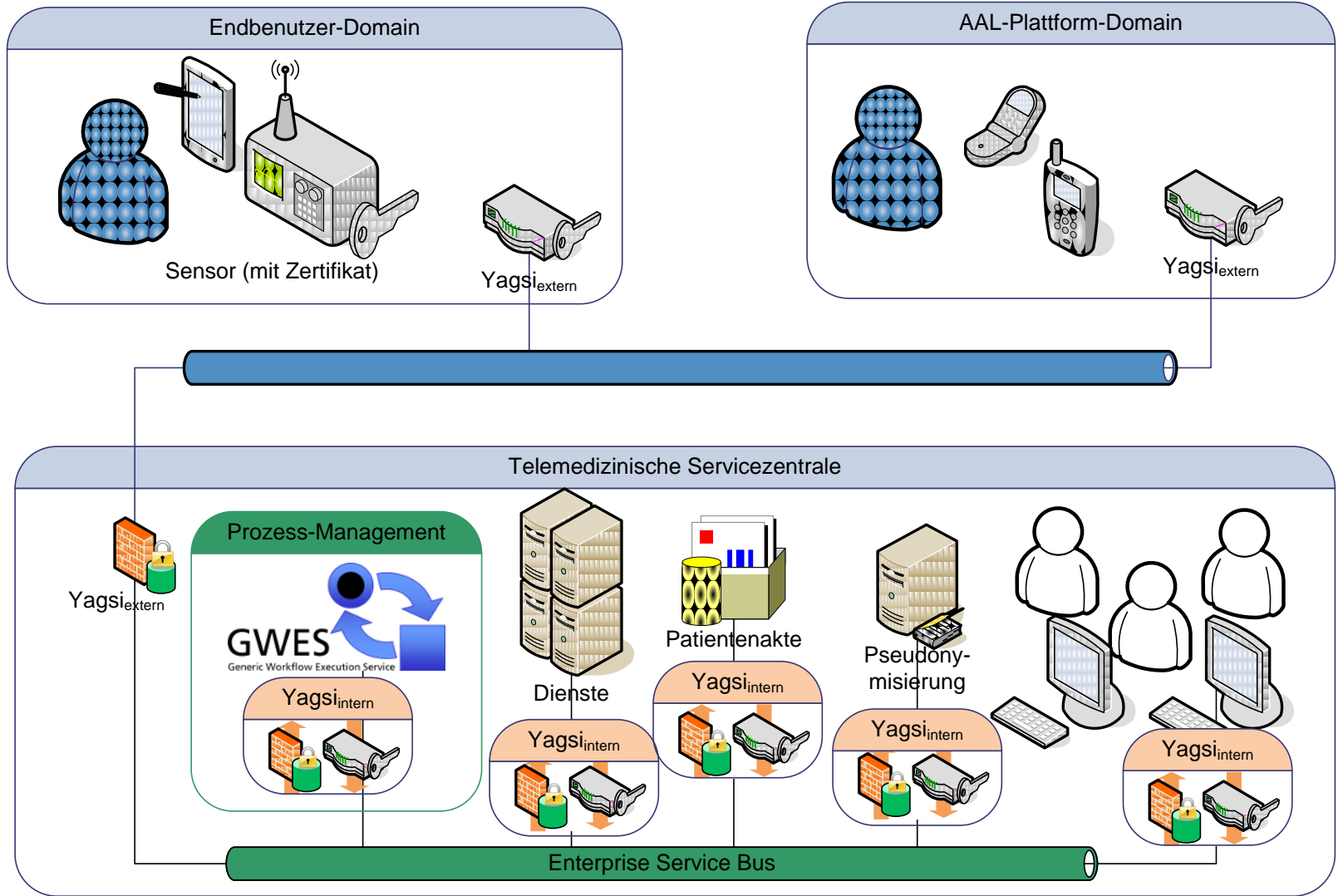
- Bereitstellung einer generischen Sicherheitsinfrastruktur, mit der die Datensicherheit bei der SOAP-basierten Kommunikation zwischen Sensoren, Anwendungen und Diensten in automatisierten IT-Prozessen (=Workflows) von SmartSenior sichergestellt werden kann.
- Schwerpunkte der Forschung:
  - Feingranulare Autorisierung
  - Beschränkte Delegation von Zugriffsrechten
  - Fallorientiertes Rollenmodell
  - Berücksichtigung von Notfällen
- Wichtig für das Gesundheitswesen: Berücksichtigung der entsprechenden Standards (z.B. bezüglich elektronischer Fallakte) und gesetzlichen Rahmenbedingungen.

# Security Token

- Security Token als SAML-Assertion: Enthält Zertifikatskette, die digitale Unterschriften vom verursachenden Nutzer und allen zwischengeschalteten Diensten enthält.
- Sicherstellung der Datenintegrität per WS-Security auf Nachrichtenebene



# Anwendungsbeispiel



# Yagsi – Technisches Konzept

## Standards

- Kommunikation zwischen Sensoren, Anwendungen und Diensten per **Web-Service (SOAP)**
- Authentifizierung per **X509-Zertifikate**
- Integrität und Vertraulichkeit per **WS-Security**
- Verbindlichkeit per **Audit-Trail (RFC3881)**
- Autorisierung per **SAML-Assertions** und **XACML**
- **Transparente** Nutzung für WS-Client und WS-Server über Verschlüsselungs-Proxy beim Client und speziellen Firewall-Dienst beim Server

## Wichtige Literatur

- Stephan Müller: Realisierung von feingranularem Rechtemanagement in einer service-orientierten Grid-Architektur. Diplomarbeit, 2007.
- Olaf Rode (Ed.): Authentisierung/Authentifizierung – Überblick über die Client- und Dienstauthentisierung im Kontext der elektronischen Fallakte. Fraunhofer ISST, 2008.
- Olaf Rode, Jörg Caumanns, Sören Bittins (Eds.): Audit Trail – Anforderung an die Erstellung von Audit Trails im Kontext der elektronischen Fallakte. Fraunhofer ISST, 2008.