ROLLEN- UND KONTEXT BASIERTE AUTORISIERUNG (RBAC) ALS SECURITY KONZEPT FÜR IHE-XDS BASIERTE ELEKTRONISCHE GESUNDHEITSAKTEN

Wozak F[1], Ammenwerth E[1], Breu R[2], Mair R[2,] Penz R[3], Schabetsberger T[3], Vogl R[4]

Kurzfassung

Durch multimorbide Patienten wird in den nächsten Jahren ein Kostenanstieg im Gesundheitssystem erwartet. Die trans-institutionale Verfügbarkeit medizinischer Dokumente kann Qualität und Effizienz im Gesundheitssystem steigern. In dieser Arbeit wird eine auf IHE-XDS basierende Architektur für verteilte elektronische Gesundheitsakten mit End-to-End Security als Infrastruktur zur sicheren Übertragung medizinischer Daten vorgestellt. Ein auf Role Based Access Control (RBAC) basierendes Sicherheitskonzept wurde dafür entwickelt.

1. Einleitung

Ein Kostenanstieg wird im Gesundheitssystem in den nächsten Jahren durch steigenden Altersdurchschnitt und Multi-Morbidität der Patienten erwartet. Verbesserte Kommunikation zwischen den am Behandlungsprozess beteiligter Organisationen führt zu Qualitäts- und Effizienzsteigerung [1] und kann somit zur Kosteneinsparung beitragen. In den nächsten Jahren wird ebenfalls mit einer konstant steigenden Menge an elektronisch übertragenen Daten im Gesundheitswesen gerechnet [2,3].

Shared Electronic Health Records (SEHRs) sind verteilte elektronische Gesundheitsakten, die eine Patienten-zentrierte Bereitstellung von medizinischen Dokumenten für autorisierte Gesundheitsdiensteanbieter ermöglichen. Folgende Aspekte sind dabei zurzeit ungelöst:

1. Es existiert keine Erfahrung wie ein SEHR zu implementieren ist um den Anforderungen der Akteure des Gesundheitswesens gerecht zu werden.

2. Es existiert keine Erfahrung zur technischen Umsetzung eines Sicherheitskonzeptes um den Schutz persönlicher Daten in dem Ausmaß zu gewährleisten, wie im österreichischem Datenschutzgesetz und internationalen Richtlinien gefordert wird.

1 Institut für Informationssysteme des Gesundheitswesens, UMIT - Private Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik, Hall in Tirol

2 Institute of Computer Science, Leopold-Franzens-Universität Innsbruck, Innsbruck

3 health information technologies tirol GmbH, Innsbruck

3. Gängige Security Verfahren bieten Point-to-Point Security auf Netzwerkebene, nicht jedoch die geforderte End-to-End Security auf Applikationsebene.

End-to-End Security garantiert eine gesicherte Übertragung medizinischer Daten zwischen beteiligten Applikationen und ermöglicht so die Überprüfung der Rolle (z.B. Arzt oder Pflegekraft) des Benutzers. Mittels Point-to-Point Security auf Netzwerkebene ist dies nicht möglich.

1.1 Zielsetzung

Hauptziel dieser Arbeit ist die Vorstellung eines Konzeptes zur Rollen- und Kontext basierten Autorisierung als Role Based Access Control (RBAC) zur Gewährleistung von End-to-End Security für verteilte elektronische Gesundheitsakten. Als Teilziel und Voraussetzung leitet sich daraus die Erstellung einer verteilten *Health Information System* (HIS) Architektur für elektronische Gesundheitsakten ab.

Die vorgestellte HIS Architektur basiert auf dem IHE XDS Integrationsprofil [4] und verwendet *Medical Data GRIDs* [5] als darunter liegende Netzwerkarchitektur.

2. Methoden

System- und Sicherheitsanforderungen konnten aus einer Analyse der funktionalen Anforderungen von Schabetsberger et al. [6] abgeleitet werden.

2.1 IHE – XDS (Cross EnterpriseDocument Sharing)

Integrating the Healthcare Enterprise entwickelt Integrationsprofile basierend auf weit verbreiteten Kommunikationsstandards um Herstellerunabhängige Interoperabilität von klinischen Systemen zu gewährleisten. Cross Enterprise Sharing (XDS) ist ein Integrationsprofil zum trans-institutionalen Austausch medizinischer Dokumente[4].

2.2 Medical Data GRIDs

Sicherheit, Skalierbarkeit und Interoperabilität sind Hauptanforderungen an die SEHR Architektur. Medical Data GRIDs kommen dafür zum Einsatz und erweitern die Definition von Data GRIDs, um den Anforderungen des Gesundheitsbereichs gerecht zu werden [5].

2.3 Role Based Access Control (RBAC)

RBAC basiert auf dem Konzept Benutzern Rollen zuzuordnen, wobei für jede einzelne Rolle wiederum Berechtigungen vergeben werden können [7].

3. Ergebnisse

3.1 Architektur

Eine Open Source Prototyp Architektur basierend auf IHE-XDS und Medical Data GRIDS ist zurzeit in Entwicklung. Prototyp 1 wurde Ende November 2006 fertig gestellt. Die Architektur basiert auf unabhängigen Diensten zur Speicherung von Dokumenten (Document Repository), Registrierung von Metadaten und Service Discovery (Document Registry), Patienten Identifikationsdiensten (PatientId Source) sowie Produzenten (Document Source) und Empfängern von Dokumenten (Document Consumer).

Die Implementierung der dafür benötigten Services erfolgte in Java als Web Services mit Apache Tomcat als Application Server und Apache Axis als Web Service Framework. Dokumente verbleiben beim Ersteller, lediglich Metadaten sind über die Registry suchbar. Eine eindeutige Patienten ID wird über die PatientId Source bezogen.

3.2 Security Konzept: Role Based Access Control (RBAC)

Für elektronische Gesundheitsakten ist ein höchstmöglicher Sicherheitsstandard im Sinne von End-to-End Security erforderlich. Daher werden neben bekannten Security Maßnahmen, wie verschlüsselte Übertragung und Einsatz digitaler Signatur, detaillierte Zugriffsberechtigungen auf medizinische Dokumente gefordert.

Effektive Zugriffsberechtigungen eines Benutzers werden daher anhand dessen Rolle von den Applikationen auf Basis der RBAC dynamisch vergeben. Die gewählte RBAC Implementierung unterstützt neben Authentifizierung / Autorisierung von Benutzern dies auch für beteiligte Services untereinander zur Vermeidung von Man-in-the-Middle Attacken. Folgende für elektronische Gesundheitsakten geforderte Sicherheitsprinzipien werden mit RBAC abgedeckt:

- 4-Augen Prinzip: Patient muss beim Arzt für einen Zugriff auf Dokumente anwesend sein. Ausnahmen: Notfallzugriff, Patient kann eigene Daten einsehen.
- Patient kann Zugriffsberechtigungen auf Akte verwalten und Teile sogar für sich selbst sperren.
- Patient kann zeitlich beschränkte Zugriffsberechtigungen für Arzt oder Angehörige erteilen.
- Patient kann sich mit der österreichischen e-card authentifizieren.

Die in Abbildung 1 dargestellte RBAC Implementierung bildet ein zweistufiges Sicherheitskonzept.

3.3 Level 1: Service Role Checks

Web Services können nur von bekannten und registrierten Web Services aufgerufen werden. In jedem Aufruf wird dazu digitales *Service Zertifikat* mitgesendet, welches die Rolle des aufrufenden Services beschreibt. Nach erfolgreicher Identifikation wird diese Rolle anschließend mit der lokalen Policy des aufgerufenen Services verglichen und so entschieden, ob der Zugriff gewährt werden kann.

3.4 Level 2: User Role Checks:

Elektronische Gesundheitsakten beinhalten unterschiedliche Dokumente, die von unterschiedlichen Personengruppen (Rollen) eingesehen werden dürfen. Mittels *User Role Checks* wird dies gewährleistet, so darf z.B. ein Apotheker nur Zugriff auf elektronische Rezepte, nicht aber auf andere medizinische Dokumente bekommen. Nach erfolgreicher Autorisierung der Services erfolgt die Überprüfung der Benutzerrollen. Das *User Zertifikat* wird ebenfalls beim Aufruf des Web Services mitgeschickt und wiederum mit der lokal konfigurierten Policy verglichen.

3.5 Implementierung mittels Web Service Security

Zur Implementierung der RBAC Konzeptes in Prototyp 1 kommt Web Service Security zum Einsatz, wobei die Autorisierung transparent für das ursprüngliche Web Service eingebunden werden

kann. Policies zum Herstellen des Bezugs zwischen Rolle und Berechtigung werden von jedem Web Service dezentral verwaltet. Dies bringt einen zusätzlichen Sicherheitsgewinn, da kein zentraler Dienst zur Verwaltung der Berechtigungen benötigt wird.

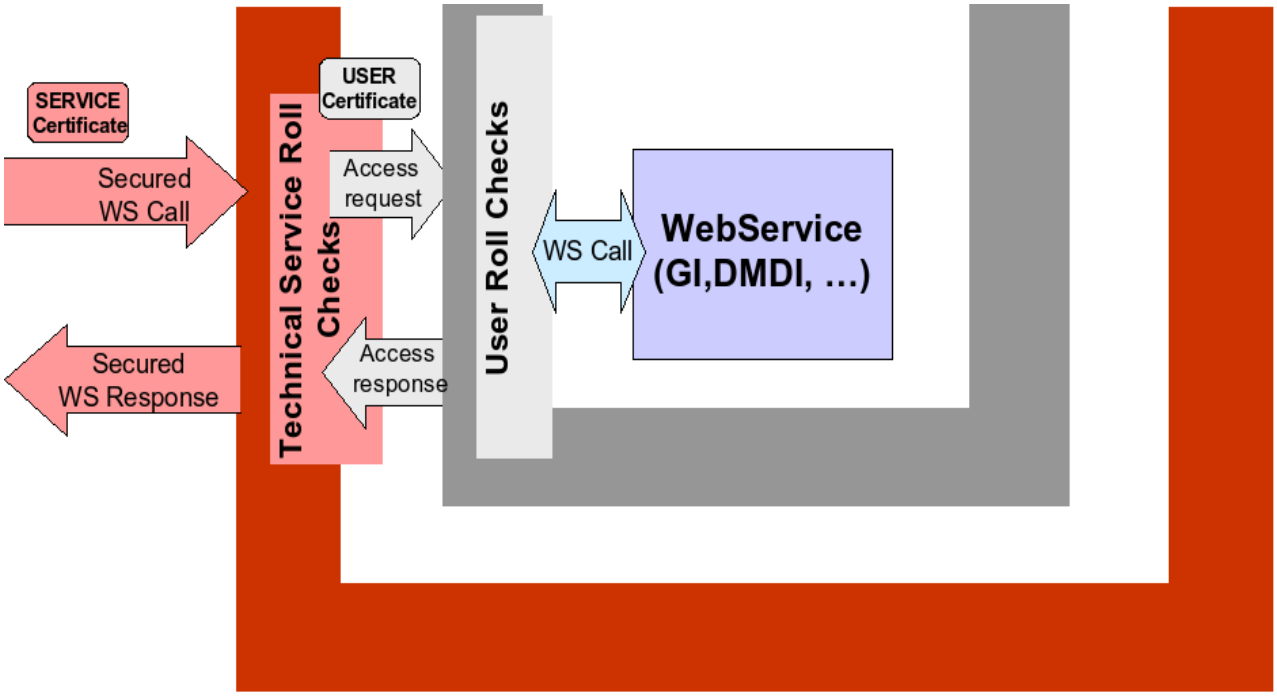

Abbildung 1: Zweistufiges Sicherheitskonzept mittels RBAC. Überprüfung statischer Service Rollen im äußeren Layer. Überprüfung dynamischer User Rollen im Inneren Layer. Nähere Informationen siehe Text.

4.Diskussion

Die Entwicklung der Prototyp Architektur wurde Ende November 2006 abgeschlossen. Zur Zeit erfolgt die Evaluierung inwieweit die funktionalen Anforderungen erfüllt werden. Das RBAC basierte Security Konzept steht dabei nicht im Widerspruch mit den IHE Security Profilen XUA und ATNA. Das RBAC Konzept dient als deren Erweiterung hinsichtlich End-to-End Security. Die Implementierung der Architektur erfolgte gemäß dem IHE XDS Standard, Anpassungen vor allem im Workflow beim Abrufen von Dokumenten waren jedoch nötig um den rechtlichen Anforderungen in Österreich zu entsprechen. GRID Middleware wie z.B. GLOBUS wurde nicht eingesetzt, da die Anforderungen für Medical Data GRIDs nicht erfüllt waren. Die Version 4 des Toolkits bietet jedoch interessante Features für Authentifizierung und Verteilung von Zertifikaten.

Neben noch zu lösenden technischen Problemen, müssen organisatorische und rechtliche Rahmenbedingungen für den produktiven Einsatz einer verteilten elektronischen Gesundheitsakte geschaffen werden. Das RBAC basierte Sicherheitskonzept leistet dabei einen entscheidenden Beitrag, um End-to-End Security zu gewährleisten

5. Referenzen

[1] Maglaveras N, Chouvarda I, Koutkias V, Meletiadis S, Haris K, Balas EA. Information technology can enhance quality in regional health delivery. Methods Inf Med. 2002;41(5):393– 400.

[2] Haux R. Health information systems - past, present, future. Int J Med Inform. 2006 Mar;75(3-4):268–281.

[3] Haux R, Ammenwerth E, Herzog W, Knaup P. Health care in the information society. A prognosis for the year 2013. Int J Med Inform. 2002 Nov;66(1-3):3–21.

[4] IT Infrastructure Technical Framework [homepage on the Internet]. IHE.net; c2006 [cited 2006 Nov 09]. Available from: http://www.ihe.net/Technical_Framework/.

[5] Manca S, Leoni L, Giachetti A, Zanetti G. A virtual grid architecture for medical data using srb. In P. Inchingolo and R. Pozzi-Mucelli (Ed.): EuroPACS - MIR 2004 In The Enlarged.

[6] Schabetsberger T, Ammenwerth E, Goebel G, Lechleitner G, Penz R, Vogl R, et al. What are Functional Requirements of Future Shared Electronic Health Records? In: Engelbrecht R, Geissbuhler A, Lovis C, Mihalas G. European Notes in Medical Informatics (CD-Rom): Connecting Medical Informatics and Bio-Informatics; 2005.

[7] Ferraiolo D, Cugini, J Kuhn, D. Role-Based Access Control (RBAC): Features and Mo tivations. Proceedings of 11th Annual Computer Security Application Conference, pages 11–15, 1995.