MEDINFO 2007
HISA Ltd Australia
© 2007 The authors. All rights reserved.

A Security Infrastructure for Shared Electronic Health Records - Role Based Access Control as IHE XDS Extension towards End-to-End Security

Florian Wozak[a], Elske Ammenwerth[a], Ruth Breu[b], Richard Mair[b], Robert Penz[c], Thomas Schabetsberger[a], Raimund Vogl[c]

[a] *Institute for Health Information Systems, UMIT - University for Health Sciences, Medical Informatics and Technology, Eduard Wallnöfer-Zentrum 1, Hall in Tyrol, Austria Hall in Tyrol, Austria*
[b] *Institute of Computer Science, University of Innsbruck, Technikerstrasse 21a, 6020 Innsbruck, Austria*
[c] *health information technologies tirol GmbH, Leopoldstraße 1/1, Innsbruck, Tyrol, Austria*

Abstract

In an aging society with continuously increasing number of multi-morbid patients rising costs of the health care system are expected. The availability of relevant medical data across institutional boundaries is expected to improve quality and efficiency in health care services. In this work an IHE-XDS compliant architecture for Shared Electronic Health Records with a concept for End-to-End security is described. Therefore a security model with Role Based Access Control mechanism (RBAC) has been designed.

Keywords:

Computerized Medical Records System, community care networks, computer security

Introduction

In an aging society with continuously increasing number of multi-morbid patients rising costs of the health care system are expected. The electronic processing of medical data, which is expected to improve quality and efficiency of health care services [1] will lead to an increasing amount of medical data exchanged across institutional boundaries [2, 3].

A variety of existing standards for Shared Electronic Health Records (SEHRs) have been analyzed and the IHE Cross Enterprise Document Sharing Profile (XDS) turned out to offer a high level of interoperability while providing concrete recommendations for implementation [4]. XDS does not specify the underlying network architecture, nor are security aspects addressed.

End-to-End security, in contrast to Point-to-Point security, allows secured information to be transmitted via intermediate nodes without breaking security. Therefore securing of information, such as encryption and digital signing is handled by communicating applications and not by the network protocol as performed for Point-to-Point security.

According to national and international rules and regulations data security is a vital aspect of SEHRs. Medical Data GRIDs seem to be appropriate to address both, interoperability required by the IHE XDS profile and demands for End-to-End security regulated by the Austrian federal law for health telematics. This approach is currently beeing developed in health@net, a large scale project for trans-regional interconnection of major health care actors in Western Austria (about 700.000 inhabitants, 1600 GPs, 12 hospitals including one University Hospital).

Materials and methods

In an initial step functional requirements for a SEHR have been analyzed [5]. Based on this analysis a technical specification has been elaborated as requirements document. To ensure the highest possible level of security and data protection, functional requirements have been analyzed along with security requirements for trans institutional workflows in a SEHR.

Therefore a methodology known as SECTET is used to develop UML models that specify workflows between the participating partners. A starting point is the document model that defines the basic objects that are managed and exchanged by the system. In parallel a role model is developed that reflects the permissions and capabilities of the users of the system. These models guide through the elicitation of security requirements [6].

IHE – XDS (Cross Enterprise Document Sharing)

The IHE Cross Enterprise Document Sharing Profile (XDS) provides an architectural approach for document sharing in heterogeneous health care environments [4].

At the Document Source medical documents are produced, which are then stored at the Document Repository and made available to the end user (Document Consumer). The Document Registry is for indexing and search functions, the PatientID source provides a unique patient identification.

Medical Data GRIDs

The architecture is designed to be highly scalable and secure, to offer standardized interfaces and provide for interoperability across institutional boundaries. For this

reason an architecture following the blueprint of Medical Data GRIDs, that is an adaptation of Data GRIDs [7] to the requirements of the medical domain, seems to be most appropriate.

Role Based Access Control (RBAC)

Role Based Access Control is a concept for specifying and enforcing enterprise protection policies, where users can be assigned roles and individual roles can be assigned access permissions [8]. RBAC is a concept successfully used in various access control systems.

Architecture

Currently an open source prototype architecture based on the IHE XDS specification is being developed. The architecture and specific modifications necessary to meet legal and organizational requirements are described as follows.

To ensure greatest possible flexibility and scalability, a distributed approach following the above introduced paradigm of Medical Data GRIDs was chosen and implemented using widespread Web service technology. Services are implemented in the Java programming language with Tomcat as application server and Apache Axis as Web service framework.

The core architecture consists of independent services responsible for storing documents and corresponding meta data, security features, unique patient identification and service discovery according to the IHE XDS specification. In Figure 1 the IHE-XDS reference architecture is shown along with the services implemented in the prototype architecture. To guarantee a high level of security beyond simple transport layer security, Role Based Access Control as a security concept has been implemented.

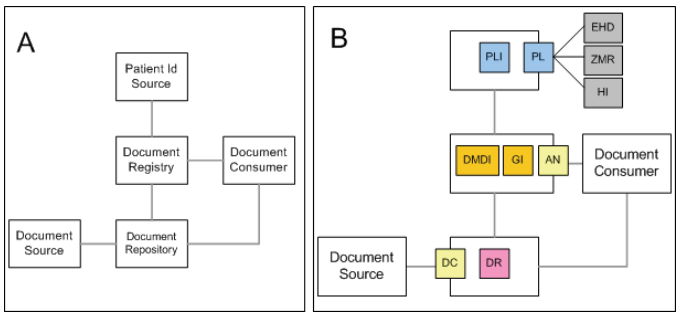

Figure 1: Health@net Architecture based on the IHE-XDS reference architecture. In (A) the IHE-XDS reference architecture is shown. In (B) specific adaptations for the health@net prototype architecture are described. Document Clearing (DC), Document Repository (DR), Document Meta Data Index (DMDI), Global Index (GI), Access Node (AN), Patient Lookup Index (PLI) and Patient Lookup (PL). Governmental services for obtaining patient identification

Core functionality is provided by the three service groups (IHE XDS Actors). Document Repository, Document Registry and PatientID Source. Medical documents remain stored in the organization where they have been produced in the Document Repository (DR). The Document Clearing service (DC) is responsible for converting documents from a proprietary format to the Clinical Document Architecture (CDA) format [9] internally used as data standard for interoperability. Local patient identification is mapped to the internally used unique identification.

The Document Registry service provides functionality for document search, per-document access permissions, a link to the physical location at the Document Repository as well as a service discovery unit. This service group comprises three services: Document Meta Data Index (DMDI), which holds search relevant meta data as well as document based access permissions.

The Global Index (GI) is responsible for finding Meta Data Index services that hold document meta data for a specific patient identified by the unique PatientID. Document consumers are only permitted to access the architecture via a gateway with well defined interfaces, provided by the Access Nodes (AN).

The PatientID Source service group provides for unique patient identification across institutional boundaries, independent form patient's nationality. The Austrian legal situation and the fact that a unique patient identification does no (yet) exist requires different services, partly provided by the Austrian government to be integrated in the architecture.

A Patient Lookup Index (PLI) is used as interface for other services (mostly DC and AN) to obtain a unique patient identification based on demographic data. A Patient

Lookup service (PL) is used to obtain this identifier transparently for the architecture from different governmental person ID sources.

Security Concept: Role Based Access Control (RBAC)

According to functional and technical requirements Shared Electronic Health Records have to fulfill highest possible security and privacy demands. Therefore fine-grained access permissions for all patient related information is required.

Well known information security techniques to ensure confidentiality, integrity, availability and authenticity are mandatory but there are still more domain specific requirements coming from patients, medical professionals or even from both. The following important aspects have been identified and can be found in the list below.

- 4 – eyes – principle (Doctor needs the patients attendance in order to access his health record). Exception: Patient can access and eventually modify his own data. Exception: Emergency access (special logging and informing of the patient).
- Possibility for the owner (patient/citizen) to completely lock/hide certain entries.
- Possibility to delegate time limited access to a doctor and possibility to delegate proxy access to family members.
- Encrypted communication and authentication based on digital certificates (mutual authentication of services).
- Austrian health insurance chip card (e-card) as digital ID-card for authentication with personal health record.

Based on those requirements a hierarchic two level security model has been elaborated as outlined in Figure 2.

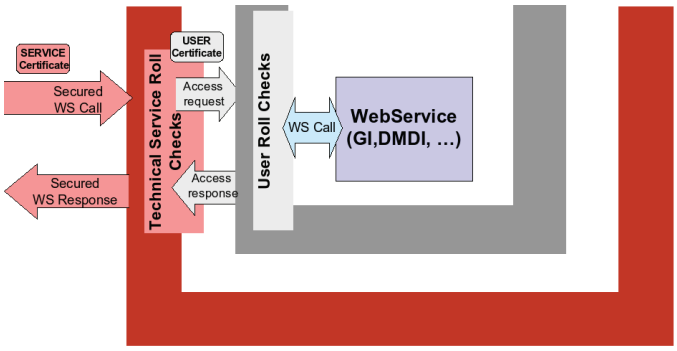

Figure 2 - Two level role check model. In the external level static service roles are checked, in the internal level dynamic user roles. For further details refer to the text.

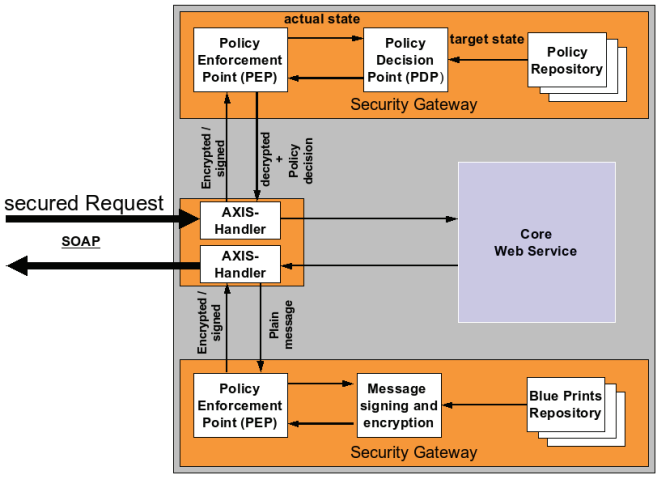

Figure 3 - Policy based security model. The middle part of the figure represents Axis Handler and Core Web Service. Decryption and verification of received messages is shown in the upper part. Encryption and signing of transmitted messages is described in the lower part of the figure. For further details refer to the text.

Level 1: Service role checks:

Each web service has to ensure, that it can only be called by registered and entitled Web services. The calling service has to send a certificate which the called service has to check. Therefore each Web service gets supplied with a service certificate signed by a trusted certification authority and stating out its role. Once a called Web service properly identified the role of the calling service it is compared to the locally configured policies in order to decide whether the call should be permitted or not.

Level 2A: Static user role checks:

After the service role check succeeded, permissions of the user that actually started the request have to be analyzed. As the Electronic Health Record will include different types of documents with different access rules they have to be checked as well. A pharmacist, for example, must not be able to see any discharge letter but, in turn, has to be able to access a patient's prescriptions. Therefore the same role based mechanism as already used in level 1 is applied.

At the time a user account is created, an appropriate user certificate is issued defining the user's profession and effective permissions (assignment procedure of permissions is beyond the scope of this work). When accessing a patient's health record this certificate is checked against the pre-configured policies of the corresponding Web service. For example: In case a user requests access to a patient's prescriptions and the user is assigned the role pharmacists, access will be granted.

Level 2B: Dynamic user role checks:

Furthermore it is important to check dynamic user roles. An authenticated pharmacist, for example, who is correctly trying to access patient's prescriptions should only be permitted to access the information if the consent of the patient is present. Again the same role based check method is applied. In Austria each citizen already has a unique health insurance smart card (e-card) with crypto card functionality. The certificate on this card (and the associated pin-code) can be used to check whether the patient has given his consent while a medical professional is trying to access his health record. Only if the patient's consent can be verified, access will be granted.

In the role based access control mechanism on each level of the security hierarchy actual permissions have to be checked. Therefore each Web service is configured with a set of policies. As the service is called from outside, an inspection is carried out whether the call confirms to the local policies and, only if so, the the requested Web service can be invoked. In case a request does not comply with configured policies the request gets rejected and logged.

For each request a state is extracted which is compared to local policies. If an adequate policy can be found where that the actual state matches the target state, a positive acknowledgment is generated and access is granted.

Implementation using Web Service Security

The security infrastructure is being implemented using Web Service Security Extensions. The Apache Web service framework Axis permits so called “Axis handlers” to be registered with the framework in order to extend it's functionality. In the architecture security functions are integrated via Axis Handlers.

This concept does not require Web services to be designed with security aspects in mind. The RBAC based security infrastructure is pluggable via the Axis handler.

The security gateway depicted in Figure 3 uses policies to map roles to access permissions. The figure describes how received data are decrypted and validated (upper part) and how send data are encrypted and signed (lower part).

Service roles and user roles are defined in the Policy Repository and can be changed dynamically. The procession of a received SOAP message is initially intercepted by the Axis handler and forwarded to the Policy Enforcement Point (PEP).

The actual state (e.g. current role of calling user and requested action) is then extracted and transmitted to the Policy Decision Point (PDP). The PDP searches for a policy in the Policy Repository which defines the requested action as permitted for the respective user. If a corresponding policy is found access is granted, the message decrypted, verified and returned to the Axis handler, which finally forwards the call to the original Web service.

Transmitted messages are processed in a similar workflow. The message is intercepted by the Axis handler and forwarded to the PEP. At this stage the message is signed and encrypted for the receiving service according to the policies in the Blue Print Repository. The Axis handler, as a last step, transmits the secured message to its destination.

The security model described in Figure 3 is the technical implementation of the two level role check model described in Figure 2.

Discussion and outlook

Currently a prototype implementation of the IHE-XDS compliant architecture with the role based access control methodology has started. The development of the network architecture follows an iterative approach which we have chosen to gradually adopt the architecture to evolving requirements of the major players. In this article the first prototype architecture is described including role and context based authorization system to provide for End-to-End security. A prototype is currently being released, which will demonstrate the conformance of the security mechanism to the above mentioned requirements.

The IHE IT Infrastructure Technical Framework [4] does offer Profiles for security, such as the Audit Trail and Node Authentication Profile (ATNA) and the Cross Enterprise User Authentication Profile (XUA). The first covers service authentication only on transport layer (without End-to-End focus), audit and centralized secure logging. The latter covers secure user authentication in trans-institutional context. XUA is not final yet, but the introduced RBAC based approach is expected to be seamlessly integrated in the XUA Profile.

Motivated by the above mentioned drawbacks (XUA is not final and ATNA only provides Point-to-Point and not End-to-End security) the RBAC based security infrastructure has been developed. Point-to-Point security allows secure information to be transferred between precisely two networked nodes. End-to-End security, however allows secure information, dedicated for a specific application, to be transmitted via an arbitrary number of intermediate nodes.

Currently static service role checks (level 1) and static user role checks (level 2A) are implemented. For dynamic user role checks (level 2B) further research concerning the application of attribute certificates is needed. Level 2B checks are expected to be integrated in the next software release, scheduled for the summer 2007.

Although the architecture is based on Medical Data GRIDs, in the prototype phase GRID middleware such as the GLOBUS Toolkit 4 [10] have not been used because requirements for Medical Data GRIDs, as outlined above, are currently not satisfactorily covered. Nevertheless GRID middleware provides interesting features particularly in the field of authentication and distribution of digital certificates. The adaptation of those concepts is planned for the next prototype.

The implementation closely sticks to the IHE XDS specification. Changes concerning the patient identification have become necessary to reflect the requirements of the Austrian federal law for health telematics. However, before IHE XDS based Shared Electronic Health Records can be used in production environment several technical and organizational aspect have to be solved.

References

[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] 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.

[6] Hafner M, Breu R, Breu M, Nowak A. Modelling Inter-organizational Workow Security in a Peer-to-Peer Environment. In: R. Bilof (Ed.): Proceedings of the 2005 IEEE International Conference on Web Services. IEEE Conference Publishing Services; 2005. p. 533–540.

[7] 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.

[8] 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.

[9] HL7 Clinical Document Architecture, Release 2.0 [homepage on the Internet]. Ann Arbor, MI: Health Level Seven, Inc.; c2006 updated 2006 Sep 27; cited 2006 Nov 09]. Available from: http://www.hl7.org/v3ballot/html/infrastructure/cda/cda.htm.

[10] Foster I. Globus Toolkit Version 4: Software for Service-Oriented Systems. In: IFIP International Conference on Network and Parallel Computing. Springer-Verlag LNCS 3779; 2005. p. 2–13.

Address for correspondence

Dipl.Ing.(FH) Florian Wozak, Msc
Institute for Health Information Systems
UMIT - University for Health Sciences, Medical Informatics and TechnologyEduard Wallnöfer-Zentrum 1
6060 Hall in Tirol Austriamail: florian.wozak@umit.at