# Privacy and Access Control for IHE-Based Systems*

Basel Katt[1], Ruth Breu[1], Micahel Hafner[1],
Thomas Schabetsberger[2], Richard Mair[2], and Florian Wozak[2]

[1] University of Innsbruck, Austria
{basel.katt,ruth.breu,m.hafner}@uibk.ac.at
[2] Health@net (CEMIT), Austria
{thomas.schabetsberger,richard.mair,
florian.wozak}@healthatnat.at

**Abstract.** Electronic Health Record (EHR) is the heart element of any e-health system, which aims at improving the quality and efficiency of healthcare through the use of information and communication technologies. The sensitivity of the data contained in the health record poses a great challenge to security. In this paper we propose a security architecture for EHR systems that are conform with IHE profiles. In this architecture we are tackling the problems of access control and privacy. Furthermore, a prototypical implementation of the proposed model is presented.

## 1 Introduction

The Electronic Health Record (EHR) represents the lifelong, time and location independent collection of all healthcare related information for a citizen stored in electronic form [8]. To realize EHR systems two distinct approaches can be applied: either a central management system can be used to store the whole healthcare data in one repository, or a distributed approach. In the distributed approach healthcare data will be stored within the internal information system of the health institution that creates them. The IHE initiative has adopted the second approach and developed integration profiles that define how current related standards can be implemented to realize distributed EHR systems.

This work is an approach to tackle access control and privacy issues in distributed EHR systems that leverage IHE profiles. We are proposing a security architecture and a prototypical implementation in the context of the Health@net project. The Health@net project [8] develops the core components of an eHealth system in accordance with IHE integration profiles.

The rest of the paper is organized as follows: in section 2 we present related work. Brief background is introduced in section 3. The security and privacy requirements are defined in section 4 and our proposed security architecture is discussed in section 5. Finally we present our prototypical implementation in section 6 before we conclude in section 7.

* eHealth 2008, September 8th and 9th, 2008, City University, London EC1.

D. Weerasinghe (Ed.): eHealth 2008, LNICST 1, pp. 145–153, 2009.

## 2 Related Work

Issues around privacy and access control in ehealth systems have been covered extensively in the literature [3, 6, 9, 21] and security requirements were defined for ehealth systems [5, 7]. Compared to these work, we have identified security requirements in special cases of distributed HER in the context of systems leverage IHE profiles. Furthermore, we propose a suitable security model that fits the adapted system architecture.

The only related work, to our knowledge, that consider security and privacy in IHE conform systems are done by Namli et al. in [18, 19]. They propose an approach to realize IHE privacy and authentication profiles using XACML and SAML. While we tackle the privacy issue as well, we identified the drawbacks of the privacy profile and the challenges related to the distributed nature of EHR in IHE systems. Accordingly, we propose a general access control and privacy related security model that goes beyond the capabilities of the proposed IHE profile(s). Within this model we offer a suitable solution for the identified drawbacks.

## 3 Background

### 3.1 Integrating the Healthcare Enterprise (IHE)

To realize the goal of EHR, the *Integration the Healthcare Enterprises* (IHE) initiative was launched in 1999 [11]. IHE defines *Integration Profiles* for a variety of systems [14]. Ten of the integration profiles are assigned to the IT infrastructure technical framework. These profiles specify the interactions and the interfaces between various healthcare applications and the messages exchanged using well known standards such as HL7 and DICOM. To address the interoperability problem in sharing electronic healthcare records, Cross Enterprise Document Sharing (XDS) profile was developed. The XDS IHE integration profile [10] assumes that these enterprises belong to one or more affinity domains. A *clinical affinity domain* is a group of healthcare enterprises that have agreed to work together using a common set of policies and share a common infrastructure. This profile does not define specific policies and business rules, however it was designed to accommodate a wide range of such policies to facilitate the deployment of standards-based infrastructures for sharing patient documents. This is managed through introducing a registry/repository architecture for storing the medical information and their metadata. Figure 1 shows the XDS-IHE repository/registry architecture diagram. The following distinct actors with separate responsibilities can be identified:

- The *Document Repository* is responsible for storing documents in a transparent, secure, reliable and persistent manner and responding to document retrieval requests.
- The *Document Registry* is responsible for storing meta information about those documents so that the documents can be easily found, selected and retrieved.

- The *Document Source* is the producer and publisher of documents. It is responsible for sending documents to the *Document Repository* entity and providing the *Document Registry* with the metadata.
- The *Document Consumer* queries the *Document Registry* for documents meeting certain criteria, and retrieves selected documents from one or more Document Repositories.

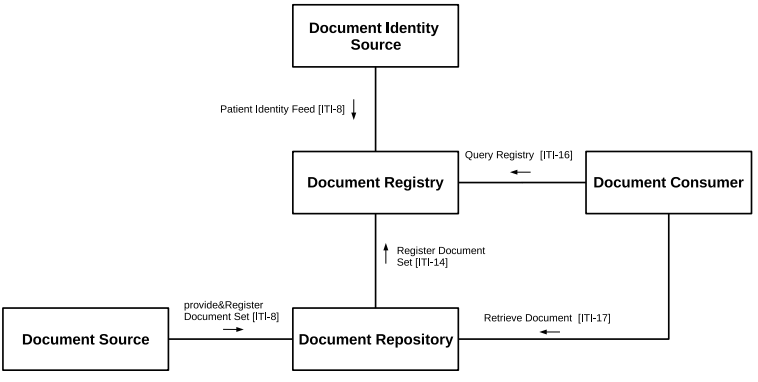


**Fig. 1.** Cross-Enterprise Document Sharing diagram

### 3.2 Access Control

According to the architecture proposed by ISO [1], the access control enforcement engine consists of two main functions: the *Policy Enforcement Point (PEP)*, and the *Policy Decision Point (PDP)*. An access request is received by the PEP. PEP queries the PDP about the access decision of the received request. According to the decision rendered by the decision point the PEP permits or denies the access to the target.

Different standards and policy languages have adopted this architecture and extended it with some additional functionalities. For example, the XACML based enforcement engine in [17] includes additionally a *Policy Administration Point (PAP)* and a *Policy Information Point (PIP)*. PAP is the entity that creates, stores, distributes and manages policies. PIP on the other hand is considered as the source of information needed to make decisions.

## 4 Security and Privacy Requirement

Based on access control and privacy requirements mentioned in IHE profiles [12, 13], the data protection regulation in Austria[1] and previous scientific study of security requirements in eHealth systems [8] we can summarize the following main requirements:

[1] http://www.ris2.bka.gv.at/Bund/

1. In the electronic Healthcare data exchange, each healthcare provider must be assigned a specific role which must be authenticated using an electronic certificate (e.g stored in the e-card).
2. Healthcare providers are only allowed to access healthcare documents they need according to the roles they were assigned. The mapping rules between different roles in healthcare paradigm and document types they require were formulated by law- and medical- experts in a set of guidelines called *Rule-Base* For example a user of the role *pharmacist* requires only documents of type *prescription*.
3. Doctors are allowed to access the healthcare documents that they create.
4. The identifiable healthcare data for specific patient is only allowed to be used under the consent of the patient for specific purpose.
5. The patient should be able to access all documents in his personal healthcare record.
6. Additionally to the general *Rule-Base* rules, the patient should be able to control the access to his personal record, i.e. defining who is allowed to access all or parts of the documents in the record, like the family doctor.

## 5 Design Model

The distributed nature of EHR and policy language requirements pose some challenges to the design of the access control system for IHE systems:

1. Two different kinds of rules must be enforced by each request to the health record: The rules representing the *Rule-Base* guidelines and the patient's personal preferences.
2. The EHR must be considered as one virtual single resource when users with full rights are accessing it. For example, if the patient is trying to get access to the complete EHR, checking his right to use each single document alone means a great overhead. Hence the access right in this case must be checked once and applied for all documents.
3. Requests to use a set of documents of the EHR for users without full rights must be processed once by the PDP. Patient's EHR consists of various document, each is considered one resource object. Nevertheless, decisions for this set of documents must be taken only once to avoid the resulting overhead.

### 5.1 Policy Types

As mentioned in section 4, two kinds of rules must be enforced by the access control system: the rules that represent the *Rule-Base* guidelines and those defined by the patient representing his personal preferences. Consequently, the system must support two kinds of security policies: standard access control and privacy policies.

*Rule-Base* rules define the rights each role in the healthcare paradigm should be assigned to: Role Based Access Control (RBAC) model [20] is to be adopted for the standard policies [3]. On the other hand, the rules that the patient defines to allow specific users to access his record for specific purposes is a privacy policy. Privacy in

the healthcare domain and its policy characteristics have been analyzed in the literature [21] and defined by the OECD guidelines [2]. One of the most important elements of a privacy policy is the *Purpose*. It states the purposes for which the information will be used as specified by the patient.

### 5.2 Decision Making Process

Decision making process is divided into two phases: the first phase will be initialized from the requesting domain and considers EHR as one resource. The second will be initialized from the different responding domains and considers each document in the EHR as single resources.

- *Phase one*: when users with full access rights (like the patient himself or the trusted family doctor) are trying to access the whole EHR, then processing the request based on single documents and in various affinity domains causes an avoidable overhead. This overhead can be reduced by (1) launching the decision process from the requesting side, before the request is distributed to the various responding affinity domains and (2) conceiving the EHR as one virtual resource by the PDP. Thus, we introduce the first decision making phase at the requesting side considering the EHR as one single resource.
- *Phase two*: is useful for normal users with no full access rights (like the specialist in the motivating example). When such users try to access multiple documents of the EHR, PEPs in the responding domains should make multiple decision requests for multiple resources. Consequently the PDP will make multiple decisions. To meet this challenge, access control system must support single decision requests with multiple resources. Thus the overhead caused by accessing multiple resources can be alleviated. In this case all requests for the whole EHR or multiple documents will be processed only once by the *PDP* and the decision(s) will be rendered once document-wise. The decisions of this phase will be called in this paper *Multiple Decision*.

### 5.3 Security Architecture

Considering the dual policies used, the multiple-resource request supported and the two phase decision making process we conclude the security architecture depicted in Figure 2.

It shows our proposed security architecture with a two-step decision making process and two types of policies to meet the security requirements illustrated in section 4 and the challenges aforementioned.

First of all, the *Enforcement Point* in the requesting side *(Req_PEP)* sends a decision request to the central PDP. The PDP considers the whole EHR as one virtual resource, and checks whether the user requesting the EHR is allowed to get access to it as a whole or not. In case of a *permit* response, the *Req_PEP* asserts the decision to all responding domains and no further checks are carried out. In case the requesting subject is allowed only to access parts of the EHR, then the *Req_PEP* will forward the request to the responding domains. The *Enforcement Point* of each responding domain sends a muli-resource decision requests to the PDP. In both decision steps the PDP gets the corresponding policies of both types from the *Administration Point* (PAP).

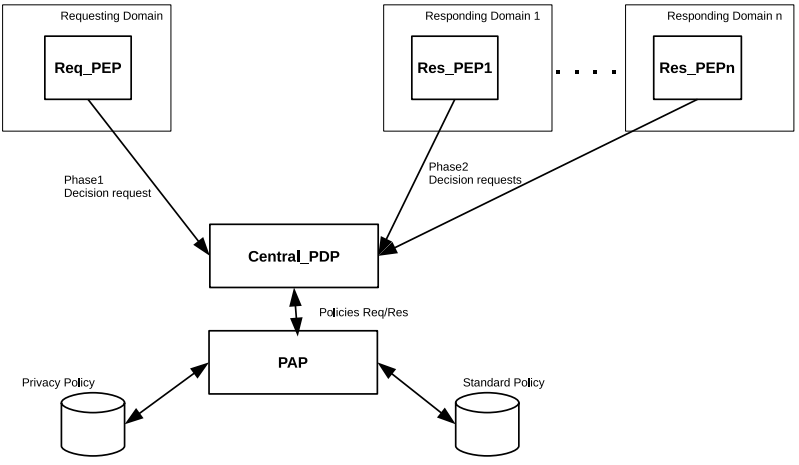


**Fig. 2.** Design model of the security architecture

## 6 Prototypical Implementation

In this section we present a practical implementation of our security architecture for systems leverages IHE profiles (especially XDS profile) using XACML as a policy language.

Figure 3 shows the prototypical implementation architecture. The system consists of one requesting affinity domain (A) (represents to the institution from where the user is making the access request) and multiple responding domains (B and C), where the documents of specific patient's EHR are stored. We are assuming the general case where the requesting and responding domains are different. When the user sends a request through the *Document Consumer* in the requesting domain the following steps will be executed:

1. First of all the user will be authenticated using the *Identity\&Attribute Provider (IP)*. The IP authenticates the user, checks his identity using the e-card system in Austria[2], and finds out his assigned role.
2. The checked identity and the assigned role will be rendered as SAML attribute assertion to the *Document Consumer*.
3. After being authenticated the enforcement point of the *Document Consumer* launches the first phase of the decision making process. The PEP sends a decision request to the PDP at the central administration entity.
4. The PDP in this phase checks whether the user has a full right to access the EHR as one resource. This is done by requesting the corresponding privacy policy of the patient and search for permit rules with target of the form

```
<subject category=access-subject> userx_id </subject>
<subejct category=owner-subject> patientx_id <subject>
<resouce> any </resource>
<actoin> read/write </action>
```

[2] http://www.chipkarte.at

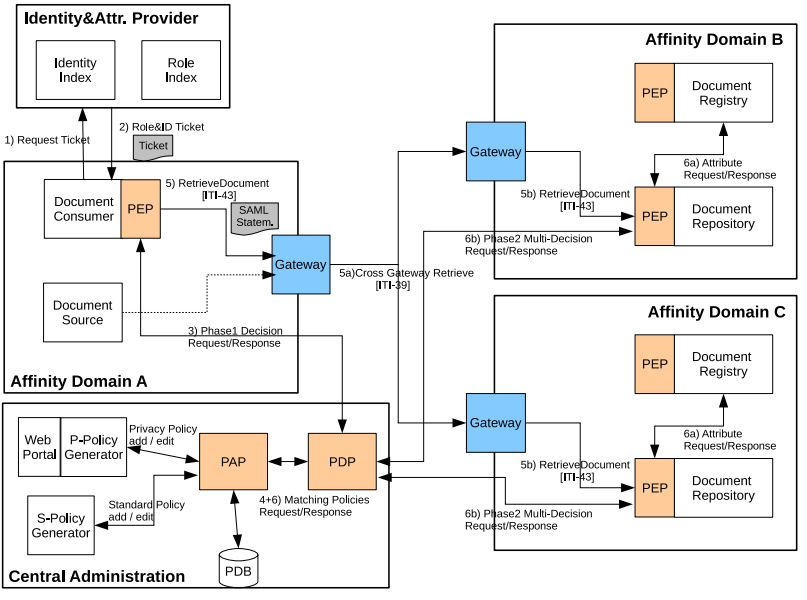


**Fig. 3.** Security Architecture

This rule shows whether the user *userx_id* is allowed to read or write all documents of the patient with the Id *patientx_id*.

5. If the decision is permit, the user (*userx*) is allowed to read/write the complete EHR of the patient (*patientx*). In this case the requesting PEP will forward the request to the affinity domains containing the EHR documents of the patient with a SAML decision statement. The PEPs in the responding domains will enforce the decision contained in the SAML assertion, i.e. permit access to all documents belonging to the patient *patientx*. Hence, no further checks are carried out. However, if the response contains a *NotApplicable* decision, which means that this rule is not applicable and the user has no full right. Therefore finer decision must be made on the document basis.
6. For finer decision, the requesting PEP forwards the request to the responding domains with attribute SAML statement containing the *Id* and the *role* of the requesting user. Consequently, all PEPs attached to the corresponding document repositories will launch the second phase of the decision making. This is done by sending *multi-resource* requests to the central PDP[4]. The PDP in turn fetches the related standard and privacy policies from the *Policy Administration Point (PAP)* and makes the multi-decision accordingly. Finally the PDP renders the response(s) to the responding PEPs to enforce them.

The complexity of the policies used requires security experts to create such policies. This raises serious difficulties in using these policies in real application, where normal users, like the patient, or non-security experts, like the system

administrators, have to generate the policies. To lessen the burden of creating and handling complex XACML policies, we are proposing two kinds of policy generators in our prototype. *Details about the policy generators are described in an accompanying paper [15].*

## 7 Conclusion and Future Work

In this paper we present our work to develop and implement a security architecture that tackles access control and privacy requirements of distributed EHR applications in the context of systems leveraging IHE profiles. Furthermore a prototypical implementation is developed and tested in a real eHealth, IHE conform application.

The documents that are released to doctors are no longer monitored and controlled. However, some security requirements demands the document be monitored and controlled [16]. To tackle this problem usage control and obligation models were proposed. These models are to be investigated in the healthcare domain in the future.

## References

1. [ACF]ITU-T Rec X.812 – ISO/IEC 10181-3:1996. Security frameworks for open systems: Access control framework. Technical report (1995)(1996)
2. OECD: Guidelines on the protection of privacy and transborder flows of personal data, http://www.oecd.org/document/18/03343en_2649_34255_1815186_1_1_1_1.00&&en-USS_01DBC.html
3. Ferreira, L.A.A., Cruz-Correia, R., Chadwick, D.: Access control: How can it improve patients healthcare? (2007)
4. Anderson, A.: Multiple resource profile of xacml v2.0 (2005), http://docs.oasisopen.org/xacml/2.0/accesscontrol-xacml-2.0-mult-profile-spec-os.pdf
5. Anderson, R.J.: Security in clinical systems (1996)
6. Blobel, B.: Authorization and access control for electronic health record systems. International Journal of Medical Informatics (2004)
7. Blobel, B., Roger-France, F.: A systematic approach for analysis and design of secure healthcare systems. International Journal of Medical Informatics (2001)
8. Hafner, M., Mair, R., Breu, R., Agreiter, B., Unterthiner, S., Schabetsberger, T.: Health@net. die verteilte elektronische gesundheitsakte- eine fallstudie in modell-getriebenem security engineering. IT-Sicherheitskongress des BSI (2007)
9. Hu, J., Weaver, A.C.: A dynamic, context-aware security infrastructure for distributed healthcare applications. In: Proceedings of the first workshop on pervasive privacy security, privacy, and trust (2004)
10. IHE Integrating the Healthcare Enterprise. It infrastructure technical framework- cross enterprise document sharing (xds). Technical report (2004)
11. IHE Integrating the Healthcare Enterprise. Changing the way healthcare connects.Technical report (2006)
12. IHE Integrating the Healthcare Enterprise. Ihe it infrastructure white paper- hie security and privacy through ihe. Technical report (2007)
13. IHE Integrating the Healthcare Enterprise. It infrastructure technical framework- basic patient privacy concents (bppc). Technical report (2007)

14. IHE Integrating the Healthcare Enterprise. It infrastructure technical framework vol.1 (iti tf-1) integration profiles. Technical report (2007)
15. Katt, B., Breu, R., Hafner, M.: Model-driven policy framework for usage control based privacy (to appear)
16. Katt, B., Zhang, X., Breu, R., Hafner, M., Seifert, J.-P.: A general obligation model and continuity enhanced policy enforcement engine for usage control. SACMAT (2008)
17. Moses, T.: extensible access control markup language (xacml) version 2.0 (2005), http://docs.oasisopen.org/xacml/2.0/accesscontrol-xacml-2.0-core-spec-os.pdf
18. Namli, T., Dogac, A.: Implementation experiences on ihe xua and bppc. Technical report, Software Research and Development Center Middle East Technical University (2006)
19. Namli, T., Dogac, A.: Using SAML and XACML for Web Service Security and Privacy, ch. 8, pp. 183–206. Idea Group Publishing (2008)
20. Sandhu, R.: Role based access control models. IEEE Computer 29(2), 38–47 (1996)
21. Yee, G., Korba, L., Song, R.: Ensuring privacy for e-health services. In: Proceedings of The First International Conference on Availability, Reliability and Security (ARES 2006) (2006)