AUTOMATING AUTHORIZATION PROPAGATION PROCESS IN PERSONAL HEALTH RECORDS

Vassiliki Koufi, Flora Malamateniou and George Vassilacopoulos
Department of Digital Systems, University of Piraeus, 80, Karaoli & Dimitriou Str., Piraeus 18534, Greece

Keywords: Personal health records, Information availability, Access control, Emergency, Authorization propagation.

Abstract: Traditionally patient records are generated, maintained and controlled by the individual health care providers where the patient has received care. This results in fragmented bits of data stored in diverse information systems which, in many cases, are not interoperable. Hence, a complete picture of a person's healthcare record cannot be obtained when and where needed. A solution to this problem can be provided by personal health records (PHR), that is electronic health records (EHR) whose architectures are based on the fundamental assumptions that the complete records are centrally stored and that each patient retains authority over access to any portion of his/her record. This paper deals with a particular security issue arising in PHRs which is concerned with the process of granting (revoking) authorization to (from) healthcare professionals without the patient's involvement. This security issue is particularly important in managing emergency cases. To deal with this problem, authorization propagation process is automated by means of context-aware technology, which is used to regulate user access to data via a fine-grained access control mechanism.

1 INTRODUCTION

Throughout their lives individuals receive care in different parts of the health care system. This results in patient health data being scattered around disparate and geographically dispersed information systems hosted by different healthcare providers (Koufi and Vassilacopoulos, 2008;Tang, Ash, Bates, Overhage and Sands, 2006). The lack of interoperability among these systems impedes optimal care as it leads to unavailability of important information regarding patient health status when this is mostly needed (e.g. in case of an emergency).

Recently there has been a remarkable upsurge in activity surrounding the adoption of Personal Health Record (PHR) systems for patients (Tang, Ash, Bates, Overhage and Sands, 2006). A PHR is a consumer-centric approach to making comprehensive electronic medical records (EHRs) available at any point of care while fully protecting patient privacy (Lauer, 2009). Unlike traditional EHRs which are based on the 'fetch and show' model, PHRs' architectures are based on the fundamental assumptions that the complete records are held on a central repository and that each patient retains authority over access to any portion of his/her record (Lauer, 2009; Wiljer, Urowitz, Apatu, DeLenardo, Eysenbach, Harth, Pai, Leonard, 2008). Thus an entire class of interoperability is eliminated since the system of storing and retrieving essential patient data is no longer fragmented. Hence, quality and safety of patient care is enhanced by providing patients and health professionals with relevant and timely information while ensuring protection and confidentiality of personal data.

Providing patients with access to their electronic health records offers great promise to improve patient health and satisfaction with their care, as well as to improve professional and organizational approaches to health care (Wiljer, Urowitz, Apatu, DeLenardo, Eysenbach, Harth, Pai and Leonard, 2008). Although many benefits have been identified, there are many questions about best practices for the implementation of PHR systems (Wiljer, Urowitz, Apatu, DeLenardo, Eysenbach, Harth, Pai and Leonard, 2008). A number of these questions are related to security issues arising in PHR systems.

As any other EHR system, PHR systems require stringent privacy protections to prevent unauthorized access or use (Yasnoff, 2008; Comini, Mazzu and Scalvini, 2008; Win, Susilo and Mu, 2006). Most PHR platforms currently deployed (e.g. Microsoft

Koufi V., Malamateniou F. and Vassilacopoulos G. (2010).
AUTOMATING AUTHORIZATION PROPAGATION PROCESS IN PERSONAL HEALTH RECORDS.
In *Proceedings of the Third International Conference on Health Informatics*, pages 82-89
DOI: 10.5220/0002747200820089

HealthVault, ICW LifeSensor) meet these requirements by assigning the patient with the responsibility of granting access to information comprising his/her health record while access to important information (e.g. blood type, allergies etc) is provided to medical staff in case of an emergency by means of an emergency data set. Although this information is valuable while providing first aid to the patient, a more comprehensive view of the his/her health data is required by the medical staff upon arrival to the emergency department of a hospital.

This paper deals with the particular security issue arising in PHR systems which is concerned with the process of granting (revoking) authorization to (from) healthcare professionals without the patient's involvement. This security issue is particularly important in managing emergency cases. To deal with this problem, authorization propagation process is automated by means of context-aware technology, which is used to regulate user access to data via a fine-grained access control mechanism. The latter is a role-based, context-aware access control mechanism that incorporates the advantages of broad, role-based permission assignment and administration across object types, as in role-based access control (RBAC) (National Institute of Standards and Technology, 2009), and yet provides the flexibility for automatically adjusting access permissions on a patient's PHR on the occurrence of unpredictable events (e.g. emergency case).

2 RELATED WORK

During the last few years, there has been a growing interest in the utilization of PHR systems as both patients and healthcare organizations realized that their use may entail a number of benefits, such as better access to information, increased patient satisfaction and continuity of care (Tang, Ash, Bates, Overhage and Sands, 2006; Wiljer, Urowitz, Apatu, DeLenardo, Eysenbach, Harth, Pai, Leonard, 2008). However, certain barriers to the integration of PHR systems to the clinical practice have been identified, most of them related to security issues (Tang, Ash, Bates, Overhage and Sands, 2006; Wiljer, Urowitz, Apatu, DeLenardo, Eysenbach, Harth, Pai, Leonard, 2008). In recognition of these barriers, a number of mechanisms have been developed in an attempt to address several issues mostly regarding access control over the health data comprising a PHR (Røstad and Nytrø, 2008; Win, Susilo and Mu, 2006; Comini, Mazzu and Scalvini, 2008.). Some of them are concerned with the provision of access to important healthcare information in case of an emergency.

In Case of Emergency Personal Health Record (icePHR) (Metavante, 2009) and My Personal Health Record (myPHR) (My Personal Health Record, 2009) are applications which, among others, ensure that life saving information is available when most needed (i.e. in case of an emergency). To this end, they provide patients with the ability to upload important health information and then print their own emergency card with information on how to access their own unique, secure web page with this emergency information. However, they don't provide mechanisms for ensuring instant availability of a complete copy of a patient's record to the medical staff treating him/her without the patient's involvement.

The system architecture proposed in this paper utilizes agent technology in an attempt to automate authorization propagation process in cases that a patient in incapable of being involved in this process. To this end, a context-aware access control mechanism has been developed which is triggered when appropriate in order to derive and grant the set of authorizations needed for the treatment of a patient.

3 MOTIVATING SCENARIO

The basic motivation for this research stems from our involvement in a recent project concerned with designing and implementing a PHR system for the provision of data access at any point of care while fully protecting privacy. This involves providing access to the appropriate people, based on patient wishes, but also granting access to the patient's data in cases where his/her involvement in the authorization propagation process is not feasible. The stringent security needs of the system, where sensitive patient information is used, motivated this work and provided some of the background supportive information for developing the prototype presented in this paper.

Suppose a healthcare delivery situation that takes place within a health district where an individual is transferred to a hospital's emergency department (ED). Upon arrival to the ED, the individual is registered as an emergency patient and undergoes a brief triage in order for the nature and severity of his/her illness to be determined. If his/her illness or injury is considered to be serious he/she is seen by a physician more rapidly than the patients with less severe symptoms or injuries. After initial assessment and treatment, the patients is either admitted to the hospital (e.g. to a clinical department or the Intensive Care Unit - ICU), stabilized and transferred to another hospital for various reasons, or discharged (Wikipedia, 2009).

Typically, a health district consists of one district general hospital (DGH) and a number of peripheral hospitals and health centers.

As many emergency department visits are unplanned and urgent, there is a need to ensure that information regarding the longitudinal patient health condition (e.g., problems, allergies, medications, diagnoses, recent procedures, recent laboratory tests) is conveyed to ED physicians automatically upon registration of a patient to an ED. Thus, inefficiencies in care, in the form of redundant testing, care delays, and less-effective treatments prescribed are eliminated and quality of care is enhanced.

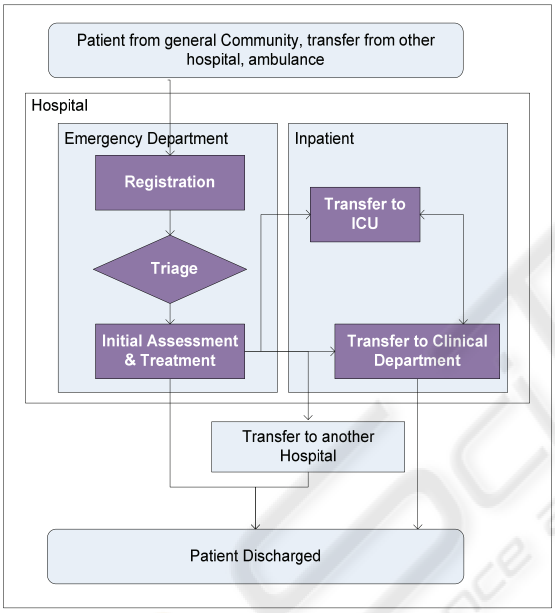
Patient from general Community, transfer from other hospital, ambulance
Hospital
Emergency Department
Inpatient
Registration
Triage
Transfer to ICU
Initial Assessment & Treatment
Transfer to Clinical Department
Transfer to another Hospital
Patient Discharged

Figure 1: Patient Flow.

Figure 1 shows an indicative high-level view of the patient flow from the time he arrives at a hospital's emergency department to the time he is discharged. Some of the roles participating in the patient's treatment are physician, nurse, physician assistant (PA), nurse practitioner with specialized training in emergency medicine and in house Paramedics and other support staff.

From an authorization perspective, the following two requirements are of interest here.

- Data access - A role holder should be allowed to exercise a dynamically determined set of permissions on certain data objects only. For example, a patient's personal physician, if authorized by the patient himself, is allowed to read certain parts of his/her medical record and to update it.
- Permission propagation - Some role holders should receive additional permissions on certain data objects in order to effectively treat the patient but these permissions should be revoked upon patient discharge. For example, for forming an appropriate plan of care, an ED physician should receive the permission to read the complete record of a patient but he/she should not be allowed to retain this permission after the patient has been discharged.

The above requirements suggest that certain data access permissions of the medical staff participating in a patient's treatment may change without the patient's intervention depending on the context (e.g. in the case that an individual is registered as an emergency patient). Moreover, contextual information, such as time and location of attempted access, can influence authorization decisions on certain data objects comprising a patient's PHR. This enables a more flexible and precise access control policy specification that satisfies the least privilege principle by incorporating the advantages of having broad, role-based permissions across data object types, like RBAC, yet enhanced with the ability to simultaneously support the following features: (a) predicate-based access control, limiting user access to specific data objects, and (b) a permission propagation function to specific role holders in certain circumstances.

4 SYSTEM ARCHITECTURE

The prototype system described here facilitates access to comprehensive patient information which is stored in a central repository. In this environment, a robust security framework is in place in order to ensure that health information follow patients throughout their care in a secure manner and that comprehensive information is made available to appropriate people when this is mostly needed (e.g. in case of an emergency) without the patient's involvement. Figure 2 shows a high-level system architecture, which is described by a three-tier model, comprising of the terminal station used by the medical staff at the department where the patient is being treated (e.g. ED, ICU etc), the PHR

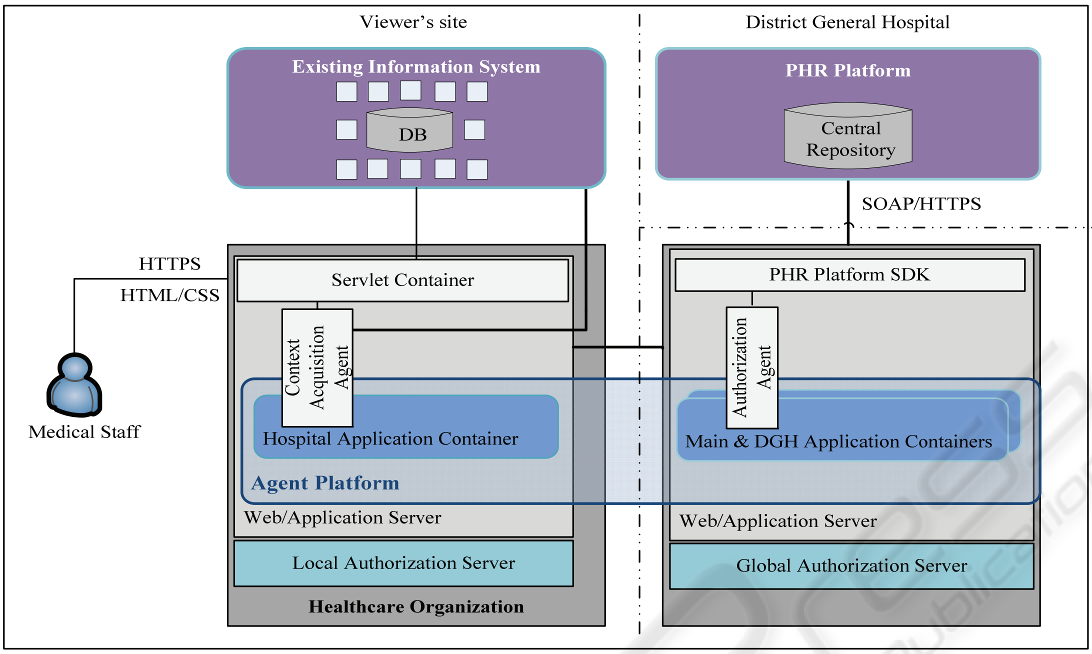

Figure 2: System Architecture.

platform and the application accessing the PHR platform.

The first tier is the terminal station used by the medical staff treating the patient (e.g. physician, nurse etc.). The terminal contains an HTTP(S)-based client, which is the terminal's web browser and provides user interaction with the system.

The second tier of the system architecture is the platform used for the implementation of the PHR system. This supports both patients in actively managing their own health and the medical staff (e.g. physicians) by ensuring the quick and secure availability of a patient's health data such as diagnosis, therapy and prescription data. In such a PHR system access authorization is exclusively granted by the owner (patient) of the record or by a "gatekeeper" he/she assigns (e.g. a relative) (ICW eHealth Framework, 2009). Different read and write permissions can be granted to and be withdrawn from the various users at any time through a terminal station.

The third tier is the application which is distributed among several hosts residing at the DGH and the other healthcare institutions. The infrastructure of this tier consists of the following components:

- *PHR Platform SDK*: It is used for the simple integration of our application into the PHR infrastructure. It provides an Application Programming Interface (API) which can be accessed from JSP/Servlet pages.
- *Agent Platform*: It is the software used for the implementation of the agents which realize the automation of the authorization propagation process in order to support healthcare professionals and frontline staff at the point of care by ensuring instant availability of the complete copy of a patient's medical record.
- *Servlet Container*: It provides a servlet container that hosts and manages the servlets delivering the system functionality. Essentially these servlets provide a web-based front end to the PHR system.
- *Web/Application Server*: It provides the hosting environment to the aforementioned components.

All web transactions are executed under the Secure Socket Layer (SSL) via HTTPS. In addition, security in communication among the agents of the agent platform is ensured by setting up a secure, confidential and mutually authenticated, connection amongst containers of the agent platform by leveraging TLS/SSL support provided by Java (Java Agent Development Framework, 2008).

5 SECURITY ARCHITECTURE

The movement towards PHR systems has created new challenges for the sharing of health information in a private and secure manner. In particular, when situations occur where access to medical

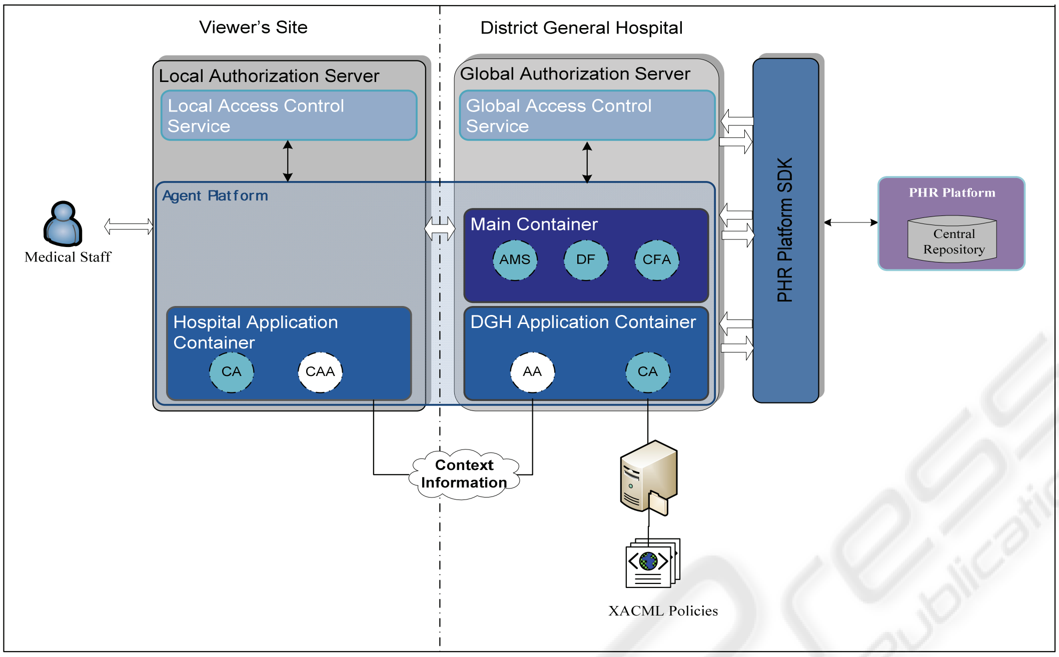
Viewer's Site
District General Hospital
Local Authorization Server
Local Access Control Service
Global Authorization Server
Global Access Control Service
Agent Platform
Main Container
AMS
DF
CFA
Hospital Application Container
CA
CAA
DGH Application Container
AA
CA
PHR Platform SDK
PHR Platform
Central Repository
Medical Staff
Context Information
XACML Policies

Figure 3: Security Architecture.

information is required but patients cannot grant permissions to the medical staff needing the information for treating them, effort should be put in the development and enforcement of a mechanism that automates the authorization propagation process while ensuring privacy and security against unauthorized access to the data.

The number, type and sophistication of tools that protect information in PHR environments are growing at an ever-increasing rate and provide the opportunity to offer health privacy protections beyond those in the paper environment. In many cases, the utilization of role-based access controls is considered as an effective means of limiting access to a patient's information to only those individuals who need it for the patient's treatment.

In our prototype system, a dynamic access control mechanism is incorporated which is based on the role-based access control (RBAC) paradigm and is context-aware. As illustrated in Figure 3, this is described by a two-tier model consisted of a global access control service, residing on a server at the DGH site, and one local access control service, residing at the viewer's site (i.e. any healthcare organization within the health district). Both services have been implemented using the Java Authentication and Authorization Service (JAAS) (Java Authentication and Authorization Service, 2008) and use a number of agents for context management.

The access control mechanism developed is middleware-based and its role is twofold. In particular, it is employed to:

- Grant/revoke authorizations of given subjects to (from) given objects by taking into account the current context (e.g. upon registration of an individual as an emergency patient). In order for these authorizations to be determined a set of access control policies are used by means of which role-to-permission assignments are specified.
- Mediate between subjects (healthcare professionals) and objects (data objects) and decide whether access of a given subject to a given object should be permitted or denied according to the context holding at the time of the attempted access (e.g. when the physician of the ED requests access to a patient's PHR).

In our prototype, users authenticate themselves by using X.509 certificates.

5.1 Access Control Policies

In our prototype system, the mapping of roles to the relevant permissions is performed by means of access control policies expressed by using the Core and Hierarchical RBAC profile of eXtensible Access Control Markup Language (XACML) (Organization for the Advancement of Structured Information Standards, 2008). These policies are expressed in the

```
<Resource>
  <ResourceMatch MatchId="&function;string-equal">
    <AttributeValue DataType="&xml;string">all
         </AttributeValue>
     ...
       </ResourceMatch>
 </Resource>
      ...
     <Action>
       <ActionMatch MatchId="&function;string-equal">
         <AttributeValue DataType="&xml;string">all</AttributeValue>
       ...
        </ActionMatch>
     </Action>
     <Condition>
       <Apply FunctionId="&function;string-equal">
   <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:environment:terminal"
           DataType="&xml;string"/>
         <AttributeValue DataType="&xml;string">inPremises</AttributeValue>
       </Apply>
                                              </Condition>
```

Figure 5: Sample Access Control Policy for Physician.

form of roles, role hierarchies, privileges and constraints.

Due to the strict security requirements on medical data comprising a PHR, the specification of access control policies not for the entire record but for its components (i.e. data objects) is of utmost importance. Since the record is organized as a hierarchy, when specifying policies on it the hierarchical resource profile of XACML (Organization for the Advancement of Structured Information Standards, 2008) can be used for the representation of these components. This profile specifies how XACML provides access control for resources that are organized as a hierarchy, such as file systems, XML documents and databases. According to this profile, non-XML data can be represented by a URI of the following form:

<scheme>://<authority>/<pathname>
where:

- <scheme> identifies the namespace of the URI and can be either a protocol (e.g. “ftp”, “http”, “https”) or a file system resource declared as “file”.
- <authority> is typically defined by an Internet-based server or a scheme-specific registry of naming authorities, such as DNS, and
- <pathname> is of the form <root name>{/<node name>}. The sequence of <root name> and <node name> values should correspond to the components in a hierarchical resource.

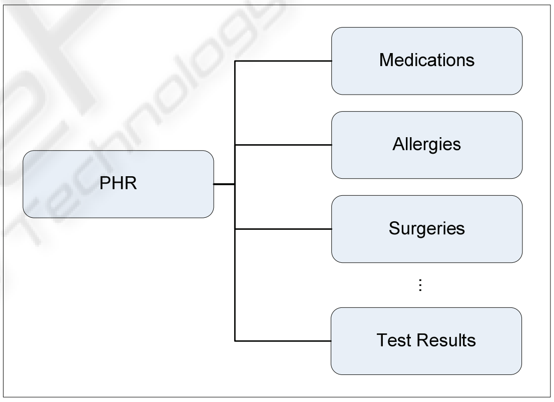

Figure 4: PHR Data Model.

Suppose that the data structure of a PHR is the one illustrated in Figure 4. Then the data object “Allergies” would be represented as follows:
“https://localhost:8443/PHR/Allergies”

The policies related to the permissions on data objects a healthcare professional should acquire while treating patient reside on a server at the DGH site. An excerpt of an access control policy for role “physician” is shown in Figure 5. This is a relatively simple policy that states that an ED physician is authorized to access the complete medical record of each patient he treats. This is specified within the tag <Resource> by means of the predicate “all” while the predicate “all” within the tag <Action> means that the physician has all kinds of permissions on the patient's medical record. Permissions on data objects are dynamically adapted by the constraints imposed by the current context. These are declared within the tag <Condition> and for the role "physician" is whether he/she is requesting patient information using a terminal within the hospital premises.

5.2 Context Information Management

In our prototype system, the management of context information influencing authorization decisions is performed by a Context Manager. Both the context information model and the Context Manager are described below.

5.2.1 Context Information Model

In our prototype system, the contextual information influencing authorization decisions is determined by a pre-defined set of attributes related to:

- the user (e.g. user certificate, user/patient relationship) and
- the environment (e.g. client location and time of attempted access)
- the healthcare provider (e.g. physicians on duty)

For example, the permissions of an ED physician accessing the system via a terminal, are adapted depending on his/her identity (included in his electronic Health Card) as well as the location of the terminal and time of attempted access.

5.2.2 Context Manager

Context information is collected by a Context Manager which has been implemented as a multi-agent system. Thus, the Context Manager consists of two kinds of agents, developed in JADE (Java Agent Development Framework, 2008):

- *Context Acquisition Agent (CAA)*: It is hosted on a server at the site of the healthcare organization where the ED belongs and is responsible for the acquisition of the contextual information required for granting authorizations and taking authorization decisions regarding access on the data objects comprising a patient's PHR.
- *Authorization Agent (AA)*: It is hosted on a server at the DGH and is responsible for automatically granting (revoking) authorization to (from) healthcare professionals without the patient's involvement. Moreover, it is responsible for managing access to patients' PHRs.

6 IMPLEMENTATION ISSUES

To illustrate the functionality of the proposed architecture, a prototype system has been developed which is based on the case scenario of Section 3.

The prototype implementation of the proposed system and the security services incorporated in it has been developed in a laboratory environment. In our implementation Apache/Tomcat is used as Web/Application Server while agents are developed using JADE (Java Agent Development Framework, 2008). The databases used by the existing information systems are developed using MySQL. The PHR system is implemented using the ICW Lifesensor Personal Health Record which can store the owner's complete medical information in one convenient and secure location (ICW eHealth Framework, 2009). The patient as owner of the record authorizes health team members or care providers to access their record and assigns specific read and write privileges (ICW eHealth Framework, 2009). ICW Java SDK is used for the integration of Lifesensor PHR to our application.

Upon arrival to the ED of a hospital, an individual is registered as an emergency patient and the authorization propagation process is triggered in order for the required authorizations to be determined and granted to the medical staff treating him. To this end, the local access control service is invoked which, in conjunction with the local Context Acquisition Agent (CAA), is accessing the local database(s) in order to retrieve the list of the medical staff being on duty at the time. The pieces of information retrieved include starting and ending time of each person's shift. As soon as the information is retrieved, it is communicated to the global access control service which, in conjunction with the Authorization Agent (AA), is determining the corresponding access rights for each person on the list according to a number of XACML policies. The latter are already defined and stored on a server at the DGH site. Finally, the deducted authorizations for each member of the medical staff are granted to him/her by means of the ICW SDK's HealthRecordManager which essentially represents the access to a given personal health record.

After the authorizations have been granted, the nurses and physicians of the ED authenticate themselves in order to gain access to this patient's full medical record by using their credentials (X.509 certificate stored in his electronic Health Card - eHC). Each access request is handled by the corresponding local access control service which is using CAA to acquire the context holding at the time of the attempted access and forwards the request to the global access control service which in cooperation with the AA decides whether access should be granted or denied to the requesting party. If the requesting party has the required privileges a connection to the corresponding PHR is established and the corresponding part of the patient's record is provided to him/her.

After reviewing the patient's medical record, the ED physician forms the appropriate care plan for the patient under treatment.

7 CONCLUDING REMARKS

Personal health records can address healthcare information needs as they can provide each person with a complete copy of his medical record. Thus, PHRs constitute a valuable tool for supporting the continuity of care and consequently the quality, access and efficiency of health care delivery. As PHR systems grow in popularity, it is important that they be managed and maintained responsibly without hindering accessibility to important information in cases that it is mostly needed (e.g. emergency cases). Hence, apart from the security and privacy controls which are common to any electronic health record system, in PHR systems a suitable mechanism should be in place that will automate the authorization propagation process without the patients' involvement. The prototype system presented in this paper deals with this security issue. In particular, a mechanism is presented whereby the process of granting (revoking) authorization to (from) healthcare professionals on patients' PHR is performed without the patient's involvement. To this end, context-aware technology is used. Thus, both clinical and administrative patient data are becoming immediately available to people who need it via accessible, secure and highly usable PHRs, fact that constitutes an enabling factor of the patient-centred shared care.

A number of issues related to the implementation of systems like the one proposed in this paper suggest directions for future work. The most important concern the means used for patient authentication as well as the way medical staff is granted access to medical data in cases where patient registration is performed after the patient has received treatment, as is often the case in EDs.

REFERENCES

Koufi, V., Vassilacopoulos, G., 2008. HDGPortal: A Grid Portal Application for Pervasive Access to Process-Based Healthcare Systems, In PervasiveHealth'08, 2nd International Conference in Pervasive Computing Technologies in Healthcare

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., Sands, D. Z., 2006. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. Journal of the American Medical Informatics Association : JAMIA (2006) 13(2): 121-126.

Wiljer, D., Urowitz, S., Apatu, E., DeLenardo, C., Eysenbach, G., Harth, T., Pai, H., Leonard, K. J., 2008. Patient accessible electronic health records: exploring recommendations for successful implementation strategies. Journal of medical Internet research, 10(4).

Lauer, G., 2009 Health Record Banks Gaining Traction in Regional Projects, http://www.ihealthbeat.org/features/2009/health-record-banks-gaining-traction-in-regional-projects.aspx

Yasnoff, W. A., 2008. Electronic Records are Key to Health-care Reform, BusinessWeek.

Win, K. T., Susilo, W., Mu, Y., 2006. Personal Health Record Systems and Their Security Protection, Journal of Medical Systems (2006) 30: 309-315.

Comini, L., Mazzu, M., Scalvini, S., 2008. Security aspects in electronic personal health record: data access and preservation, Digital Prevention Europe, Briefing Paper.

Røstad, L., Nytrø, Ø, 2008. Personalized Access Control for a Personally Controlled Health Record, In CSAW'08, 2nd ACM Workshop on Computer Security Architectures

My Personal Health Record (MyPHR), http://myphr.ca/

National Institute of Standards and Technology (NIST), 2009. Role Based Access Control (RBAC) and Role Based Security, http://csrc.nist.gov/groups/SNS/rbac/

Java Agent Development Framework, http://jade.tilab.com/

Organization for the Advancement of Structured Information Standards (OASIS), 2008. Core and Hierarchical Role Based Access Control (RBAC) Profile of XACML v2.0, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf

Java Authentication and Authorization Service, http://java.sun.com/javase/6/docs/technotes/guides/security/jaas/JAASRefGuide.html

ICW eHealth Framework, Lifesensor, 2009. http://idn.icw-global.com/solutions/lifesensor/lifesensor.html

Wikipedia, 2009. Emergency Department, http://en.wikipedia.org/wiki/Emergency_department

Metavante, In Case of Emergency Personal Health Record, https://www.icephr.com/