MEDIS – A WEB BASED HEALTH INFORMATION SYSTEM
Implementing Integrated Secure Electronic Health Record

Snezana Sucurovic
Institut Mihailo Pupin, Volgina 15, Belgrade,Serbia and Montenegro

Keywords: Electronic Health Record (EHCR), Security, Privacy.

Abstract: In many countries there are initiatives for building an integrated patient-centric electronic health record. There are also initiatives for transnational integrations. These growing demands for integration result from the fact that it can provide improving healthcare treatments and reducing the cost of healthcare services. While in European highly developed countries computerisation in healthcare sector begun in the 70's and reached a high level, some developing countries, and Serbia and Montenegro among them, have started computerisation recently. This is why MEDIS (MEDical Information System) is aimed at integration itself from the very beginning instead of integration of heterogeneous information systems on a middle layer or using HL7 protocol. MEDIS has been implemented as a federated system where the central server hosts basic EHCR information about a patient, and clinical servers contain their own part of patients' EHCR. Clinical servers are connected to a central server through the Internet and the system can be accessed through a browser from a place that has an Internet connection. A user also has to have a public key certificate to be able to login. As health data are highly sensible, MEDIS implements solutions from recent years, such as Public Key Infrastructure and Privilege Management Infrastructure, SSL and Web Service security as well as pluggable, XML based access control policies.

1 INTRODUCTION

MEDIS is based on European Committee for Standardisation standards ENV 13606 (CEN, 2002) and ENV 13729 (CEN, 2002), where the former defines architecture of EHCR, and the latter secure authentication. Applying these standards provides interoperatibility and their component-oriented architecture is suitable for distributed systems such as MEDIS. CEN ENV 13606 standard named "EHCR Communication" is a high level template which provides a set of design decisions which can be used by system vendors to develop specific implementations for their customers. The main item in CEN architecture standard is an Architectural Component. The Architectural Components are organised in a hierarchical structure. For a patient, there is a Root Architectural Component which represents a folder of patient record in the system and contains the basic information about a patient. On the other hand, there is a Record Component established by original component complexes (OCCs), selected component complexes (SCC), data items (DI) and link items (LI). An OCC comprises (according to data homogeneity) four basic components: folders, compositions, headed sections and clusters. A SCC contains a collection of data representing an aggregation of other record components that is not determined by the time or situation in which they were originally added to the EHCR. It may contain a reference to a set of search criteria, a procedure or some other query device whereby its members are generated dynamically (actually a distributed query, for example "current medication"). A Link Item is a component that provides a means of associating two other instances of architectural component and specifying the relationship between them ("caused by", for example). A Data Item is a Record Component that represents the smallest structural unit into which the content of the EHCR can be broken down without losing its meaning. A component is in a lower position in hierarchy if it contains more homogenous data. An example: Emergency Admission (Folder 1) > Assessment (Composition 1) >Accident Details (Section 1)> Causes of accident (Section 2) > Accident cause, as text (Data Item 1).

Each Architectural Component has reference to access control policy for that component defined as a Distribution Rule (Fig. 4). The Distribution Rule

Sucurovic S. (2006).
MEDIS – A WEB BASED HEALTH INFORMATION SYSTEM - Implementing Integrated Secure Electronic Health Record.
In *Proceedings of the Eighth International Conference on Enterprise Information Systems - ISAS*, pages 160-164
DOI: 10.5220/0002444001600164

comprises classes Who, Where, When, Why and How which define who, where, when, why and how is allowed to access the component (Table 1).

Table 1: Distribution Rule objects.

Classes	Attributes	Type
Who	Profession	String
	Specialization	String
	Engaged in care	Boolean
	Healthcare agent	Class
Where	Country	String
	Legal requirement	Boolean
When	Episode of care	Boolean
	Episode reference	String
Why	Healthcare process code	String
	Healthcare process text	String
	Sensitivity class	String
	Purpose of use	Class
	Healthcare party role	Class
How	Access method (read, modify)	String
	Consent required	Class
	Signed	Boolean
	Encrypted	Boolean
	Operating system security rating	String
	Physical security rating	String
	Software security rating	String

2 THE MEDIS ARCHITECTURE

MEDIS has been implemented as a federated system. Architectural Components are created in compliance with CEN ENV 13606 and stored there where they are created – at hospitals and clinics and are accessed via a central server which contains a Root component and the addresses of the clinical and hospital servers. Architectural components that are hosted on the clinical and hospital servers have pointers to supercomponents and linked components (Fig. 1.). HTML pages are created on the central server and contain five frames: the required Architectural Component (AC) in the right frame, links to subcomponents and linked components in the left upper frame, links to Selected Component Complex (actually distributed queries) in the left lower frame, the AC position in the hierarchical structure of EHCR in the upper frame and information about a user in the lower frame. (Fig. 2). A physician can define the position in EHCR (and therefore HTML page) which will appear when he requests EHCR for a patient.

In the MEDIS prototype there is an authentication applet (Sucurovic, 2005) which is processed in a browser and, after successful authentication, a HTML page has been generated using JSPs on the central server. The Clinical Servers tier has been implemented in Java Web Services technology using Apache Axis Web Service server and Tomcat Web Server. Business logic has been implemented in reusable components – Java Beans.

3 IMPLEMENTING SECURITY IN MEDIS

As health data are highly sensitive, security has been the main item in MEDIS. We've implemented authentication, access control and encryption and, in that way, we've met requirements for privacy and confidentiality. MEDIS implements solutions from recent years, such as Public Key Infrastructure and Privilege Management Infrastructure, SSL and Web Service security as well as pluggable, XML based access control policies.

3.1 Authentication

Using a password as a means of verification of claimed identity has many disadvantages in distributed systems. Therefore, MEDIS implements CEN ENV 13 729 (CEN ENV, 2002) which defines authentication as a challenge-response procedure using X.509 public key certificates (Sucurovic, 2005). However, MEDIS implements not only public key certificates management, but also attribute certificates management (Blobel, 2003), (Sucurovic, 2006). Originally, X.509 certificates were meant to provide nonforgeable evidence of a person's identity. Consequently, X.509 certificates contain information about certificate owners, such as their name and public key, signed by a Certificate Authority (CA). However, it quickly became evident that in many situations, information about a person's privileges or attributes can be much more important than that of their identity. Therefore, in the fourth edition of the X.509 Standard (2000), the definition of an attribute certificate was introduced to distinguish it from public-key certificates from previous versions of the X.509 Standard.

In the MEDIS project X.509 PKCs are supposed to be generated by public Certificate Authority, while ACs are supposed to be generated by MEDIS Attribute Authority. The public key certificates are transferred to users and stored in a browser. The attribute certificates are stored on LDAP server, because they are supposed to be under control of MEDIS access control administrator. In the MEDIS approach attribute certificates contain user's

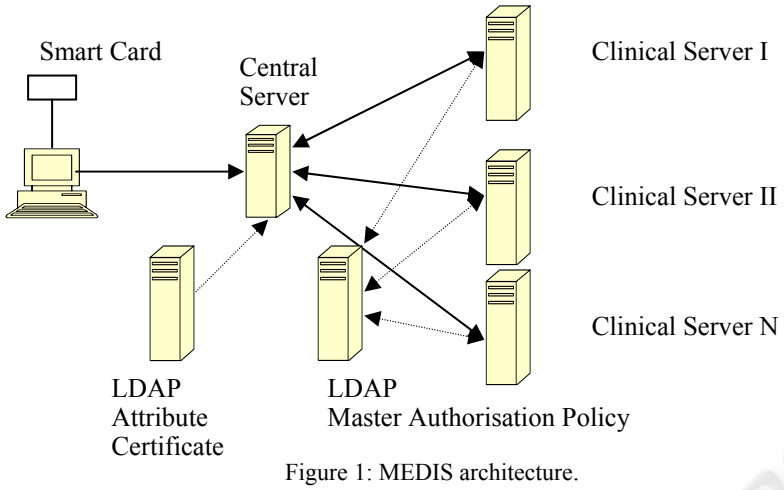

Figure 1: MEDIS architecture.

attributes as XML text. There are two types of public key and attribute certificates: the Clinicians' and Patients' as distribution rules contain a flag which denotes if the Architectural Component is allowed to be read from a patient.

3.2 Access Control

In a complex distributed system, such as MEDIS, access control is consequently very complex and has to satisfy both fine grained access control and administrative simplicity. This can be realised using plugable, component based authorisation policies (Beznosov, 2004). An authorisation policy is the complex of legal, ethical, social, organisational, psychological, functional and technical implications for trustworthiness of health information system . One common way to express policy definition is XML schemadata. These schemes should be standardised for inter-operatibility purposes (Blobel, 2004). The MEDIS project aims at developing the authorisation policy definitions, using XML scheme, which are based on CEN ENV 13 606 Distribution Rules (CEN 2002).

The MEDIS project has adopted XML as the language for developing constrained hierarchical Role Based Access Control and, at the same time, has focus on decomposing policy engines into components (Beznosov, 2004), (Zhou, 2004), (Blobel, 2004), (Chadwick, 2003), (Joshi, 2004). The MEDIS project authorisation policy has several components (MEDIS Technical Report, 2005). First, there is an XML schema of user attributes that corresponds to the attribute certificate attributes. User attributes are transfered in SOAP Headers. Secondly, there are Distribution Rules attached to each Architectural Component (Fig. 3). Third, there is an Authorisation Policy on the clinical server. It defines hierarchies of How, When, Where, Why and Who attributes (hierarchy of Roles, Professions, Regions etc). In that way, a hierarchical RBAC can be implemented, with constraints defined by security attributes (software security, physical security rating etc.) and non-security attributes (profession, specialisation etc.). There are, also, two master Authorisation Policies. The Master Authorisation Policy for Hierarchy defines which combination of, for example, role hierarchy and profession hierarchy is valid. There is another master Authorisation Policy – the Master Authorisation Policy for DRs: it defines which combinations of attributes in a Distribution Rule are allowed in general and for an archetype. There is an enable/disable flag, which defines if the given combination of hierarchies is enabled or disabled (for the first master Authorisation Policy) and if the given combination of attributes in a Distribution Rule has been allowed or forbidden (for the second master Authorisation Policy). There are in fact, two administrators: one on the clinical server and another on the central LDAP server. In that way, this approach provides flexibility and administrative simplicity.

As in (Joshi, 2004) grouping information content into concept clusters reduces complexity of the specification process and security administration. In the MEDIS project there is a content based access control specification on three levels: conceptual, archetype and instance, i.e. master authorisation policies can be defined on the conceptual and archetype level while there are Distribution Rules related to the Architectural Component, as access control specification on instance level.

Figure 2: CEN ENV 13606 Composition Component example.

3.3 Encryption

The MEDIS project implements Web Service security between the clinical and central server and SSL between the central server and a client (Microsoft, IBM, 2004). We use Apache's implementation of the OASIS Web Services Security (WS-Security) specification – Web Service Security for Java (WSS4J) (W3C Recommendation, 2002). WSS4J can secure Web services deployed in most Java Web services environments; however, it has specific support for the Axis Web services framework. WSS4J provides the encryption and digital signing of SOAP messages as well as the transfer of SAML attributes in SOAP Header. In our application Attribute Certificate's attributes are transferred in SOAP Header. The RSA algorithm has been chosen for signing and the TripleDES for encryption. Communication between the browser and Web Server has been encrypted using SSL. Currently, Netscape 6 browser and Tomcat 5.0 Web Server are used and the agreed chiper suite between them is SSL_RSA_WITH_RC4_128_MD5.

4 CONCLUSION

The aim of MEDIS project is the development of a prototype of secure national healthcare information system in which communication is based on the Internet. Compared to other existing Web based EHCR the originallity of the MEDIS is CEN ENV 13606 based architecture where Root Component is hosted on a central server and other components in hierachy are placed on clinical servers. As health data are highly sensitive MEDIS implements solutions from recent years, such as Public Key Infrastructure and Privilege Management Infrastructure, SSL and Web Service security as well as pluggable, XML based access control policies. The MEDIS project aims at giving contribution to standardisation of access control policies based on CEN ENV 13606 Distribution Rules definition. The MEDIS project aims at contributing to initiatives for building integrated national and global healthcare information systems.

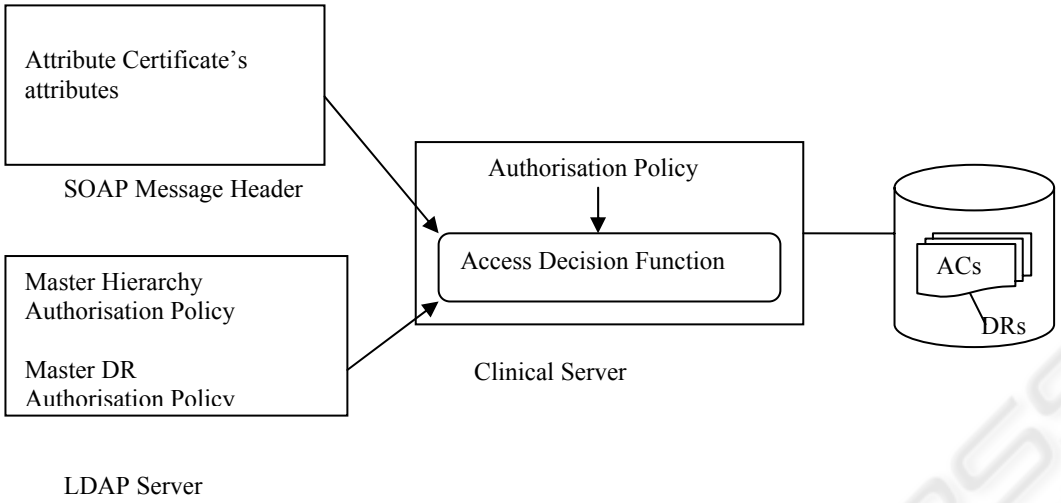

Figure 3: MEDIS access control components.

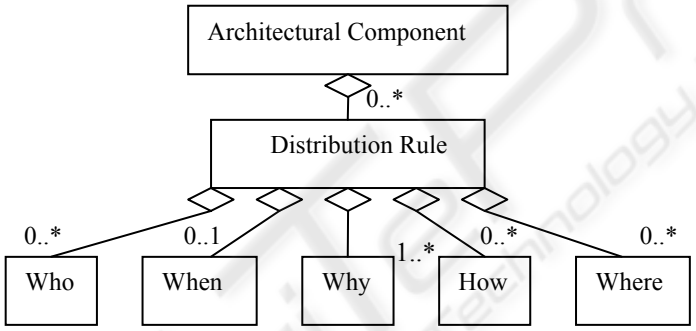

Figure 4: Distribution Rule (CEN ENV 13606 Part 3).

REFERENCES

Beznosov K., 2004, On the Benefits of Decomposing Policy Engines into Components, *In. 3rd Workshop on adaptive and Reflect Middleware*, Toronto

Blobel B. et. al., 2003, Using a privilege management infrastructure for secure Web-based e-health applications, Computer Communications, Elsevier

Blobel B., 2004, Authorisation and access control for electronic health record system, Intern. Journal of Medical Informatics, Elsevier, No.73, pp. 251-257,

Chadwick D. et. al., Role based access control with X.509 Attribute Certificates, IEEE Internet Computing, March/April 2003, pp. 62 – 69

Commite Europen de Normalisation ENV 13606 Standard, 2002, *Extended Architecture*

Commite Europen de Normalisation ENV 13729 Standard, 2002, *Secure user identification*

Joshi J. et. al., Access Control Language for Multidomain Environments, IEEE Internet Computing, November/December 2004, pp. 40-50.

MEDIS Technical Report, Retrieved September 28,2005 from http://www.imp.bg.ac.yu/dokumenti/MEDISTechnicalReport.doc

Microsoft and IBM White Paper, Security in Web service world: A Proposed Architecture and Roadmap, Retrieved September 28,2005 from http://www-128.ibm.com/developerworks/webservices/library/ws-secmap

Sucurovic S., Jovanovic Z., February 2005, Java Cryptography & X.509 Authentication, Dr. Dobb's Journal, San Francisco

Sucurovic S., Jovanovic Z., 2006, Java Cryptography & Attribute Certificate Management, Dr. Dobb's Journal, San Francisco

XML Encryption Syntax and Processing, W3C Recommendation, 2002

XML Signature Syntax and Processing, W3C Recommendation, 2002

Wei Z. et. al., 2004, Implement role based access control with attribute certificates, ICACT 2004, *International Conference on Advanced Communication Technology*, Korea