Secure Healthcare Information Exchange for Local Domains

Guy C. Hembroff
School of Technology
Michigan Technological University
Houghton, United States
hembroff@mtu.edu

Sead Muftic
SETECS Inc.
Silver Spring, United States
sead.muftic@setecs.com

Abstract— **The National Institutes of Health, along with other healthcare related agencies, continue to define the importance of exchanging medical data between hospitals and other healthcare providers. However, issues within the medical field such as interoperability, scalability and security continue to plague electronic exchange of information within the healthcare sector.**

In this paper we present an approach, called Secure Healthcare Information Exchange for Local Domains (SHIELD), which defines strategic components within an architecture that solves the problem of interoperability, scalability and security. Our solution integrates biometric and smart card technology that permits each hospital to exchange medical data with other hospitals within the trusted federation, without sacrificing the ability for individual hospitals to maintain their own policy enforcement. This research is currently being implemented within one Regional Center and fourteen hospitals within the Upper Peninsula of Michigan in the United States.

Keywords-security; biometrics, electronic medical records; interoperability; federation; smart card; healthcare; HL7

I. INTRODUCTION

Over recent years, the standard Electronic Medical Record (EMR) has seen increased exposure and use by the medical sector. Healthcare organizations recognize its potential to increase patient safety, streamline operations within the medical organization and provide monetary savings to both the patient, insurance carrier and medical institution. However issues such as interoperability, scalability and security, involving patient confidentiality and privacy outlined by the Health Insurance Portability and Accountability Act (HIPAA) [1] have made solutions to this problem challenging.

Michigan Technological University (MTU) and SETECS® are jointly designing, installing, and activating Secure Healthcare Information Exchange System for Local Domains (SHIELD) to permit a secure healthcare information exchange system for Michigan's Upper Peninsula hospitals. The system will include fourteen hospitals and one regional center. The purpose of the system is to provide secure, authorized and synchronized exchange of patient records between all hospitals associated with the Upper Peninsula Healthcare Network (UPHCN). The system has been designed to incorporate the following:

- Redesigning SETECS® security products for the healthcare security initiatives and satisfy the UPHCN's additional security and functional requirements; and
- Provide accurate method of patient, physician, nurse and staff identification throughout the developed federation of hospitals; and
- Develop and extend interoperability and security between electronic medical record (EMR) systems throughout all hospitals located in the project.

This document describes the components of the SHIELD system, their individual functions and operations, along with the use and the overall integrated security system. The project is expected to be completed October 1, 2009.

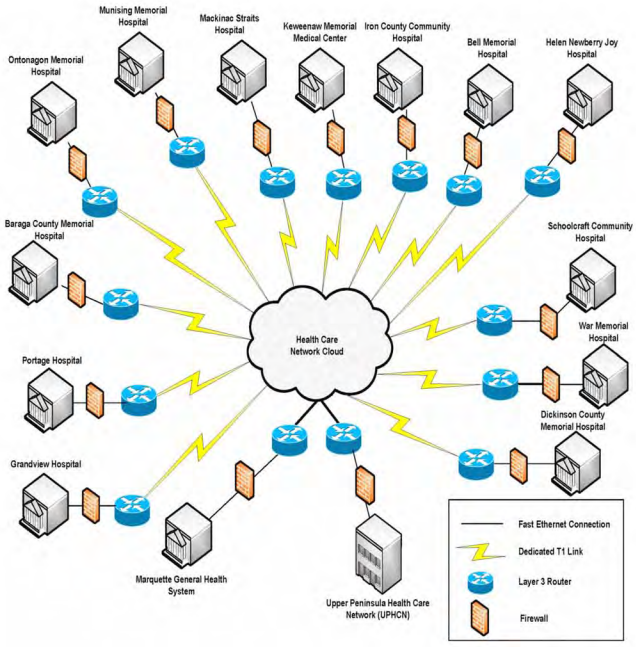
A. Background

The state of Michigan's Upper Peninsula is significantly rural and contains a low population of 356,791 residents dispersed over a large geographical area that accounts for only 14 persons per square mile [2]. As a result, access to advance healthcare for individuals within this area is very limited.

To combat this issue, thirteen hospitals have joined the area's only Level II Trauma Center and UPHCN to form a cohesive entity that strategically maximizes technology and resources to better serve the patient. The creation of this network permits smaller hospitals to utilize advanced medical technology that their patients would normally be not able to receive. An illustration of the area's network architecture is illustrated in figure 1.

The Level II Trauma Center, Marquette General Health Systems (MGHS) is centrally located within the Upper Peninsula of Michigan, which grants each of the thirteen hospitals the opportunity to regularly transfer patients between their institution and MGHS and back. Therefore, having the ability to successfully transfer patients' EMR data between hospitals is critical to increase patient safety within this region.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5969
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5969



B. *Requirements and needs*

The participating hospitals and the UPHCN, as the coordinating institution, have specified the following functional and security requirements for their healthcare information exchange system:

- Accurately identify each patient using biometric technologies
- Accurately track patients in each institution and throughout the region
- Securely exchange and share medical information electronically between the region's institutions
- Securely exchange medical documents between medical institutions throughout the region
- Provide a secure and scalable role-based security system to control access to patient's records

II. Related Work

A significant amount of research has been conducted towards exchanging EMR data between healthcare institutions [3-6]. These investigations stem from organizing the framework of healthcare networks to allow for secure transfer of EMRs [3,6-8] to Health Level 7 (HL7) Web-based applications that are able to view patient's medical and billing information [9].

Problems associated with healthcare providers' employees obtaining authorized access to secure clinical information by traditional logon approaches have been investigated by [10]. This research proves that often complex passwords, which meet "strong" password policy criteria, are often written down by physicians and staff to easily remember. The study also points out that a healthcare environment is often quite different than a traditional business environment regarding the use of their computer services. An example can be seen when you have multiple nurses and physicians accessing a single PC on the floor of the hospital.

Research conducted by [11] describes the use of smart cards access to Web-based medical information systems. This research examines using an open-distributed system with smart card technology to place patient EMR data. This integration provides the flexibility of patients to become "mobile" with their Patient Health Record (PHR) information and also provides a schema that does not require a central storage solution.

III. Problem Statement

Creating a flexible, scalable and secure system that provides interoperability between all institutions and their applications is complex. Work by [11] implemented smart cards over a distributed system to provide patients with a flexible method of carrying their EHR information. However, with this approach, the smart card is required to access the records. Healthcare institutions provide countless examples of patients arriving at the facility, such as in an emergency situation, where they may be unconscious and unable to provide their pin number with the smart card, or may not have the smart card with them at all. In these instances it is critical to have a system designed to provide methods to access patient medical data under a secure format that is scalable, flexible and provides interoperability between not only patient smart cards but also between each healthcare provider.

The goal of this paper is to provide a conceptual framework in meeting all the critical requirements to effectively exchange medical data and documents between healthcare institutions and their patients. This research expands on past research and offers an effective solution that is currently being implemented within medical institutions.

IV. Components and Structure of the SHIELD System

To meet stated requirements of the proposed architecture, we have designed the SHIELD system at strategic layers. This is a comprehensive architecture specifically designed to successfully achieve security, interoperability, and scalability between healthcare organizations. The first layer is an instance of the developed system in each hospital. While the second, is an instance of the developed system structured for the Regional Center to offer the hierarchical approach for this federation. The structure and components of the SHIELD system in each hospital and in the Regional Center are shown in figure 2.

A. *SHIELD System Design for Hospitals*

In each hospital, an instance of the SHIELD system comprises of three subsystems:

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5969
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5969

a) *Registration System:* used to register all patients and professionals employed in the hospital.

b) *Hospital Security System:* manages security credentials for employees. This includes certificates, authentication and authorization tokens, and security policies.

c) *Extended EMR System:* used to manage patients' medical records both internally and externally. Internally, by using the local EMR system to reference patient. Externally, by synchronizing databases with other EMR systems in other hospitals and Regional Center.

The Registration System containing the Identity Management Server (IDMS) contains the following within each hospital:

a) *Smart Card Station:* shown in Fig. 2, is used to enroll employees/patients and capture fingerprint biometric data and photo of individuals.

b) *Local IDMS Server:* shown in Fig. 2 integrated within the Hospital Security Server, is used to store registration data for employees in order to enforce their access and authorization privileges.

c) *Local IDMS Station:* not shown in figure due to being integrated either the Hospital Security Server or used remotely from separate PC. This station is used to manage personal registration data in the IDMS server and their security credentials for local employees.

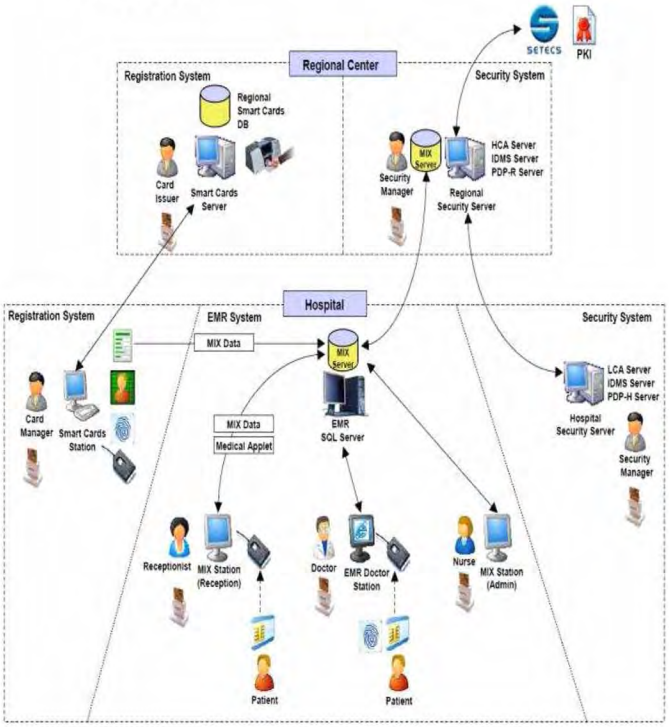


Figure 2. SHIELD Architecture and Components

Hospital Security System comprises of the following within each hospital:

a) *Local Certificate Authority (CA) Server:* indicated in Fig. 2 as the LCA server, it is used to generate and distribute X.509 certificates to all other components of the system.

b) *Policy Decision Point (PDP) Server:* shown in Fig. 2 as PDP-H Server, is used to create local hospital authorization policy and to make authorization decisions.

The Extended EMR System in each hospital contains the following:

a) *Medical Information Exchange (MIX) Server:* displayed in Fig. 2 adjacent to the standards EMR server, used store patient authentication based on fingerprint biometric and/or smartcard authentication. System has also been designed to cross-reference new Registration and Security systems and existing EMR system. This server also has the responsibility of a Policy Enforcement Point (PEP) for all local Web applications in each hospital.

b) *EMR Registration Station:* this station is equipped to run new Web-based application which uses patients' fingerprint biometric data for patient authentication.

c) *EMR Physician Station:* has been developed to run another Web-based application which uses physician/nurses or other staff fingerprint biometric data to authorize access to patients' EMRs.

d) *EMR Transfer Station:* runs a third Web-based application, which manages transfer of patients'' medical data and documents between hospitals within the secured federated architecture. Physicians and staff will utilize this Web interface view patient's EMRs in which they have security access to observe.

B. SHIELD System Design for the Regional Center

In the Regional Center, an instance of the SHIELD system comprises of two subsystems:

a) *Registration System:* used to issue smart cards to all employees and patients of hospitals associated within federated architecture.

b) *Regional Security System:* is used to complement Security System servers in each hospital.

The Registration System within the Regional Center incorporates the following:

a) *Smart Card Production Server:* used to issue smart cards to all employees in hospitals and to all patients.

b) *Smart Card Central Server:* is utilized to hold data for all smart cards within issues within the region.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5969
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5969

Security System within the Regional Center comprises of the following:

a) *Regional CA Server:* indicated in Fig. 2 as the HCA server, it is used to certify Local CA Servers in each hospital.

b) *Regional IDMS Server:* shown in Fig. 2 as IDMS Server, is used for registration of individuals and defined components in the Regional Center.

c) *Regional PDP Server:* shown in Fig. 2 as PDP-R Server, maintains common elements and policies for all hospitals.

d) *Regional MIX Server*: shown in Fig. 2 as Mix server, is used as bridge for synchronization, inter-hospitals data and documents transfers, and for conversions of EMR data and formats.

C. *Interrelationships Between System Components in Hospitals and the Regional Center*

Smart Card Stations in hospitals are linked to the Smart Card Central Server in the Regional Center. The individual stations submit registration data for patients and professionals to issue their smart cards. The MIX server in each hospital is linked to the MIX Server in the Regional Center. Hospitals exchange referenced to medical data and electronically medical documents using the MIX Server in the Regional Center. Policy Decision Point (PDP) Servers in each hospital access the Regional PDP server to fetch regional security policy, which is extended with additional policies in each hospital to create policy sets specific to that respective site and globally compliant to the regional authorization policy. Two certificates of the Local CA servers in hospitals are certified by the Regional Certification Authority server in the Regional Center. Two certificates of that CA Server are in turn certified by SETECS®, US National Policy CA Server, thus linking Michigan's Upper Peninsula Private Key Infrastructure (PKI) into global SETECS® international PKI.

V. Operations and Use of the SHIELD System

The SHIELD system has been designed to manage identities and security credentials of patients and professionals who are currently employed by the participating hospitals. The system is maintained by security administrators in each hospital and in the Regional Center.

In order to implement security services within a federated environment, the system will be established in the form of multiple autonomous domains. Our developed architecture utilizes standards to ensure compliancy and scalability options are being met.

- IDMS compliant to the Federal Information Processing Standard 201 (FIPS 201) a Personal Identification Verification (PIV) standard
- PKI components, protocols and services handling X.509 certificates
- Web Security Services (WSS), comprising components and protocols based on World Wide Web Consortium (W3C), Organization for the Advanced of Structured Information Standards (OASIS), Internet Engineering Task Force (IETF), and Liberty Alliance standards, secure Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Security Assertion Markup Language (SAML)
- Secure transactions services for wired and wireless devices based on Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME), and SAML standards
- Patient Registration Server capable of registering each patient into a unique Master Patient Index (MPI) number, which will be used to accurately cross reference patients throughout the federated architecture.
- Smart Cards Management Services (CMS) compliant to the FIPS 201 standard and GSA requirements for architectures suitable for large–scale card deployment services.

The following subsections describe the procedures for each of the three current groups enrolled within the system.

A. *Patient Procedures*

1) Registration of Patients: A patient visits a hospital and approaches the reception desk. If the patient has not registered within any of the areas federated sites, they will be directed to the Smart Card Station. The station operator will register the patient, capture his/her photo and also 2 fingerprints, using a fingerprint biometric reader. All data will be deposited in the Smart Card Central Server in the Regional Center, where smart card will be issued for the patient.

2) Activation of the Medical Smart Cards: When a patient whom has recently received their medical smart card visits one of the fourteen hospitals within the federation they will be again directed to the Smart Card Station. There, the patient's photo printed on the card, which will match the photo located on the hospital Web application, and his/her fingerprints inside the smart card chip will be verified. If verification is successful, the paitent will set up his/her own smart card PIN. At the same time MIX Cross-Reference Data and MIX Medical Data will be loaded into the card. At this stage the card is ready to be used for patient's authentication in all hospitals within the designated federation.

3) Subsequent Hospital Registration: With the medical smart card activated, a patient approaches the reception desk within the hospital. They will insert the card into a smart card reader available at the MIX station. After presenting his/her PIN and/or fingerprint, the patient's registration information will be retrieved. Any changes within patient's registration information will be updated at this time.

4) At the Phyician's office: If privacy and protection of patient's medical data is needed, this information will be retrieved only after a patient inserts and activates their medical smart card. Physicians, nurses and other medical personnel

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5969
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5969

will have SHIELD security card which will be used to authorize their access to the medical Web application and patient's medical data. These individuals will be able to acess medical data stored at the local EMR server directly, using local EMR application and data stored at other hospitals using the MIX Cross-Reference data accummulated at the hospital's MIX server.

5) Patient Transfer to Another Federated Hospital: When a patient is transferred to another hospital, medical administrators will use Web application to create MIX Cross-Reference Data at the hospital's MIX server and transfer that data to the Regional MIX server. MIX Cross-Reference data will be accumulated at the hospital's MIX server, so that the complete medical history of a patient is available at each of the federated site's MIX server.

6) Patient Transfer from Another Federated Hospital: When a patient visits a new hospital, the authorized hospital personnel will use a Web application at the MIX station to retrieve all of the patient's Cross-Reference Data, add recent data from the local MIX Cross-Reference Data, and include other data at the MIX server. This data will be stored into the patient's medical smart card. As a result, the hospital MIX Server will contain cross-references to all paitent's medical data in all other hospitals, while the patient's medical smart card will now contain MIX Cross-Reference data from the hospital.

B. Professional Procedures

1) Registration of Professionals: All professionals employed within each of the federated hospitals that requre access to patient's demographic and medical data, primarily physicians and nurses, will also be registered within the SHIELD system. The Smart Card Station within a hospital will also be used for the registration of these individuals. In addition to data sent to the Regional Smart Card Central Server for issuance of security smart cards, the data for professionals will also be stored within the IDMS Server at each hosptial. This segment of data will be used for authorization policy of the hospital's security system.

2) Activation of the Security Smart Cards: When the security smart cards are received back from the Regional Center, they will be activated, equivalent as with the patient's medical smart cards. However, instead of MIX data being loaded onto the card, security data will be placed into the chip card and used for authentication and authorization of professionals.

3) Access to Web Medical Applications: To obtain access to the medical Web applications, all professionals will insert the card in the smart card reader. After activating the card by providing PIN and/or fingerprint, security data will be retrieved from the card and used by the security system for single sign-on (SSO) user authentication and role-based authorization. Both of these security services will be enforced by the local seucrity policies that have been put in place by the security administrators of each system.

C. Regional Center Security Administrator Procedures

1) Issuance of Smart Cards: Based on registration data submitted by hospitals' Smart Card Stations, security administrator in the Regional Center will issue SHIELD medical smart cards for paitents and security smart cards for professional staff. The respective cards will be mailed to both patients and professionals, as their home address field must be completed prior to submitting successful card request.

2) Creation of Regional Security Policy: The security administrator in the Regional Center will create regional security policy, which will be applicable to all federated hospitals across the region. The policy will contain common attributes, such as dictionary of roles and shared policy rules. The policy will be distributed to all hospitals' security servers. This common policy agreement, coordinated with the UPHCN Regional Center, is appended to individual policies set forth by each hospital. This process ensures that common policy is practiced throughout the federation, however each hospital is permitted the flexibility to implement additional policies that may be only specific to their site.

D. Hospital Security Administrator Procedures

1) Import Regional Security Policy: Security administrator in each hospital will import regional security policy from Regional Center. This policy can then be included within the hospital's local security policy.

2) Regsistration of Local Groups and Applications: In order to create local policies in each hospital, security administrators will specify local groups, register users into those groups, register local applications, and local authorization rules.

3) Creation of Local Security Policy: Security administrator will create local security policies in their respective hospitals by combining local policies and regional policity into their policy sets. Those policy sets will be used to support and enforce authentication and authorization of proffesionals when accessing medical applications and using medical data. To ensure scalability and consistency within the security policies, an agreed pre-set of regional policies have been determined by the aggregate group of fourteen hospitals and the UPHCN. This allows a common set of approved security policies for the federation and any additional healthcare organizations wishing to join the network would have to adhere to. While this promotes scalability and consistency, the architecture's security design also permits local sites to develop their own specific security polices to conform their organizations security policy regulations. Therefore critical access hosptials (CAHs) who may have different security policy requirements from non CAHs will be able to tailor local security policy settings to their needs. Any conflict between a regional security policy and local security

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5969
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5969

policy setting would be decided by the local security policy setting. This permits the local organization to make final determination of its site's security policy.

VI. Conclusion and Future Work

The SHIELD system has been designed to provide interoperability, scalability, security and flexibility to electronic medical data and document exchange. Our solution incorporates fingerprint biometrics and smart card technology within a distributed system that allows healthcare providers to accurately track patients and securely exchange medical information. This solution interfaces with existing hospital EMR technology to provide an architecture that does not require central storage of data, but rather utilizes each site's existing storage to "pull" information from hospital MIX servers where it is displayed under a designed web Graphical User Interface (GUI) application. Security for the system is enforced through the CAs, policies within the federation and through smart cards to ensure that only authorized personnel have access to patient's records. The system also provides the option to merge both regional policies and individual hospital policies to provide flexibility to each site and their respective security administrators. Our solution is scalable in that it is built on accepted technical and medical standards that permit other healthcare providers the ability to join the federation. In addition, patients enrolled within the region, can go to any of the hospitals and use their smart card and/or fingerprint to register or have their personal medical records viewed.

The development of this project also leads to other areas of research that we intend to pursue as future work. One particular area of interest is the exchange of information for home health monitoring. We plan to extend our current infrastructure to securely permit home health monitoring and synchronization of patient health information from smart cards from remote sites, such as the patient's home. Additional topics of interest that we are currently researching are the following:

- Access control model for patients' healthcare smart cards
- Role-based authorization system for medical data based on security smart cards
- Concept of secure medical information exchange (MIX) server
- Patients' privacy issues in global integrated medical information systems
- Security architecture for large-scale distributed medical applications

VII. List of Abbreviations

CA : Certificate Authority
CMS : Card Management System
EMR : Electronic Medical Record
FIPS201: Federal Information Processing Standard 201
GUI : Graphical User Interface
HIPAA : Health Insurance Portability and Accountability Act
HL7 : Health Level 7
IDMS : Identity Management Server
IETF : Internet Engineering Task Force
MGHS : Marquette General Health System
MIX : Medical Information Exchange
MPI : Master Patient Index
MTU : Michigan Technological University
OASIS : Organization for the Advancement of Structured Information Standards
PDP : Policy Decision Point
PEP : Policy Enforcement Point
PHR : Patient Health Record
PKI : Private Key Infrastructure
PIV : Personal Identification Verification
SAML : Security Assertion Markup Language
SHIELD: Secure Health Information Exchange for Local Domains
S/MIME: Secure Multipurpose Internet Mail Extensions
SOAP : Simple Object Access Protocol
SSL : Secure Sockets Layer
SSO : Single Sign-on
UPHCN : Upper Peninsula Healthcare Network
W3C : World Wide Web Consortium
WSS : Web Security Services
XML : Extensible Markup Language

Acknowledgment

We would like to thank the UPHCN, all participating hospitals and the state of Michigan for their input and support of this project.

References

[1] HIPAA. Health Insurance Portability and Accountability ACT. Available online at http://www.hipaadvisory.com [11/2/08].

[2] U.S. Bureau of Census. Demographic Inforamtion on Partner Hospital Counties in Michigan (2000). Available online at http://www.census.gov [10/25/08].

[3] M. Beyer, K. Kuhn, C. Meiler, S. Jablonski, R. Lenz. "Towards a flexible, process-oriented it architecture for an intergrated healthcare network," in *Proceedingsof ACM Symposium on Applied Computing*, 2004.

[4] K. Garson, C. Adams. "Security and privacy architecture for an e-hospital environment," in ACM International Conference Proceeding Series, vol. 283, pp. 122-130, 2008.

[5] C. Juo, P. Humenn. "Dynamically authorized role-based access control for secure distributed computation," in *Proceedings of ACM Workshop on XML Security*, 2002.

[6] B. Blobel. "Authorization and access control for electronic health record system," Intern. J. Med. Infor. 73, pp. 251-257, 2004.

[7] Y. Al-Salqan. "Security and confidentiality in healthcare informatics," in *Proceedings of IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterpises*, 1998.

[8] R. Raman, V. Jagannathan, R. Reddy. "Secure collaboration technology infrastructure for collaborative enterprises," in *Proceedings of IEEE Workshop on Enabling Technologies Infratstructure for for Collaborative Enterprises*, 1997.

[9] D. Essin, T. Lincoln. "Healthcare information architecture: elements of a new paradigm," in *Proceedings of IEEE Workshop on New Security Paradigms*, 1994.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5969
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5969

[10] E. Bardram. "The trouble with login: on usability and computer security in ubiquitous computing," in Personal and Ubiquitious Computing, vol 9, pp. 357-267, 2005.

[11] T. Alvin, S. Chan. "Integrating smart card access to web-based medical information system," in *Proceedings of the 2003 ACM symposium on Applied computing*, pp. 246-250, 2003.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5969
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5969