PACIS 2011 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

9 July 2011

A Test Vehicle For A Secure And Resilient Architecture For Compliance In Index-Based E-Health Environments

Vicky Liu
Queensland University of Technology, v.liu@qut.edu.au

William Caelli
Queensland University of Technology, w.caelli@qut.edu.au

Yingsen Yang
Queensland University of Technology, hidenobu@gmail.com

ISBN: [978-1-86435-644-1]; Full paper

Recommended Citation

Liu, Vicky; Caelli, William; and Yang, Yingsen, "A Test Vehicle For A Secure And Resilient Architecture For Compliance In Index-Based E-Health Environments" (2011). *PACIS 2011 Proceedings.* Paper 119.
http://aisel.aisnet.org/pacis2011/119

A TEST VEHICLE FOR COMPLIANCE WITH RESILIENCE REQUIREMENTS IN INDEX-BASED E-HEALTH SYSTEMS

Vicky Liu, Information Security Institute, Faculty of Science and Technology, Queensland University of Technology, Australia, v.liu@qut.edu.au

William Caelli, Information Security Institute, Queensland University of Technology, Australia, w.caelli@qut.edu.au

Yingsen Yang, Queensland University of Technology, Australia, hidenobu@gmail.com

Lauren May, Information Security Institute, Queensland University of Technology, Australia, laurenmay53@hotmail.com

Abstract

Increasingly, national and international governments have a strong mandate to develop national e-health systems to enable delivery of much-needed healthcare services. Research is, therefore, needed into appropriate security and reliance structures for the development of health information systems which must be compliant with governmental and alike obligations. The protection of e-health information security is critical to the successful implementation of any e-health initiative. To address this, this paper proposes a security architecture for index-based e-health environments, according to the broad outline of Australia's National E-health Strategy and National E-health Transition Authority (NEHTA)'s Connectivity Architecture. This proposal, however, could be equally applied to any distributed, index-based health information system involving referencing to disparate health information systems. The practicality of the proposed security architecture is supported through an experimental demonstration. This successful prototype completion demonstrates the comprehensibility of the proposed architecture, and the clarity and feasibility of system specifications, in enabling ready development of such a system. This test vehicle has also indicated a number of parameters that need to be considered in any national indexed-based e-health system design with reasonable levels of system security. This paper has identified the need for evaluation of the levels of education, training, and expertise required to create such a system.

Keywords: indexed-based e-health systems, security architecture for health information systems, test vehicle.

1 INTRODUCTION

Numerous countries across the globe have national e-health initiatives at some stage of investigation or implementation. Nations such as Australia, New Zealand, the United Kingdom, the Netherlands, Canada, the United States, and Singapore are active in e-health initiatives. Normally, a national e-health system relies on indexing services to determine the locations of a patient's health records. Indexing services therefore play a central role in enabling disparate health records to become accessible across multiple repositories. Australia's National E-health Strategy (2008) also acknowledges that a central indexing or addressing mechanism is needed to link related health records which may reside in one or more locations. Moreover, the security, control and management of these indexing systems are subject to emerging and strict governance imperatives. This paper outlines three national index-based e-health initiatives from Australia, Canada, and Germany, and compares to the authors' approach.

In order to address the requirements for enhanced security in national e-health systems, a security architecture for index-based e-health environments is proposed. This architecture is based on the broad outline of the Australian Government's National E-health Strategy (2008) and National E-health Transition Authority (NEHTA)'s Connectivity Architecture (2010).[1] This proposal, however, could be equally applied to any distributed, index-based health information system involving referencing to other and disparate health information systems.

This paper assesses the feasibility and comprehensibility of the proposed architecture through the implementation of a small test vehicle. The practicality of the proposed security architecture is demonstrated through the implementation of this test vehicle. This research elucidates a logic process model with functional specifications to be used as development guidelines and functional assessment for conforming implementations.

Section 2 reviews three national index-based e-health initiatives and identifies the relationship of their strategies to the authors' approach. Section 3 reports on the test vehicle background which is based on our previous work. The purpose, scope, and selection of software development tool sets of this test vehicle are detailed in Section 4. Section 5 lists the structure of the test vehicle with logic process modules and provides a description of one exemplary functional requirement specification. Section 6 uses two scenarios to illustrate the key information flows within the implementation of the test vehicle. An analysis of the test vehicle implementation is presented in Section 7. Finally, our conclusion is presented and suggestions are made for further research.

2 RELATED WORK

Numerous countries across the globe have a national e-health initiative at some stage of investigation or implementation. This section outlines three national index-based e-health architectures and identifies the relationship of their strategies to the authors' approach.

2.1 Australia's National E-health Strategy

Australia's national e-health approach adopts a concept of a distributed Individual Electronic Health Record (IEHR) which is expected to be developed across geographic regions, according to the strategic directions specified in the Australian Government's National E-Health Strategy (2008). IEHR has been referred to as the Personally-Controlled Electronic Health Record (PCEHR) by the Australian Government (Morris 2011). The PCEHR system intends to contain summarised patient health information which aggregates the health records coming from original health information into integrated records across multiple locations. Australia's national e-health strategy also acknowledges that a central indexing or addressing mechanism is needed to link related health records which may

[1] NEHTA was established to accelerate the adoption and progression of e-health in Australia in 2005.

reside in one or more locations. NEHTA provides a design and implementation guide on Endpoint Location Service (ELS) (2009) for indexing purposes.

Significantly, the protection of e-health information security plays a critical role in the success of any e-health implementation (National E-health Transition Authority 2008a). In response to this concern, this paper proposes a security architecture for index-based e-health environments, based on the broad outline of Australia's National E-health Strategy (2008a), NEHTA's Connectivity Architecture (2008b), and NEHTA's ELS Implementation Guide (2009). The proposed architecture demonstrates a logic model for indexing and supports secure communications between healthcare providers and the Index System (Sections 5 and 6).

2.2 Canadian Electronic Health Record (EHR) Solution

Canada's national e-health architecture, outlined in the Electronic Health Record Solution (EHRS) Blueprint (Canada Health Infoway 2006, 2008), comprises all subsets of jurisdictional EHR systems. Each jurisdictional EHR system consists of integrated and cross-referenced health data replicated from source data systems. Canada's EHRS Blueprint is a highly cross-referencing and index-based scheme linking relevant health records located at various registries and repositories. With Canada's EHR approach, each participating healthcare entity interacts with the jurisdictional EHR system via a message broker called the Health Information Access Layer (HIAL) to upload and retrieve shared health data from the EHR system.

The HIAL element is part of Canada's EHR Infostructure (Canada Health Infoway 2006, 2008), acting as a gateway to provide a collection of services between the EHR services and participating healthcare systems. The technology infrastructure of HIAL exists "in the cloud," and does not reside at the healthcare entity's end. This is in contrast to the proposed Healthcare Interface Processor (HIP) facility. Namely, this research uses a HIP facility which resides at each participating healthcare site to provide a secure communication channel for an untrusted health information system connected to the main Index System. In addition, the proposed HIP facility acts as an interface/gateway for a healthcare provider's system to connect to other health information systems to exchange health information in a secure and reliable manner.

2.3 German National E-health Project

The architecture of the German national e-health project, Telematics (Blobel & Pharow 2007; Jürjens & Rumm 2008), comprises three major components:

(1) Local health systems connected to the national e-health platform (bIT4Health) for accessing central services of the Telematics infrastructure through a gateway interface, bIT4Health Connector. The Connector, a hardware-based facility or integrated software with an information system, is installed at the local health system site to enable semantic interoperability and to provide data security services;

(2) The central Telematics platform provides three subsystems: (i) Generic Common Services; (ii) Common Services; and (iii) Security Services. The Security Services subsystem of interest to this research is needed to access shared health data, such as authentication, authorisation, the signature timestamp, and access logging; and

(3) The backend system, which provides a set of resource providers to manage accessible data stores and external services.

The design of the bIT4Health Connector and the proposed HIP facility share the following basic features:

- Both are installed at the local health system site; and
- Both act as a gateway/interface between the central service system and the local health system for the provisioning of semantic interoperability.

In contrast, the major differences between the bIT4Health Connector and the proposed HIP facility are as follows:

- The HIP facility builds on a trusted system to provide a resilient platform to carry out its tasks from Layers 1 to 7 of the seven-layer OSI model; and
- HIP not only intends to enable semantic interoperability for healthcare information exchange, but also provides critical security services, including presenting a trusted path to the national e-health infrastructure, mutual authentication, data protection, accountability, and operational flexibility with an emergency override function.

3 TEST VEHICLE BACKGROUND

To access an individual's health records from disparate sources, health record indexing services provide lookup services for finding the source locations of health information, and even for the connection requirements for accessing the repository of health data. In our previous paper (Liu et al. 2010), we proposed a secure architecture for an index based e-health environment based on the strategic directions from the Australian Government's National E-health Strategy (2008), and NEHTA's proposed Connectivity Architecture (2008b) and ELS (2009). Figure 1 illustrates the proposed connectivity architecture with the required structures to support secure communications in the national e-health environment, including: (i) The Index System itself; and (ii) the proposed Healthcare Interface Processor (HIP) facility.

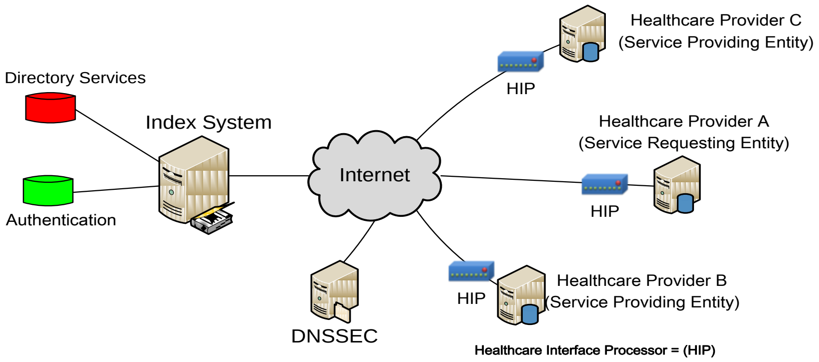

Figure 1. A Secure Architecture for Index-Based E-health Environments

The Index System, a centralised facility run at a national level, should be built on a high-trust computer platform to perform authentication and indexing services. The design rationale underlying HIP, a resilient and qualified facility built on top of a trusted base-embedded hardware and software platform, is to act as a proxy server to establish a secured communication channel connecting to the Index System and for health information exchange between healthcare providers. This design could isolate a potentially hostile or compromising system connected to the national e-health network. Wherever a connection to the national indexing system is required, a HIP facility has to exist in some form.

Generally, health information is stored across a number of different health information systems. A national Index System must be available for the provision of directory services to determine the distributed locations of the source systems holding the related health records. This architectural model draws on important lessons from the Internet's Domain Name System (DNS).[2] This approach embraces the hierarchical and distributed nature of DNS, and defines the required components for a secure architectural design in a national e-health scheme. This architecture also mandates that participating healthcare providers need to adopt a high-trust interface module, the proposed HIP, as the application proxy to connect to the Index System, as well as to link to other health information systems.

A first point of contact in any Index System must itself be verified for authenticity and integrity. In Internet terms, the client system must be certain that it is connected to the correct Index System and

[2] RFC 1034 provides an introduction to the DNS functions and protocol for standard data and query types.

not to some fraudulent system or via some intermediate node point capable of monitoring all traffic. A fundamental security issue must therefore be addressed, viz. the veracity of domain names. Trusted domain name resolution services are a critical element in the overall trusted architecture of any index-based healthcare system to combat attacks on the system, such as name resolution cache poisoning, and traffic diversion/monitoring attacks. This security architecture not only provides an indexing service, but also incorporates a trusted name resolution scheme for the enforcement of security in communicating with the authorised Index System.

This research concentrates on the Australian national e-health environment from a security perspective. However, this proposed architecture could be equally applied to any distributed, indexed-based healthcare information system involving referencing of disparate health data collections or repositories.

4 IMPLEMENTATION DECISION

This section describes the purpose and scope of the development of the test vehicle, as well as the decision made as to the selection of software development tool sets.

4.1 Purpose for the Prototype Development

The primary objective of this implementation has been to determine the parameters needed for an appropriate evaluation of any index-based, e-health system project. To date, our research has identified the normal and obvious parameters of the need for optimised performance, coupled with acceptable levels of system security. In fact, this test vehicle indicates a number of additional parameters that need to be considered in any large-scale experimental design, including:

- Clarity and comprehensibility of the overall architecture and allied specifications to enable ready development of prototype systems;
- The need for evaluation of the level of education, training and expertise required by ICT professionals to create and manage such systems; and
- Determination of the guidelines for the creation and assessment of experimental information systems and the associated configurations chosen for the development of such systems.

These three parameters have been readily determined even though the experiment performed was of a minimal nature.

4.2 Prototype Scope

This proposed architecture concerns the development of a secure architecture design to facilitate patient information sharing and data collection via a national Index System. For demonstration purposes, this paper describes a test environment that consists of a simulated single national Index System and three participating healthcare organisations.

The national Index System in the test environment performs fundamental services, including authentication and directory services. It provides basic authentication services to verify the identity and credentials of healthcare providers; nevertheless, the focus of this paper is to demonstrate the operation of the indexing services themselves. For test reasons, we have used a conventional username/password authentication mechanism. This module, however, will allow for the incorporation of token-based authentication mechanisms as required. The experimental Index System will provide lookup index referencing to the healthcare service requesting-entity to locate the healthcare information stored at various locations. The Index System facilitates the healthcare service entities in their need to deposit index references for patient records on the Index System.

One healthcare service entity simulates a role of a service requesting-entity, referring as the entity that uses a service provided by another entity. The other two healthcare entities act as service-providing entities that offer health information to another entity.

4.3 Selection of Software Development Tool Sets

Since open-source software has risen to great prominence, we have acquired software development tool sets for this prototype based on the concept of open-source technology development. The particular software has been chosen against the contexts of reliability, sustainability, performance, efficiency, accessibility, security, portability, interoperability, total cost of ownership, and maintenance. The selected software development tools are listed in Table 1:

Web Services framework	Data Access Connection Management (interface)	JNDI
	Web Services Description Language (WSDL)[3] converter	Axis2
	Web Server	Tomcat
Programming language		Java
Database Management System (DBMS)		Derby
Operating System		Ubuntu

Table 1. Development Tool Set

5 PROTOTYPE STRUCTURE

Figure 2 illustrates that the prototype structure consists of one national Index System and three participating healthcare entities managing their own healthcare information systems. The Index System is a centralised system run at a national level providing authentication and indexing services. Of the three healthcare service entities, one plays the role of a service-requesting entity, and the others act as service-providing entities.

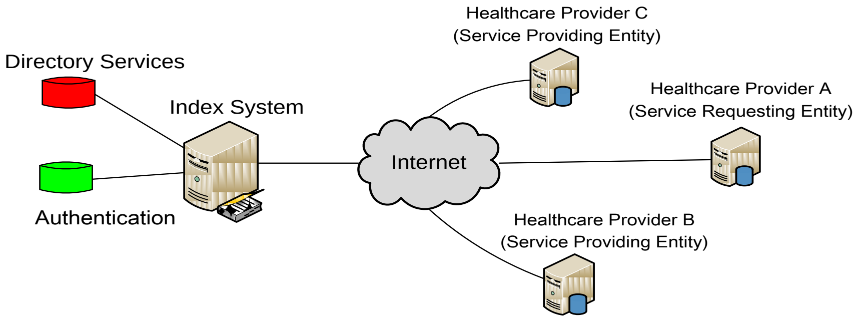

Figure 2. Prototype Structure

5.1 The Simulated Index System

Generally, health information is stored over a number of various incompatible health information systems. Indexing services must be available for the provision of directory services to maintain location information for the source systems holding the related health data. The main functions of the Index System should include: (a) authentication services; and (b) publication and discovery healthcare to information services. As various healthcare organisations may have their own specific access to authorisation requirements and processes, privilege management is performed by service providers locally.

In the prototype, the Index System links to an authentication database and directory service repository. The interface used to access the directory services of the Index System is a WSDL interface implementation. The Index System is constructed on Ubuntu and deploys a Web Services stack including:

- Tomcat Web Server, which acts as an enabling platform for the implementation of Axis2 and JNDI;

[3] WDSL is used to describe how to access network services in XML format. More detail is available at http://www.w3.org/TR/wsdl#_introduction, viewed 17/02/2010.

- Axis2, which acts as a Web Services engine for generating and implementing healthcare applications on a Web Services platform consistent with WSDL specifications; and
- JNDI, which is deployed to manage data connections between the healthcare applications and the DBMS.

For the technical implementation of directory services, each participating healthcare organisation in the national e-health scheme is required to submit its service locator information to the Index System. The submitted information includes the organisational healthcare provider identifier system Uniform Resource Locator (URL), and associated public key. When a new patient record is created on the health information system, the health information system will send an index reference for the new patient record along with its organisational healthcare provider identifier to the Index System. A lookup operation searches for any entry matched with a patient's Individual Healthcare Identifier (IHI) and returns an aggregated list of service instances. The aggregation list of service instances identifies the target system location and information necessary for service invocation. From a database structure perspective, Figure 3 illustrates two exemplary tables and a view (virtual table) in the directory service database: (a) Service Location; (b) Index Reference for Patient Records; and (c) Service Instance View.

The Service Instance View comprises the query results on the target systems which hold the identified patient's health data aggregated from (a) and (b) above.

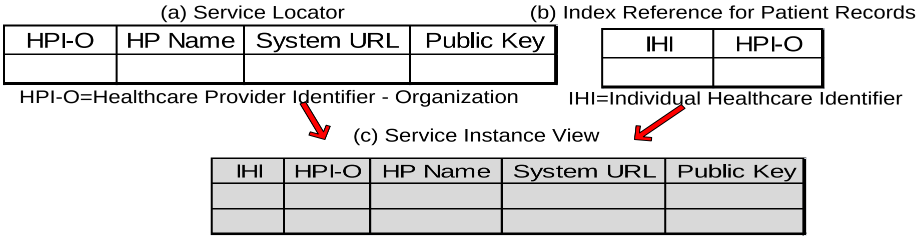
(a) Service Locator
HPI-O
HP Name
System URL
Public Key
(b) Index Reference for Patient Records
IHI
HPI-O
HPI-O=Healthcare Provider Identifier - Organization
IHI=Individual Healthcare Identifier
(c) Service Instance View
IHI
HPI-O
HP Name
System URL
Public Key

Figure 3. Example of Tables and View of the Directory Service Database

The prototype implementation of the Index System consists of the following system processes to provide authentication, publication, and discovery for healthcare information services:

- Service Locator Registration and Update;
- Index Reference for Patient Records;
- Acceptance of Lookup Query;
- Authentication Operations;
- Resolution of Lookup Query; and
- Delivery Resolution for Lookup Query.

A functional requirement specification provides a description of a particular system process, as well as identifies the data parameters to be entered into that system process. Owing to paper-length limitations, the functional requirement specifications of the system processes listed above are not included in this paper but are available on request.

5.2 Virtual Health Information Systems

In general, participating healthcare organisations within a national e-health scheme may use disparate healthcare information systems across multiple platforms. With this test environment, however, we set up the three healthcare organisations to deploy their own healthcare information systems based on the same open-source architecture and software. The main reason for using the same structure for the three healthcare information systems in the test environment is that each participating healthcare organisation implements a consistent Web Services interface to support service provision and invocation; therefore, interoperability can still be achieved. In the test environment, the health information system implements service provision and invocation in WSDL through support of Web Services interfaces.

Each virtual healthcare information system resides on the Ubuntu operating system and deploys its own healthcare Web services framework, including:

- Tomcat Web Server, which acts as an enabling platform for the implementation of Axis2 and JNDI;
- Axis2, used as a convertor between Java classes and the WSDL format;
- JNDI, used to manage data connections;
- Derby, deployed as the Database Management System; and
- Java applications to invoke and/or provide healthcare services.

A healthcare service entity can play two major roles: as a (i) healthcare service-requesting entity and/or a (ii) healthcare service-providing entity. A service-requesting entity refers to the entity that uses a service provided by another entity. A service-providing entity is an entity that offers a service used by another entity. A service-providing entity can be a healthcare provider, healthcare organisation, or organisation commissioned to provide services for healthcare providers or healthcare organisations.

In the prototype, the healthcare service-requesting system includes the following system processes:

- Request for Service Locator Registration and Update;
- New Patient Creation;
- Lookup Query Handler;
- Reception for Query Resolution; and
- Service Invocation for Patient Data.

The system processes of the healthcare service-providing system in the prototype include:

- Reception for Patient Data Request;
- Token Verification;
- **Authorisation Logic;**
- Retrieval of Patient Data
- Response to Emergency Access Override;
- Delivery of Requested Patient Data; and
- Notification for Available Health Reports.

Due to paper-length limitations, this paper can only provide an exemplary description of functional requirement specifications from one of the system processes listed above, Authorisation Logic.

5.2.1 An Exemplary Description of Functional Requirement Specification – Authorisation Logic

The purpose of this system process is to make an access decision upon a patient data request is received at the healthcare service-providing system. The Reception for Patient Data Request process passes the authentication token to the Token Verification process to validate the authenticity of the token. Upon successful token verification, then the requesting healthcare provider's identifiers (i) HPI-O; (ii) HPI-I; and (iii) patient's IHI are passed to the Access Authorisation process. If the access is allowed, the Retrieval of Patient Data process retrieves the request data, or else the Authorisation Logic process produces an "access denied" message.

Not only does the Authorisation Logic process carry the "Sensitivity Label" mechanism outlined by NEHTA (2008c), but also extends this with "inclusive access" and "exclusive access" provisions to support a finer level of granularity for consent. NEHTA argues that it is necessary to have the "Sensitivity Label" function in place for health data. This enables individuals and their healthcare providers to have the appropriate level of access allowable over sensitive health data. NEHTA suggests two label categories: (i) "Clinical Care", and (ii) "Privileged Care." The "Clinical Care" label normally refers to clinical information that may be accessed by all healthcare providers involved in the healthcare of the patient. Health data labelled as "Privileged Care" can only be accessed by healthcare providers who have been nominated by the patient. NEHTA's approach uses a coarse granularity for consent. This may not be sufficient to meet the situation where information access control needs to be enforced at a finer level of granularity, however. In contrast, this research represents the following access rules, with the flow chart shown in Figure 4.

The inclusive and exclusive access lists should be defined by patients in conjunction with advice from their healthcare providers when health information is created. Normally, patients make decisions on who is allowed to access their health information. Patients with reduced decision-making capacity may need to compromise some level of their health information privacy to receive the most effective health services.

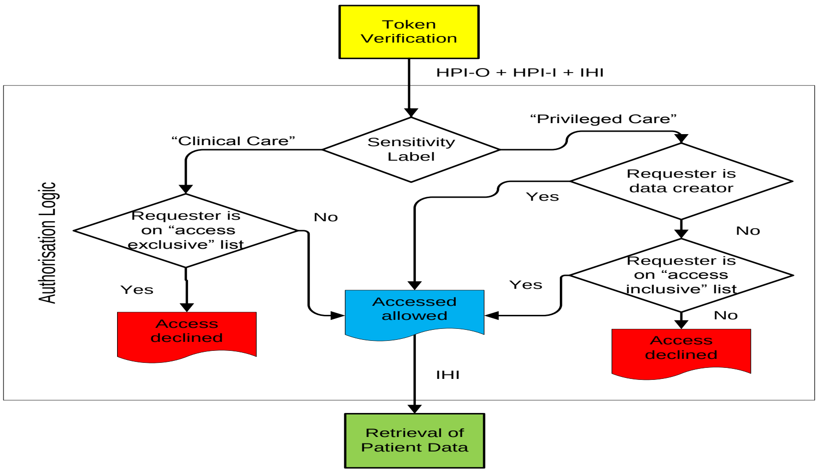

Figure 4. Flow Chart for Authorisation Logic

6 KEY INFORMATION FLOWS

Scenario 1 shows how the proposed system carries out security measures, including authentication, confidentiality, integrity, access control, and transmission security. Scenario 2 demonstrates how the proposed system provides the flexibility of having an emergency override function by switching to a defined emergency policy while activating audit trail functions.

- Scenario 1: A new patient's medical history enquiry; and
- Scenario 2: Emergency override access.

6.1 Enquiry for New Patient's Medical History

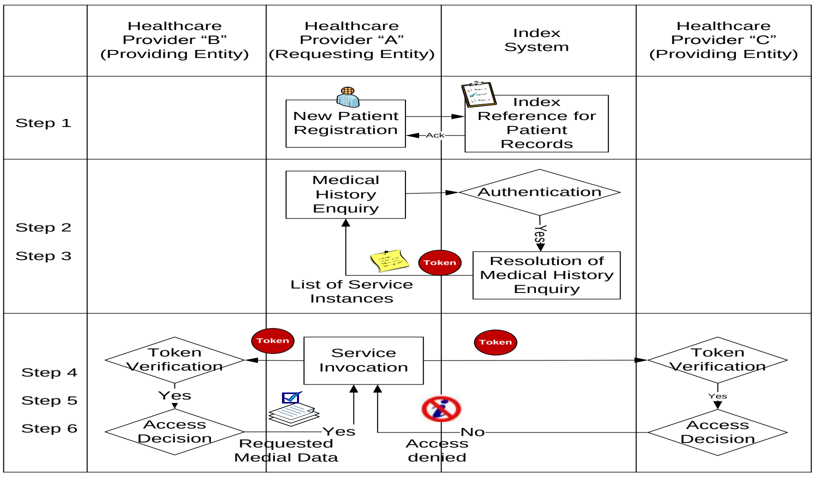

Figure 5. Enquiry for New Patient's Medical History

A new patient, Peter, presents himself for the first time to a medical clinic "A" to seek medical attention. The treating physician in the medical clinic A, David, needs to access Peter's medical history to enable more effective and efficient diagnosis and treatment. It is assumed that David has no prior knowledge that Peter's medical history is located at medical clinics "B" and "C." In this case, the medical clinic A acts as a healthcare requesting entity. "B" and "C" play a role as healthcare service-providing entities. Peter's medical data held at B is labelled "Clinical Care," but Peter's mental medical data held at C is labelled "Privileged Care." David queries the Index System for the source of Peter's medical data. Upon successful authentication, the Index System responds to the request with the source of medical history and signed token for service invocation. David presents the authentication token to medical clinics B and C to request Peter's medical data. As a result, the medical clinic B provides the requested data. The medical clinic C, however, declines the data request because David is not authorised to access Peter's medical data labelled "Privileged Care."

Figure 5 illustrates the key information flows of the interactions between the healthcare requesting entity, Index System, and healthcare service-providing entities with the consequent steps. Meanwhile, this illustration presents how the proposed system architecture can enable secure communications between healthcare providers and the Index System in the national e-health environment.

Note that all request and response messages prior to transmission are signed and encrypted for confidentiality, authentication, and message integrity purposes.

1 **A New Patient Registration**

1.1 A new patient, Peter, is registered in A's health information system.

1.2 A's health information system sends a request to enrol this new patient index to the master Index Reference for Patient Records on the Index System.

1.3 Once index reference enrolment to Index Reference for Patient Records on the Index System is successful, the Index System sends an acknowledgement to A.

2 **Medical History Source Enquiry**

2.1 To be able to query the directory services, a requesting entity must be presented to the Index System with its identity and credentials, including Healthcare Provider Individual Identifier and the affiliated Healthcare Provider Organisational Identifier. David logs onto the Index System with A's HPI-O and David's HPI-I.

2.2 Upon successful authentication, David queries the source of Peter's medical history.

3 **Resolution of Medical History Source Enquiry**

3.1 The Index System searches the master patient index references based on the entry matched to Peter's IHI.

3.2 There are two matched entries found in this case. The Index System then responds with a signed token, coupled with the list of the service instance information for service invocation.

4 **Service Invocation**

4.1 David contacts B to request Peter's medical history with the signed token and other necessary information for service invocation.

4.2 David also contacts C to request Peter's medical history with the signed token and other necessary information for service invocation.

5 **Service Provision from the Medical Clinic B**

5.1 B validates the signed token and request.

5.2 Upon successful verification, B makes an access decision based on David's profile against Peter's medical data.

5.3 Peter's medical data held at B's health information system is labelled as "Clinical Care", so David's access request is granted.

5.4 The requested data is sent to David.

6 **Service Provision from the Medical Clinic C**

6.1 C validates the signed token and request.

6.2 Upon successful verification, C makes an access decision based on David's profile against Peter's medical data.

6.3 Peter's medical data is labelled as "Privileged Care" at C's health information system, but David's is not on the "inclusive access" list to access Peter's sensitive medical data, so David's access request is declined.

6.4 The request declined message is sent to David.

6.2 Emergency Override Access

There are some cases when medical data must be accessible even in the absence of authorised permission. For example, if the authorised viewer of a patient's case file is not present, but the patient requires emergency treatment, then the availability of the information is more important than its privacy. The service-providing system is programmed to respond to the request for emergency access.

Figure 6 shows the interactions between the healthcare-requesting entity, Index System, and healthcare service-providing entities in an emergency. This illustration also justifies how the proposed system architecture provides the flexibility of having timely access to the requested data with an emergency override function while activating audit trail functions in such circumstances.

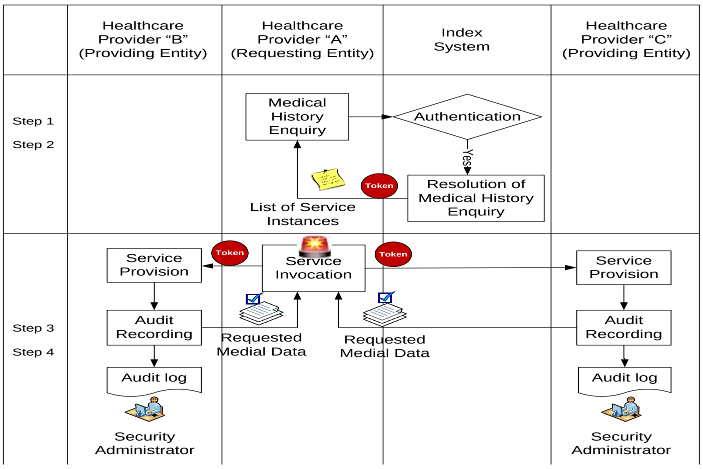

Figure 6. Emergency Override Access

Note that all request and response messages prior to transmission are signed and encrypted for security purposes.

1 **Medical History Source Enquiry**
The emergency services attending physician queries the Index System for the source of the patient's medical history with the physician's identity and credentials and the patient's IHI.

2 **Resolution of Medical History Source Enquiry**
The Index System searches the master patient index references based on the entry matched to the patient's IHI. The Index System then responds with a signed token coupled with the list of the service instance information for service invocation to the requesting entity.

3 **Service Invocation**
The service requesting entity presents the signed token to the healthcare service-providing entity for an emergency access to the patient's medical history.

4 **Service Provision**
After the healthcare service-providing entity validates the signed token, the process moves into auditing mode without passing through the access decision-making process. To improve privacy accountability and consumer trust through audit trails, the audit trail records who accessed the data and when the data was accessed. The security administrator and patient should be notified of the detection of any unauthorised access.

7 RESULTS AND ANALYSIS

This prototype project used approximately 288 hours of development effort. This includes times for (i) understanding the architecture and system specifications; (ii) selecting development tool sets; (iii) coding, testing and debugging; and (iv) system documentation. This prototype development was undertaken as a postgraduate student project by working 24 hours per week, completed over 12 weeks during one semester. The prototype developer had three years of practical experience working within the IT industry as an application programmer familiar with Java, JSP, Tomcat, and Oracle database systems. At the beginning of prototype development, to create the healthcare application integration structure based on Web Services, the developer had to self-educate on how to develop distributed Web-based applications using the Simple Object Access Protocol (SOAP) [4] and WSDL specifications.

Although this experiment has been performed in a minimal manner, the successful completion of this prototype demonstrates the comprehensibility of the proposed architecture as well as clarity and feasibility of system specifications for enabling ready development of such a system. As demonstrated, to create such a prototype system does not require high levels of specialised system development expertise.

This paper describes the technical aspects of the procedures involved in the development of the test vehicle for the proposed security architecture. The result of this paper is useful for providing development guidelines and functional assessment for conforming implementations. This experiment has been to ensure that the system specifications may be readily understood and implemented within a reasonable timeframe and with modest resources. Scalability issues, however, have been not addressed in this experiment.

For the purpose of system analysis, the Australian Government's National E-health Strategy (2008) Index Scheme proposal has been used as particular framework in the research undertaken. This research, however, may be more generally applied to any distributed, indexed-based healthcare information systems involving index referencing of disparate health data collections.

The implementation of DNS Security Extensions (DNSSEC)[5] (Arends et al. 2005a, 2005b, 2005c) has not been incorporated within the test environment, however. For overall trust, DNSSEC would be assumed as a mandatory component to combat the recent increase in DNS cache poisoning and traffic diversion attacks. It is assumed that the first step is to perform the enforcement of trusted communication to the authorised Index System prior to the interactions between the service-requesting entity and the Index System. To achieve this, from a technical underlying process, the health information system should be pre-configured to contact a DNSSEC-capable server to perform a trusted name resolution. This enables the server to defend against false DNS data and to assure that connections are only established with the legitimate Index System.

There is one master Index System and three participating healthcare service entities in the test environment. The Index System is a centralised service implemented at a national level; however, it should be replicated for resilience purposes. This resilient pattern can be seen in the hierarchical and distributed structure of the DNS.

In this test environment, each healthcare service entity connects to the national e-health network system without using the proposed application proxy facility - HIP. It is envisaged that HIP should be used to provide a secured communication channel for an untrusted health information system connected to the Index System, as well as for health information exchange between healthcare providers. Wherever a connection to the national indexing system is required, a HIP facility has to exist.

The authors argue that the load of the national Index System should be relatively lightweight to be able to perform e-health indexing services efficiently. This can mitigate against Index System explosion and traffic bottleneck risks. Such an approach is favourable in a geographically large country such as Australia. To be scalable and to provide effective and efficient operation, the access control and authorisation process is best performed close to where the source system is. This is because each healthcare service provider might implement the service differently based on its own health information system access requirements. Additionally, this prototype system extends the "Sensitivity Label" mechanism outlined by NEHTA (2008c) with "inclusive access" and "exclusive

[4] SOAP, a platform-independent protocol, normally uses HTTP/HTTPS as the mechanisms for exchanging XML-based messages over networks.

[5] The DNSSEC, through use of Public Key Cryptography, enables DNS "zones" to "digitally sign" the necessary nameserver tables so that, on distribution, such tables can be checked for authenticity and integrity by the receiver.

access" provisions to support fine-granular access control constraints. Further experimentation would be valuable to elucidate requirements in other regimes and architectures.

The United States' *Health Insurance Portability and Accountability Act (HIPAA) 1966* was enacted to encourage a move towards electronic health information systems, while requiring safeguards to protect security and privacy. The Resource Guide for Implementing the Health Insurance Portability Accountability Act (HIPAA) Security Rule (Hash et al. 2008) provides guidelines for the implementation of the technical safeguards specified in the HIPAA Security Rule. These guidelines cover access control, audit control, integrity, authentication, and transmission security. This research meets all the requirements of the technical safeguards mentioned in this resource guide. One of the access control management activities in this resource guide addresses implementation of the mandatory requirement to "establish an emergency access procedure." This research meets the requirement by providing the flexibility of having an emergency override function by switching to a defined emergency policy in such circumstances, while activating vigorous audit trail functions. In addition, this research ensures that all information prior to transmission is digitally signed and encrypted for confidentiality, authentication, and message integrity.

8 CONCLUSION AND FUTURE WORK

The successful completion of this prototype development has achieved the following anticipated outcomes:

- The proposed architecture is comprehensible and feasible to enable ready development of prototype systems;
- The creation of such a prototype system does not require high levels of specialised system development expertise, assuming all cryptographic functions are provided;
- The logic model outlined in this paper can be used as development guidelines and assessment for the functionality of conforming implementations; and
- The proposed architecture has met all the requirements of the Resource Guide for Implementing the Health Insurance Portability Accountability Act (HIPAA) Security Rule (Hash et al. 2008).

This prototype development was not aimed at performance and scalability testing of the proposed architecture. Nevertheless, performance and scalability represent two factors that need to be carefully examined in the development and deployment of any e-health record system. Such analysis is, however, out of the scope and resources of the current project and must be left to future work. It is essential to test the scalability and performance of the proposed architecture against a high order of magnitude in health record infrastructure in the future.

This prototype is developed under a general-purpose operating system that is a "Discretionary Access Control (DAC)" system. It is intended that the system structure be migrated to a more secure platform supporting "Mandatory Access Control (MAC)"-type principles usual in a trusted operating system. Since the indexing services and health information exchange are mission critical, the index system and health information systems must be protected from internal and external threats through the use of modern "Flexible Mandatory Access Control (FMAC)" structures. Under such an operating system, and as distinct from the less secure DAC-based systems, even a system administrator may not have permission to access the health record data. In these systems, there is no "super-user" capable of obtaining access to all system resources at any time. If an individual subsystem is "captured," propagation of exposure will not extend beyond the compromised subsystem itself, a vital concern in any e-health environment, including the "Labelled Security Protection Profile (LSPP)" of international standard ISO/IEC15408.

Part of our future work is to build a HIP prototype. The HIP prototype development is a non-trivial task, which requires sustained collective efforts to incorporate the prescribed provisions, including security, ease of use, flexibility, interoperability, and resilience features. It is intended that such HIP development would involve the production of a number of laboratory prototypes and even the creation of a small production prototype run. The proposed secure and resilient architecture for compliance in index-based e-health environments is therefore timely and critical at present.

References

Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S. (2005a). *RFC4033 DNS Security Introduction and Requirements*, viewed 07/09/2009, <http://www.ietf.org/rfc/rfc4033.txt>.

---- (2005b). *RFC4034 Resource Records for the DNS Security Extensions*, viewed 07/09/2009, <http://www.ietf.org/rfc/rfc4034.txt>.

---- (2005c). *RFC4035 Protocol Modifications for the DNS Security Extensions*, viewed 07/09/2009, <http://www.ietf.org/rfc/rfc4035.txt>.

Australian Health Ministers' Advisory Council (2008). *National E-Health Strategy Summary*, viewed 1/09/2009, <http://www.health.gov.au/internet/main/publishing.nsf/Content/National+Ehealth+Strategy>.

Blobel, B. and Pharow, P. (2007) A model driven approach for the German health telematics architectural framework and security infrastructure, *International Journal of Medical Informatics*, 76 (2), 169 -175.

Canada Health Infoway (2006). *EHRS Blueprint Executive Overview*, viewed 15/06/2010, <http://www2.infoway-inforoute.ca/Documents/EHRS-Blueprint-v2-Exec-Overview.pdf>.

---- (2008). *A "Conceptual" Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2*, viewed 19/05/2010, <http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf>.

Hash, J., Bowen, P., Johnson, A., Smith, C.D. and Steinberg, D.I. (2008). *NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, viewed 22/10/2010, <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>.

Jürjens, J. and Rumm, R. (2008) Model-based security analysis of the German health card architecture, *Methods of Information in Medicine*, 47 (5), 409-416.

Liu, V., Caelli, W., Smith, J., May, L., Lee, M., Ng, Z., Foo, J. and Li, W. (2010). Secure Architecture for Australia's Index Based E-health Environment In *Proceedings of the The Australasian Workshop on Health Informatics and Knowledge Management in conjunction with the 33rd Australasian Computer Science Conference* Brisbane, Australia.

Morris, M. (2011). *PCEHR System Overview*, viewed 10/02/2011, <http://www.health.gov.au/internet/main/publishing.nsf/Content/A30BBA1FBD5C9870CA2578220071D7E1/$File/PCEHR%20System%20Overview%20-%20Speech%20Notes.pdf>.

National E-health Transition Authority (2008a). *Privacy Blueprint for the Report on Feedback Individual Electronic*, viewed 01/09/2009, <http://www.nehta.gov.au/component/docman/doc_download/587-privacy-blueprint-for-the-iehr-report-on->.

---- (2008b). *Connectivity Architecture Version 1.0*, viewed 29/07/2010, <http://www.nehta.gov.au/component/docman/doc_download/624-connectivity-architecture-v10->.

---- (2008c). *Privacy Blueprint for the Individual Electronic Health Record*, viewed 9/05/2010, <http://www.audiology.asn.au/pdf/NEHTA_Privacy_Blueprint.pdf>.

---- (2009). *Endpoint Location Service Implementation Guide Version 1.2*, viewed 30/12/2010, <http://www.nehta.gov.au/component/docman/doc_download/795-endpoint-location-service-implementation-guide-v12>.

---- (2010). *Connectivity Introductory Guide Version 1.1*, viewed 25/10/2010, <http://www.nehta.gov.au/component/docman/doc_download/1041-connectivity-introductory-guide-v11>.