An Agent-based Infrastructure for Secure Medical Imaging System Integration

Weina Ma and Kamran Sartipi
Department of Electrical, Computer and Software Engineering
University of Ontario Institute of Technology
Oshawa, ON, L1H 7K4, Canada
{*Weina.Ma, Kamran.Sartipi*}*@uoit.ca*

Abstract

This research paper examines the weaknesses of the trusted models applied on the domain of medical image sharing between the PACS (Picturing Archiving and Communication System) and image-enabled EHR (Electronic Health Record) systems. In this paper, we propose implementing an agent-based infrastructure in the legacy PACS systems along a common infrastructure that we have proposed in our earlier work. The proposed architecture allows for capturing PACS communication messages; identifying users; extracting user actions to feed into an action-based access control mechanism; and integrating with modern authentication and authorization technologies (OpenID and OAuth). We also provide a UML model for the patient consent directives to allow for systematic enforcement of their impact on the proposed access control technique. Finally, we implemented a prototype of the proposed architecture using open source tools to demonstrate the feasibility and extendibility of our proposed solution.

Keywords: Security; Medical imaging; PACS; DICOM; Multi-agent; Access Control; EHR; Consent Directives.

1 Introduction

Diagnostic Imaging (DI) solutions maintain and manage patient radiology images (e.g., CT scans, Xray, MRI, ultrasound), and their corresponding written reports in digital formats, for the purpose of diagnosis, treatment improvement or medical science research. Radiology images and reports constitute a vital part of patient's EHR and the PACS systems are responsible for storage, distribution and display of medical images for interpretation and review by the clinicians [1]. Over the past decades PACS systems have taken an increasingly important role in the workflow of DI solutions in a single radiology department. PACS systems are complex integrated systems equiped with the necessary hardware and software to integrate: digital image acquisition devices namely modalities (e.g., CT scanner, MRI system); digital image archives where the acquired images are stored; and workstations where radiologists view the images. DICOM (Digital Imaging and Communications in Medicine) is the universal standard for PACS image storage and transmission, which defines the file format and network communication protocol. DICOM is based on a client-server model, however it does not transfer user information between parties. Without appropriate user information it is impossible to securely integrate PACS systems with the common infrastructure and implement further access control polices and audit trails. A new feature "User Identity Negotiation" [2] is available as an optional mechanism to DICOM standard; however its implementation is not commonly adopted by the PACS vendors.

A federated DI domain allows for centralized image capturing, long-term archiving and non-proprietary sharing of radiology information across a large distributed network. Since medical data contains sensitive information that may affect the lives of people, security and privacy aspects of DI systems must be primarily concerns in sharing images within a federated PACS and EHR systems. In the case of the Canadian Diagnostic Imaging Repository (DIr) projects, compliance with security control requirements is achieved through a trusted model where each local diagnostic imaging system is responsible for ensuring that personal health information is adequately protected [3]. A key challenge with this trusted model is the lack of federated capabilities as follow: i) user authentication is local to each system that imposes a significant administrative burden to ensure that individuals are uniformly identified in each sys-

Acknowledgement. This research was conducted with collaboration of Dr. David Koff and Dr. Peter Bak and Ms. Jane Castelli at MIIRC@M Centre of McMaster University. This research was funded by an ORF grant for the project "Secure Intelligent Content Delivery System for Timely Delivery of Large Data Sets in a Regional/National Electronic Health Record".

tem; ii) access control rules are local to each system, i.e., consistency of access rules across all systems has to be managed manually; iii) patient consent directives and their impact on access control are not communicated automatically to each system; and iv) existing PACS systems are comparatively closed systems without external interface.

In an earlier work [4], we proposed a common infrastructure that suggested the use of techniques and standards such as: cooperative multi-agents, single sign-on service OpenID, OAuth authorization flow, action-based access control mechanism, and behavior-pattern based security policy enhancement. We are enhancing this overall infrastructure by integrating with legacy PACS systems. In this paper, we propose a solution to seamlessly integrate heterogeneous PACS systems with this common infrastructure. The main contributions of this paper include:

- *Establishing identity of PACS users*: by employing adaptive agents in each PACS system to provide user identity negotiation mechanism, and then authenticate established users against common infrastructure, without any upgrade to the existing PACS systems.
- *Data acquisition and user action extraction*: by deploying acquisition agents inside existing PACS systems to capture communication messages, and then gather user "Action Tuple" properties (i.e., user name, command, action, medical image ID, patient ID, etc.) through a DICOM standard analyser. These properties are applied to feed the evaluation of consent-directive-based access control and action-based access control.
- *Patient electronic consent directive model*: by providing consent directive access control policy scheme to represent and transform paper-based consent directive forms. We utilize UML model to present such privacy access control polices, which helps PACS administrators manage consent directives electronically.

The remaining of this paper is organized as follows. Section 2 describes the work related to our approach. In Section 3 we discuss the underlying technologies used in our designation. In section 4 we describe our approach and implementation in detail, and present how it will be applied to our common infrastructure. Section 5 includes an end-to-end case study to demonstrate how the proposed approach works. Finally, Section 6 provides a brief discussion and concludes our paper.

2 Related Work

IHE (Integrating the Healthcare Enterprise) is an initiative by healthcare professionals and industry [5] which aims to set up consolidated healthcare information sharing through standard based approaches. It guides enterprises in using established standards such as DICOM and HL7 (Health Level Seven) to accomplish interoperability based on existing IT infrastructure. In practice, a provincial DI-r communicates with distributed PACS and RIS (radiology information system) relaying on the infrastructure promoted by IHE cross-enterprise document sharing for imaging (XDS-I) integration profile [6], as well as a set of security and privacy profiles [6] in compliance with the health insurance portability and accountability act (HIPAA) regulations.

David S. Mendelson and Peter R. G. Bak evaluated IHE and the evolution of image sharing from file to transportable media (e.g., compact disks) to direct electronic exchange over the Internet [3]. A real-world example of networks, Philadelphia Health Information Exchange (PHIE) and Jersey Health Information Exchange (NJHIE), was used to demonstrate the IHE-compliant infrastructure and integration with PACS/RIS systems, regardless of vendors. Besides, through addressing a grid computing based infrastructure called *caGrid*, the paper highlighted advantages of using grid computing to emphasis on security, authentication and performance infrastructure.

In an earlier work [4], we proposed a general secure sharing infrastructure of medical images between PACS and EHR systems. The proposed environment in that work was based on federated authentication and authorization techniques (OpenID and OAuth), and associated agents with dedicated tasks to provide both action-based and behavior-pattern based access control. The approach proposed in this paper focuses on integration with heterogeneous PACS and authentication of the PACS users by the OpenID provider. Furthermore, all accesses to patient images within each PACS are controlled by global consent directives and action-based access control polices.

3 Background

PACS Architecture

Figure 1 illustrates three main components (acquire, store, view) of a typical PACS network and sample DICOM messages (C-Store, C-Move, C-Find) [7]. Various modalities such as CT modality and X-ray modality, acquire patient's images and send them to the PACS server using DICOM command (C-Store). A central PACS server acts as database to store medical images from all modalities. Multiple clients (DICOM Viewers) can search, retrieve and display medical images through C-Find or C-Move request.

DICOM Standard

DICOM enables digital image acquisition devices, digital image archives, digital camera, printers, scanners and workstations, manufactured by different vendors, to send images to the PACS system. All real-world data such as patient information, studies, images, image acquisition devices, image viewer applications, are viewed by DICOM as objects

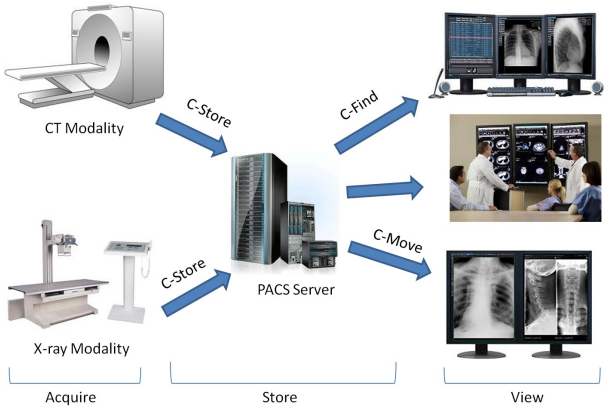

Figure 1. Major PACS components and sample DICOM messages

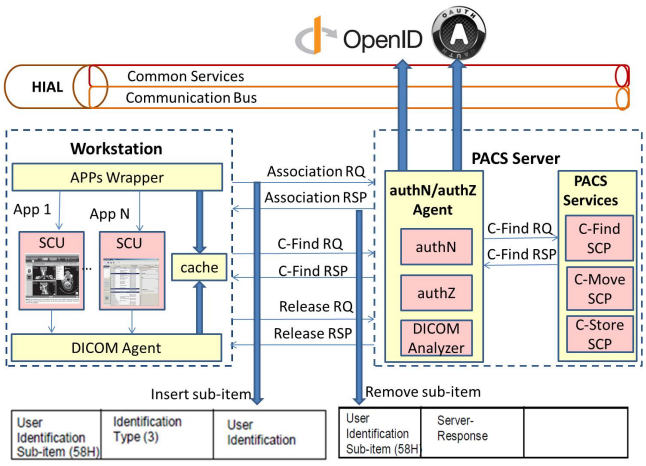

Figure 2. Agent-based architecture in legacy PACS systems

with respective properties or attributes [7]. DICOM maintains a list of all standard attributes (totally more than 2000 of them), known as the DICOM data dictionary [8], for the sake of ensuring consistency in attribute name and processing [7]. Therefore, as soon as the communication message is captured as data attribute, it can be transmitted and processed between various DICOM applications.

4 Approach

In the industry world of PACS, the state of the art of authentication and authorization provision can be viewed as: i) anyone who can enter the lab and logon to the workstation computer is allowed to do anything; ii) after the client application entity (IP, port, AE Title) is added to the PACS server's trusted list, any user logged on as a client application can access images stored at the server site. Application entry is the identity between parties. The PACS server understands which client application it is talking to, but has no knowledge about the exact user; and iii) IHE proposes that the client has to get a service ticket after being authenticated to access the service. However, kerberized DICOM has been proposed and is under development, but not finalized yet.

Due to the above security weaknesses of the existing PACS systems, we designed and implemented an agent-based solution to imply single sign-on user authentication from any PACS, and enhanced fine-grained access control on the user level rather than the application level.

4.1 Proposed Agent-based Architecture in Legacy PACS

In DICOM lingo, a basic DICOM operation has two actors: service class user (SCU) and service class provider (SCP) [7]. Figure 2 is an episode of SCU-SCP model, which presents the process of querying DICOM images. The process contains three stages: i) association establishment between SCU and SCP, in which SCU sends a C-Find request with search criteria; ii) SCP responds by sending images that match the query; and iii) association release when no further processing is required. Figure 2 also illustrates the agent-based architecture in one PACS system, and demonstrates how PACS authentication and authorization workflow are consolidated against HIAL (Health Information Access Layer). The major subsystems of this architecture are the *Workstation* and the *PACS Server*. The *workstation* consists of the following components:

- **APPs Wrapper**. It is the only portal of all integrated PACS client applications at one workstation or modality. Any existing application (App 1...App N) can be launched by APPs Wrapper and run independently. Before launching the target application, APPs Wrapper prompts to input user name and password. The user information is persisted in the local cache until the user logouts from the target application. The workflow of existing applications remain unchanged.

- **DICOM Agent**. It captures all outgoing DICOM messages. If the message is an association establishment request (Association-RQ), the DICOM Agent retrieves the corresponding user information from the cache and inserts the user identity sub-item into the Association-RQ message. User identity sub-item supports three methods [2]: user name in plain text (type 1); user name plus passcode (type 2); and Kerberos service ticket (type 3). In turn, if an incoming message is an association response (Association-RSP), the DICOM Agent has to remove the user identity sub-item from

DICOM message and log audit according to the reply result. In this way, both the client application (App 1...App N) and the PACS services benefit from extended user identity negotiation without any change in their workflows.

The *PACS Server* consists of the following components:

- **authN/authZ Agent**. This agent monitors all incoming DICOM messages. After receiving Association-RQ message, the DICOM Analyzer locates the user identity sub-item and extracts the user name and password (credentials). DICOM Analyzer also looks into the DICOM data dictionary to find attributes related to the user action such as user operation type, target image ID and patient ID. Then the *authN* component authenticates PACS user against OpenID protocol, using identified user name and password. The *authZ* component checks if access request is allowed by the OAuth authorization server using an extracted user action properties. Consent directive polices and action-based access control policies are integrated with OAuth. Our previous work explained in detail the flow of OpenID authentication and access control process using OAuth authorization protocol.

- **PACS Services**. If the access is granted, the request C-Find-RQ is sent to the real PACS service (C-Find SCP); the PACS searches in the local image database and returns back the matched images to the SCU. The workflow of SCP remains unchanged. C-Move and C-Store are other sample service providers to retrieve or store images.

4.2 Patient Electronic Consent Model

We summarised several existing paper-based consent disclosure forms used in Canadian hospitals [9, 10, 11, 12] and produced a UML class diagram to model such privacy-based access control polices. Figure 3 illustrates such a class diagram for patient consents expressed as access control polices in the form of XACML policy language model [13]. Due to the space limitation, we only discuss a subset of attributes for the classes. The class *Consent Policy* is associated with author who signed the consent; *Patient Record*; *Relationship To Patient* between author and patient; *Custodian* who is delegated for disclosing patient's health information; *Purpose of Disclosure*; the kind of *information* that can be disclosed; *effective duration* of this signed consent; particular *context* to allow or deny disclosure; method of disclosure of information; and specifying *list of granted or denied recipient* who can be individuals and/or organizations. As for selecting applicable policies to access request, in a simple case, such consent polices will be evaluated using patient ID that is defined as an attribute of target class.

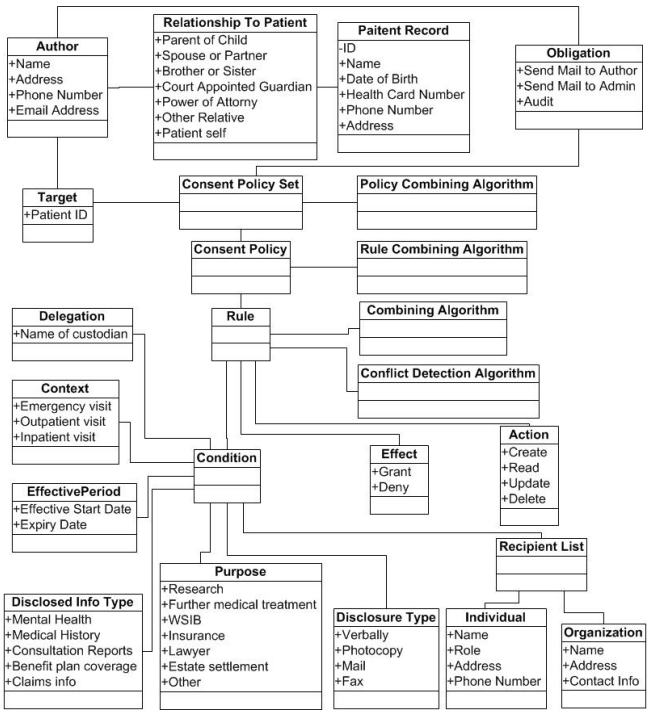

Figure 3. eConsent Class Diagram

4.3 Implementation

Figure 4 illustrates the physical architecture for integration of a vendor-independent PACS systems with a DI-r. It also presents how to authenticate and authorize PACS users against common services provided by HIAL regardless of accessing images stored inside the PACS or stored in DI-r. The major components are discussed below.

- **ClearCanvas PACS**. ClearCanvas [14] is an open source DICOM and PACS/RIS informatics and extensible platform, which includes viewing, archiving, management, workflow and distribution of images. A distributed ClearCanvas DICOM viewer and a DICOM server are deployed to simulate an existing PACS system in hospitals. Also DICOM agents are deployed on each workstation to capture outgoing and incoming DICOM messages. One agent is deployed in front of the DICOM Server assisting in integration with OpenID and OAuth. *RIS* and *HIS* in this physical architecture are place-holders for future research.

- **HIEOS XDS Repository and Registry**: Health Information Exchange Open Source (HIEOS) [15] is an implementation of, primarily server-side, IHE Cross Enterprise Document Sharing (XDS.b) document-registry and document-repository services. We employ HIEOS to simulate an abbreviated image-enabled

EHR system, which provides web service interfaces to retrieve and store images.

- **Client Registry RI**. Client Registry Reference Implementation [16] supports standard based interfaces including IHE Patient Identifier Cross-Reference HL7 v3 (PIXV3) [6] and Patient Demographic Query HL7 v3 (PDQV3) [6]. PIXV3 provides cross-referencing of patient identifiers from multiple domains. PDQV3 provides services to query patient information according to user defined search criteria. Both XDS Repository/Registry services and image source depends on this component for patient identifier mapping and information query.

- **FEM and Image Source (Dcm4chee)**. To enable ingestion of foreign exams, an integration component FEM (Foreign Exam Management) needs to take responsibility for localizing data on behalf of the PACS system, such as assisting in forwarding DICOM C-FIND or C-MOVE requests to DI-r, and morphing DICOM tags to ensure that images can be accepted by the local PACS system seamlessly. Dcm4chee [17] is a collection of open source applications and utilities for the healthcare enterprise, and the core is a robust implementation of the DICOM standard. In our project, dcm4chee acts as an integration component which receives images forwarded by FEM, and then trigger a workflow to send DICOM Manifest (KOS file) to XDS Repository and Registry.

- **Authentication and Authorization Services**. HIAL (Health Information Access Layer) provides common services which are responsible for: i) authentication of PACS users based on established identity of the PACS user; and ii) making access control decisions for the image accessing request using action tuples extracted by agents.

5 Case Study

The case study examines the workflow based on our proposed agent-based system architecture, and presents how our suggested patient consent model is applied on access control. Let us consider an example that requests to retrieve a patient's medical image stored in the local PACS. The followings are the stakeholders involved in this scenario: McMaster research lab and Juravinski hospital (two of the Hamilton Health Sciences organizations), both of them are on the HHS PACS network; Tom, an adult patient; Eric, Tom's primary physician who works at Juravinski hospital; and Mike, a researcher who works at McMaster research lab.

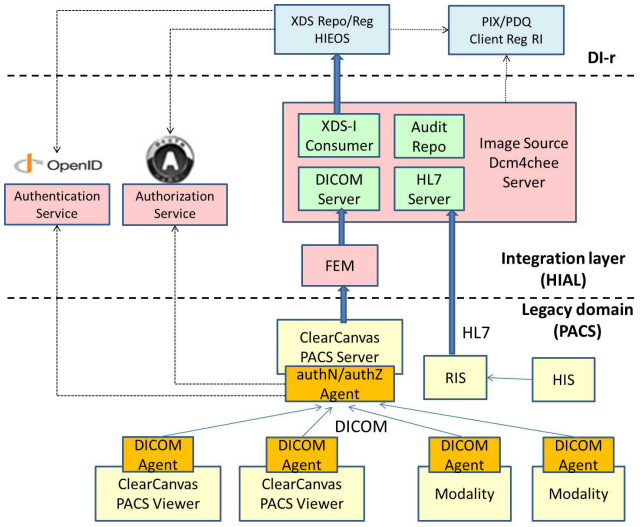

Figure 4. Integrated physical architecture based on open source tools

Table 1 specifies two classic access control policies in healthcare domain (a patient consent policy; and a user role-centric security policy). In a traditional environment, patients have to sign a paper-based consent disclosure form at each hospital as long as they have a medical record in that hospital. The consent disclosure form is designed and enforced locally, and by no means to communicate electronically between hospitals. The traditional environment is incapable of enforcing policy 2 since access control is based upon application identity rather than user identity. It means any physician or healthcare staff can view a patient's images as long as they are able to successfully logon.

With our proposed approach, consent directive policies (policy 1) are able to be defined once but applied to everywhere. Moreover, policy 2 is in a position to control access in user level. The process of enforcing policy 1 and policy 2 on image access request is as following. Now Mike, working in the research lab of McMaster, wants to view patient Tom's images from Jan 01, 2014 to Feb 01, 2014. The agent deployed at McMaster acquires the DICOM message, and then it calls authentication service during the stage of association negotiation; it also calls authorization service after extracting user action tuple. Table 2 explains data elements encapsulated in DICOM C-Find request in human readable text. After successfully authenticated the PACS user, authorization server will select applicable polices with request scope "patientID:12345, documentType:image, client:TOM". According to the attribute (patient ID) of target defined in policies, policy1 and policy2 are intended to serve this request. The request is granted and an accessing request is forwarded to the PACS

Table 1. Access control policies

1	Patient Tom authorizes Hamilton Health Sciences to disclose his diagnostic treatment and care information from Jan 01, 2010 to Dec 31, 2014 at the following sites McMaster, Chedoke and Juravinski.
2	Only primary physicians are allowed to view and change patient's images; other healthcare staffs working in Hamilton Health Sciences only have the privilege of viewing patient's images.

Table 2. Attributes extracted from DICOM message

Message Field	Tag(Grp, Elmt)	Value	Description
Group Length	(0000, 0000)	128	The even number of bytes
SOP Class UID	(0000, 0002)	1.2.840.10008.5.1.4.1.2.1.1	Contains the SOP UID for this C-FIND query root.
Command Field	(0000, 0100)	0020	DICOM C-Find-Rq command
Message ID	(0000, 0110)	9527	Unique numerical ID for this message
Priority	(0000, 0070)	0000	0000 (medium priority) 0001 (high) 0002 (low)
Data Set Type	(0000, 0800)	non-0101	0101 means data set is empty.
Query	(0008, 0052)	IMAGE	Defines level or hierarchy search:("PATIENT", "STUDY","SERIES", "IMAGE")
Query Parameter	(0010, 0020)	12345	Patient ID
Query Parameter	(0008, 0020)	20130101-20130201	Study Date: range matching between dates in YYMMDD format.

server. After a while, Mike wants to modify one of patient Tom's images, this access is denied since Mike is a non-primary physician of Tom and only has readable privilege for his images.

6 Conclusion

Current PACS systems have a closed architecture and suffer from security weaknesses due to an adopted trusted model and communication standards. Establishing user identity and capturing user action attributes are major challenges, when we construct a common infrastructure for secure sharing of medical images between the PACS and EHR systems. This paper contributes to the domain of legacy PACS systems by providing a solution to securely integrate heterogeneous PACS and EHR systems. The steps for such an integration are as follows: deploy cooperative agents in each legacy PACS system to capture DICOM messages, and establish user identity without changing the existing PACS workflow; enforce authentication of PACS users against OpenID provider; extract user action properties and enforce authorization on user against OAuth; and model consent directives using UML class diagram. Universal consent directive polices and action-based access control policies are applied on requests from each PACS system. In the continuation of this research, we will enhance our proposed architecture by incorporating the capabilities of cloud infrastructure to allow care providers to deliver better healthcare services.

References

[1] Barton F Branstetter. Practical Imaging Informatics: Foundations and Applications for PACS Professionals. In *Springer*, pages 33–47, 2009.

[2] DICOM Supplement99: Extended Negotiation of User Identity. http://medical.nema.org/ [2005].

[3] D. Mendelson, P. Bak, E. Menschik, and E. Siegel. Image Exchange: IHE and the Evolution of Image Sharing. pages 1817–1833, 2008.

[4] Kamran Sartipi, Krupa A. Kuriakose, and Weina Ma. An Infrastructure for Secure Shairng of Medical Images between PACS and EHR Systems. In *International Conference on Computer Science and Software Engineering (CASCON)*, pages 245–259, 2013.

[5] Integration the Healthcare Enterprise website. http://www.ihe.net/.

[6] IHE IT Infrastructure Technical Framework Integration Profiles Volume 1. http://www.ihe.net/ [Aug 2012].

[7] Oleg S. Pianykh. Digital Information and Communication in Medicine (DICOM): A practical Introduction and Survival Guide. In *Springer*, pages 7–16, 2011.

[8] DICOM standard part 6: Data Dictionary. http://medical.nema.org/ [2011].

[9] Hamilton Health Sciences Consent to Disclosure Personal Health Information. http://www.hhsc.ca/ [Mar 2013].

[10] Alberta Blue Cross Consent to Disclosure Personal Health Information. https://www.ab.bluecross.ca/ [Feb, 2013].

[11] Durham Mental Health Services Consent to Disclosure Personal Health Information. http://www.dmhs.ca/.

[12] HIPAA Authorization for Research. http://privacyruleandresearch.nih.gov/.

[13] eXtensible Access Control Markup Language (XACML) Version 3.0. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html [Jan 2013].

[14] Open Source ClearCanvas PACS Website. http://www.clearcanvas.ca/.

[15] Open Source HIEOS Home Page. http://sourceforge.net/projects/hieos/.

[16] Open Source Client Registry RI Website. http://te.marc-hi.ca/.

[17] Open Source Clinical Image and Object Management Dcm4che Home Page. http://www.dcm4che.org/.