



## iCARDEA

“An Intelligent Platform for Personalized Remote Monitoring of the Cardiac Patients with Electronic Implant Devices”

### SPECIFIC TARGETED RESEARCH PROJECT

**PRIORITY Objective ICT-2009.5.1: Personal Health Systems - a) Minimally invasive systems and ICT-enabled artificial organs: a1) Cardiovascular diseases**

## iCARDEA Deliverable D6.5.1 Security and Privacy of the Interoperability Layer

<i>Due Date:</i>	September 30, 2011
<i>Actual Submission Date:</i>	November 01, 2011
<i>Project Dates:</i>	Project Start Date : February 01, 2010 Project End Date : January 31, 2013 Project Duration : 36 months
<i>Leading Organization:</i>	<i>Contractor</i> FORTH

## Document History:

Version	Date	Changes	From	Review
V01	October 27, 2011	Initial draft	FORTH	All partners
V0.2	October 28, 2011	SRDC Comments, updates	SRDC	FORTH
V0.3	November 1, 2011	FORTH updates on ATNA	FORTH	All partners

Contributors
--------------

FORTH: Stelios Sfakianakis, Yiannis Petrakis, Catherine Chronaki
--

SRDC: Gokce B. Laleci Erturkmen, Elif Eryilmaz, Yildirak Kabak, Prof. Dr. Asuman Dogac
--

Project co-funded by the European Commission within the Seventh Framework Programme (2007-		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission	
RE	Restricted to a group specified by the consortium (including the Commission	
CO	Confidential, only for members of the consortium (including the Commission Services)	

## iCARDEA Consortium Contacts:

SRDC	Asuman Dogac	+90-312-2101393	+90(312)2101837	asuman@srdc.com.tr
OFFIS	Wilfried Thoben	+49-441-9722131	+49-441-9722111	thoben@offis.de
SRFG	Manuela Plößnig	+43-662-2288-402	-	manuela.ploessnig@salzburgresearch.at
FORTH	Catherine Chronaki	+302810391691	+302810391428	chronaki@ics.forth.gr
SALK	Bernhard Strohmer	+43-6624482-3481	+43-6624482-3486	b.strohmer@salk.at
SJM	Karl Eberhardt	+43-16073067	-	keberhardt@sjm.com
Medtronic	Alejandra Guillén	34916250361	+34913346453	alejandra.guillen@medtronic.com
HCPB	Josep Brugada	+34932275703	+34932275459	jbrugada@clinic.ub.es

## Table of Contents

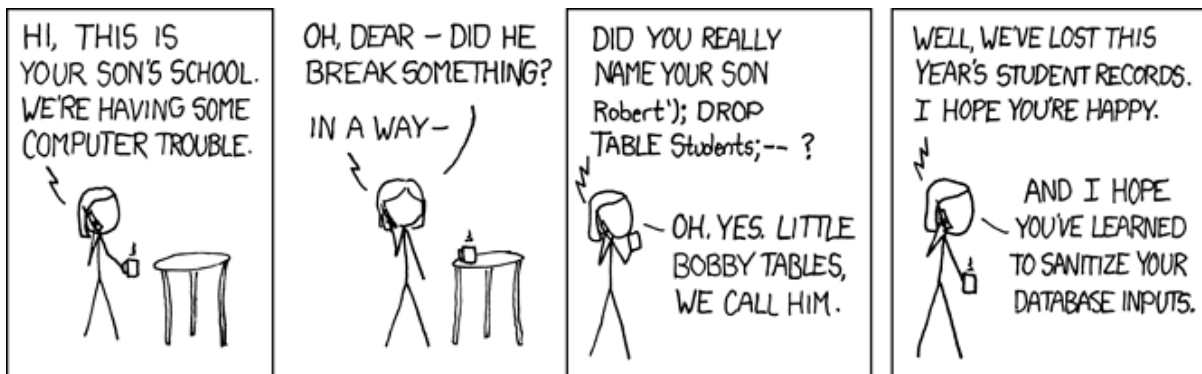
1	PURPOSE .....	6
1.1	Definitions and Acronyms .....	6
2	Introduction.....	7
3	Standards .....	9
3.1	TLS and Digital Certificates .....	9
3.2	ATNA integration profile.....	9
3.3	SAML.....	10
3.4	OpenID .....	10
4	The iCARDEA Security Infrastructure.....	11
4.1	An Analysis of iCARDEA Security Infrastructure .....	13
4.2	The iCARDEA Certification Authority .....	15
4.3	The iCARDEA Audit Repository .....	16
4.4	The iCARDEA Id Provider .....	19
5	References .....	22

## Table of Figures

Figure 1 ICARDEA Deployment architecture.....	8
Figure 2: iCARDEA Interoperability Infrastructure – IHE Integration Profiles /Transactions .....	11
Figure 3 Interfaces provided by the EHR Interoperability Framework.....	12
Figure 4 iCARDEA Security Infrastructure .....	13
Figure 5 A template audit record message for ITI-41.....	18
Figure 6 The initial "welcome" page of the Id Provider .....	19
Figure 7 "Signing up" to the Id Provider .....	19
Figure 8 The user is asked to give the same username and password that he/she uses for logging into the SALK MS Windows machines .....	20
Figure 9 The login page of the Id Provider .....	20
Figure 10 The initial page of the Id Provider after the user has successfully logged in. ....	21

# 1 PURPOSE

This document aims to provide details on the design principles and the implementation of the security infrastructure at the core interoperability layer of the iCARDEA layer. Its main focus therefore is on the interactions and the communications taken place among the iCARDEA components but also in relation to the end user sessions. The document does not consider the components' internal security mechanisms to protect patient clinical data, such as the way data are stored in databases, the user accounts, and the needed safeguards to defend against unauthorized access: these issues need to be dealt separately by each component on a case by case basis. In particular we will not deal with security issues such as the ones described in the following comic strip:



## 1.1 DEFINITIONS AND ACRONYMS

Table 1 List of Abbreviations and Acronyms

Abbreviation/ Acronym	DEFINITION
ATNA	Audit Trail and Node Authentication
AX	OpenId Attribute Exchange extension
CA	Certification Authority
DNS	Domain Name Service
CDA	Clinical Document Architecture
CIED	Cardiovascular Implantable Electronic Device
CM	Care Management
EHR	Electronic Health Record
HIS	Hospital Information System
HL7	Health Level 7
IdP	OpenId Identity Provider
IP	Internet Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
ISO	International Standards Organization
OASIS	Organization for the Advancement of Structured Information Standards
PCC	IHE Patient Care Coordination technical framework
PCD	IHE Patient Care Device technical framework

PHI	Protected Health Information (USA)
PHR	Personal Health Record
PIX	Patient Identifier Cross-Referencing
RP	OpenId Relying Party
SAML	Security Assertion Markup Language
SReg	OpenId Simple Registration extension
TLS	Transport Layer Security
XDS	Cross-Enterprise Document Sharing profile

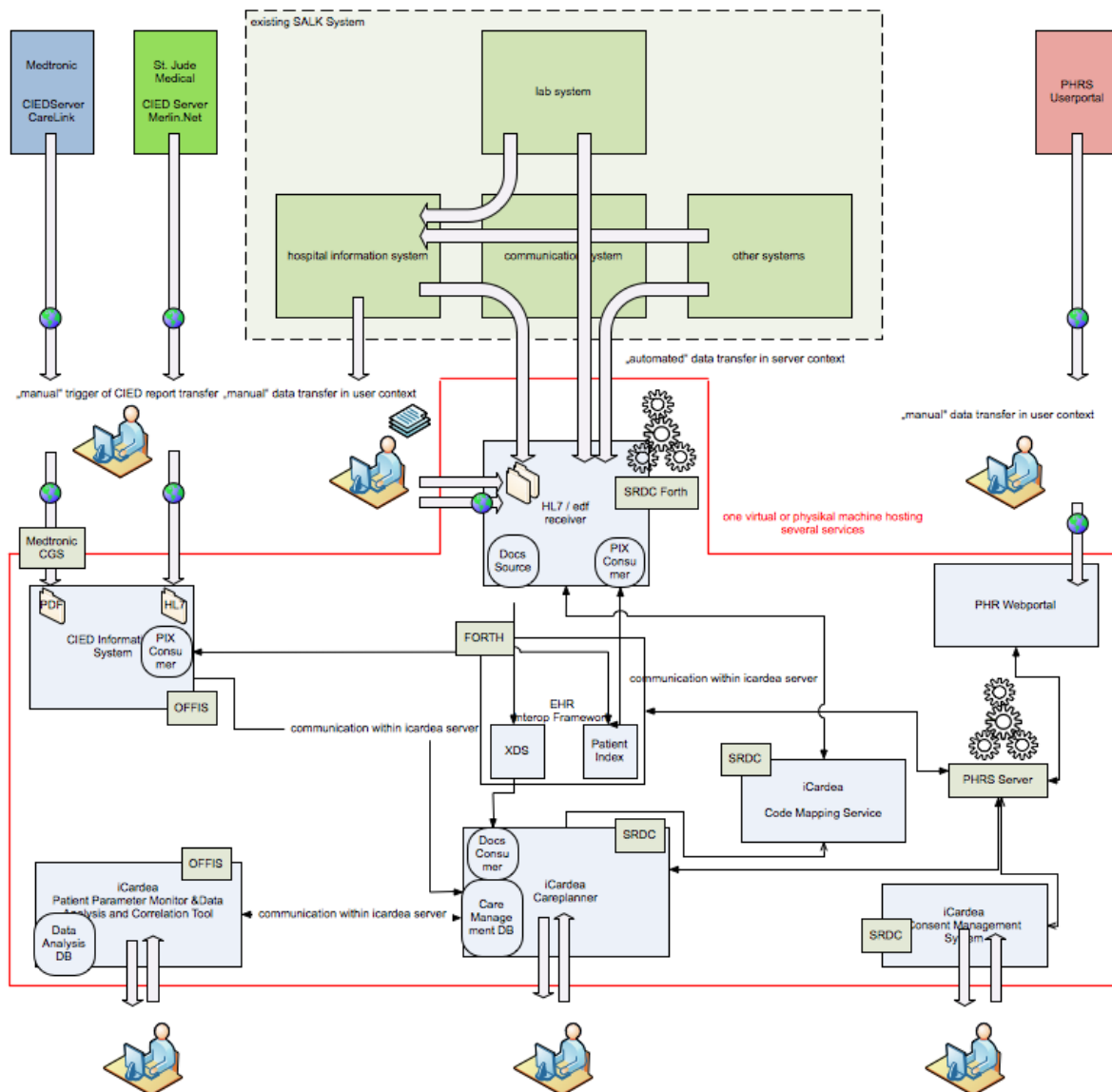
## 2 Introduction

Security is a property of a system that spans it both vertically and horizontally. It cannot be defined concretely in a single definition but rather as an aggregation of characteristics and principles that should be sufficiently supported by any IT system. In a setting such as the iCARDEA platform, the following security related concepts are extremely related:

- **Authentication:** The identity of a user, process, or device should be verified, so that any access to the data goes along with the information of the principal who triggered it.
- **Authorisation:** The security infrastructure must ensure that the resources are accessible only to those people who are authorised to do so.
- **Confidentiality:** It must be assured that any data produced or handled within the iCARDEA environment is not exposed to unauthorised persons. This can be accomplished through authorisation mechanisms, encryption technology and privacy enhancing techniques.
- **Integrity:** The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. In the iCARDEA system the sensitive patient data should be transmitted in a way such that any modification to them after their dispatch should not go undetected by the receiving party.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action.
- **Privacy:** Since much work to be carried out within the iCARDEA environment deals with clinical data concerning patients' private information, it should be assured that privacy is well protected. One of the basic principles of privacy protection is disclosure of information on a need to know bases. For example: In many cases researchers are able to complete their work without knowing the identity of the patients concerned in their study. This can be accomplished through de-identification and pseudonymisation.

In this document we will particularly focus on the way these security characteristics are supported by the iCARDEA interoperability layer. As can be seen in Figure 1, which depicts the deployment architecture in the SALK pilot site, the main components of the interoperability framework are the ones taking care of the management of patient identifiers and the storage, retrieval, and updating of patients' clinical data from EHR, PHR and CIED. The whole system is built upon the IHE integration profiles so that international standards such as the ones from HL7 are used to implement the specific clinical information needs.

- IHE Care Management (CM) profile is implemented by the EHR Interoperability Framework, the PHR Interoperability System and the iCARDEA Care Planner
- IHE Implantable Device - Cardiac – Observation (IDCO) profile is implemented by the CIED Information System and the iCARDEA Care Planner
- IHE Patient Identifier Cross-Referencing (PIX) profile is implemented by the EHR Interoperability Framework, the PHR Interoperability System, the iCARDEA Care Planner, and the CIED Information System
- IHE Cross-Enterprise Document Sharing profile (XDS) profile is implemented by the EHR Interoperability Framework



**Figure 1 iCARDEA Deployment architecture**

The communication protocols used comply with the IHE specified “transactions” that are pertinent to the use case at hand (PCC-09 and PCC-10 for IHE CM profile, and PCD-09 for IHE-IDCO profile, ITI-21 and ITI-9 for the IHE-PIX profile and ITI-41, ITI-18, and ITI-43 for the IHE-XDS Profile).

The IHE transactions also specify some of the security mechanisms that should be in place. Most of these mechanisms relate to the Confidentiality, Integrity, and Accountability

properties described above. For each such requirement the IHE integration profiles reference a set of standards that are appropriate on the specific case. We will briefly survey these common standards in the following section.

## 3 Standards

### 3.1 TLS AND DIGITAL CERTIFICATES

Transport Layer Security (TLS) [1] and its predecessor, Secure Sockets Layer (SSL) [2], are cryptographic protocols that provide communication security over the Internet. TLS provides for both data integrity and confidentiality (via encryption) and it's based on the use of X.509 [3] *digital certificates* and the *public-key cryptography*.

TLS/SSL is very common in the "public" internet in the form of HTTPS, the "secure" version of the HTTP protocol that is used extensively in order to guarantee confidentiality in online bank transactions or other business scenarios. Using TLS the user is sure that there is a secure communication channel between her browser and the server machine so that all the information transmitted cannot be modified or eavesdropped by any system or device in the middle of the established communication path. There's an additional safeguard so that the user knows that she's really contacting the server she supposes to, based on the DNS name of the server and the name that is referenced on its digital certificate. Furthermore, client authentication is also possible, so that the server is sure that the requesting user is a legitimate one, when *mutual authentication* is configured in the server.

As noted above TLS is based on the notion of digital certificates. A certificate is a digital form of identification that is usually issued by a *certification authority* (CA) and contains identification information, a validity period, a public key, a serial number, and the digital signature of the issuer. For authentication purposes, a TLS client or server uses an X.509 certificate to provide another party with strong evidence that attests the identity of the party that holds the certificate and the corresponding private key.

The trust between the client and the server is established when the certificates are signed by a Certification Authority (CA) accepted by both parties. A CA is a mutually trusted third party that confirms the identity of a certificate requestor (usually a user or computer), and then issues the requestor a certificate. The certificate binds the requestor's identity to a public key. CAs also renew and revoke certificates as necessary. For example, if a client is presented with a server's certificate, the client computer might try to match the server's CA against the client's list of trusted CAs. If the issuing CA is trusted, the client will verify that the certificate is authentic and has not been tampered with. Finally, the client will accept the certificate as proof of identity of the server.

### 3.2 ATNA INTEGRATION PROFILE

The *Audit Trail and Node Authentication (ATNA)* Integration Profile establishes security measures which, together with the Security Policy and Procedures, provide patient information confidentiality, data integrity and user accountability.

ATNA Integration Profile contributes to access control by limiting network access between nodes and limiting access to each node to authorized users. Network communications between secure nodes in a secure domain are restricted to only other secure nodes in that domain. Secure nodes limit access to authorized users as specified by the local authentication and access control policy.

- *User Authentication*: The Audit Trail and Node Authentication Integration Profile requires only local user authentication. The profile allows each secure node to use the access control technology of its choice to authenticate users. The use of

Enterprise User Authentication is one such choice, but it is not necessary to use this profile.

- *Connection Authentication*: The Audit Trail and Node Authentication Integration Profile requires the use of bi-directional certificate-based node authentication for connections to and from each node. The DICOM, HL7, and HTTP protocols all have certificate-based authentication mechanisms defined. These authenticate the nodes, rather than the user. Connections to these machines that are not bi-directionally node-authenticated shall either be prohibited, or be designed and verified to prevent access to Protected Health Information (PHI).
- *Audit Trails*: User Accountability is provided through Audit Trail. The Audit Trail needs to allow a security officer in an institution to audit activities, to assess compliance with a secure domain's policies, to detect instances of non-compliant behaviour, and to facilitate detection of improper creation, access, modification and deletion of PHI.

On the technical front, ATNA requires the use of TLS to cater for the transport layer integrity, confidentiality, and (service) authentication for both the server and the client. The accountability requirement is supported by the introduction of an *Audit Record Repository* that is a central repository for log messages. For this repository the ATNA profile proposes the use of TLS transported SYSLOG messages (RFC 5425)[4].

### 3.3 SAML

*Security Assertion Markup Language (SAML)* [5,6] is an XML-based open standard for exchanging authentication and authorization data between security domains that is, between an *identity provider* (a producer of assertions) and a *service provider* (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

The single most important problem that SAML is trying to solve is the *Web Browser Single Sign-On (SSO)* problem, a problem also addressed by the OpenID protocol [7]. Single sign-on solutions are abundant at the intranet level (using cookies, for example) but extending these solutions beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies.

SAML assumes the *principal* (often a user) has enrolled with at least one identity provider. This identity provider is expected to provide local authentication services to the principal. However, SAML does not specify the implementation of these local services; indeed, SAML does not care how local authentication services are implemented (although individual service providers most certainly will).

Thus, a service provider relies on an identity provider to identify a principal. At the principal's request, the identity provider passes a SAML assertion to the service provider. On the basis of this assertion, the service provider makes an access control decision.

### 3.4 OPENID

OpenID is an open standard that describes how users can be authenticated in a decentralized manner, eliminating the need for services to provide their own ad hoc systems and allowing users to consolidate their digital identities.[6]

The OpenID protocol does not rely on a central authority to authenticate a user's identity. Moreover, neither services nor the OpenID standard may mandate a specific means by which to authenticate users, allowing for approaches ranging from the common (such as passwords) to the novel (such as smart cards or biometrics).

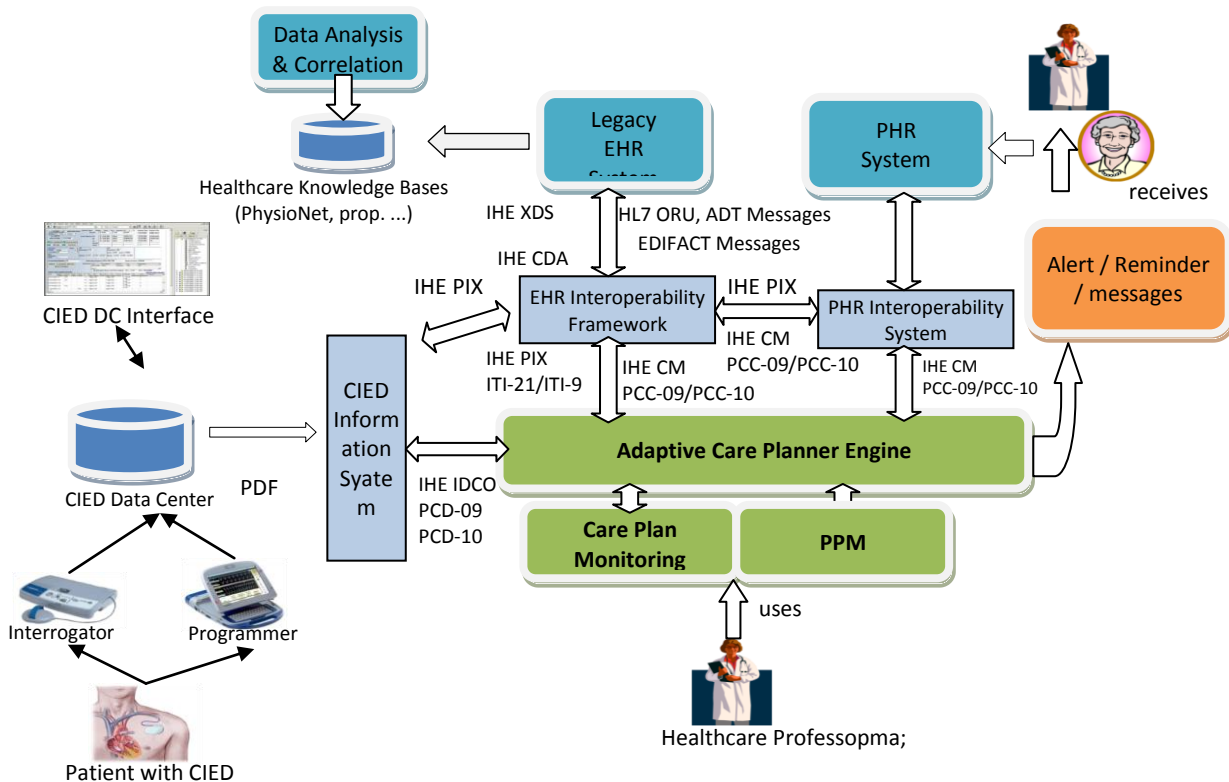
The term OpenID may also refer to an identifier as specified in the OpenID standard; these identifiers take the form of a unique URI, and are managed by some "OpenID provider" that handles authentication.

In essence OpenID is a web based solution to the Single Sign-On problem, that is for the user to reuse his identity and credentials when signing up into multiple web sites. It defines

two main actors: the Relying Party (or “Consumer”), which is the web site the user tries to log-in, and the Identity Provider (IdP), which is the site providing OpenID authentication to their users. The idea is that the users need to register once in one Id Provider and then use the OpenID they acquire from there to create accounts in multiple OpenID compliant web sites. So Identity Providers offer identity verification and Id information while Relying parties display log-on form (“Login with your OpenID”).

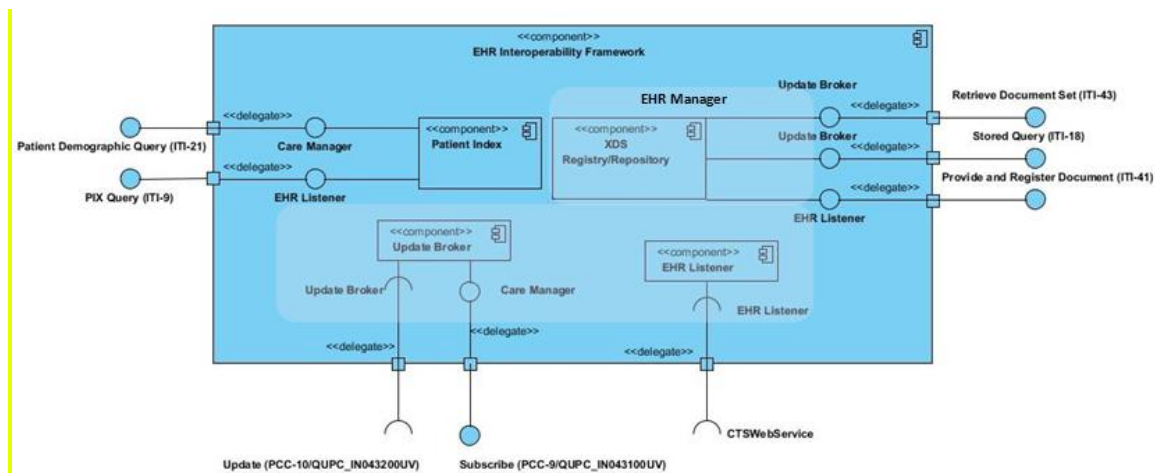
In addition to the Single Sign-on functionality, OpenID through the use of extensions, supports the dissemination of user information, such as the name, gender, date of birth, etc. The simplest such extension is Simple Registration [8], while a more modern and extensible way is the one specified by the Attribute Exchange [9].

### 4 The iCARDEA Security Infrastructure



**Figure 2: iCARDEA Interoperability Infrastructure – IHE Integration Profiles /Transactions**

The main iCARDEA components comprising the interoperability framework are shown in Figure 3 along with their IHE compliant interfaces. In Figure 3, the detailed IHE based interfaces provided by EHR Interoperability Framework is presented in a separate figure.



**Figure 3 Interfaces provided by the EHR Interoperability Framework**

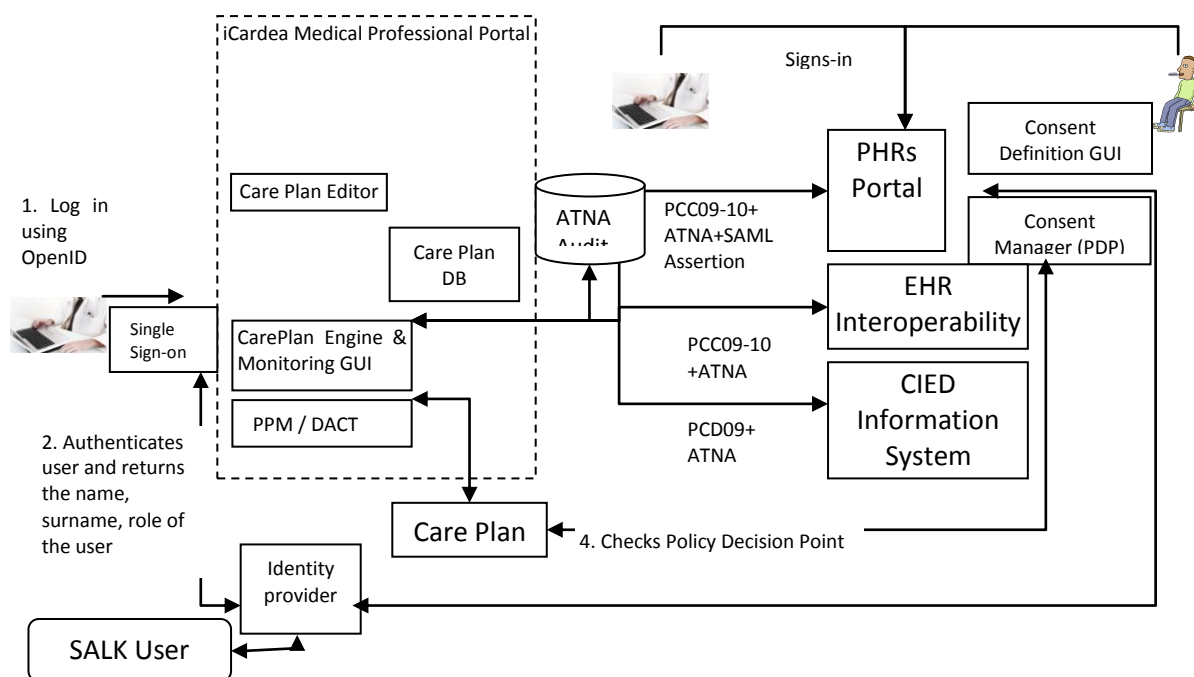
As presented in section 3, the IHE-ATNA profile ensures connection authentication, transport later integrity and confidentiality. All of the IHE based transactions used in the iCARDEA architecture (ITI-21, ITI-9, PCC-09, PCC-10, PCD-09, ITI-41, ITI-18, ITI-43) are secured through the implementation of the ATNA profile: Each component will encrypt the messages exchanged through TLS and digital certificates. Implementation also ensures accountability, as ATNA Audit Trails are also be maintained. User authentication and single sign-on mechanisms are facilitated through the Identity Provider implemented based on the OpenID protocol. Finally, privacy is ensured through iCARDEA Consent Manager, which is discussed in detail in iCardea Deliverable 5.4.1.

In the following sections, we will first of all present an analysis of security requirements between several different iCARDEA components through use cases. This analysis helped us to identify the core components of iCARDEA Security Infrastructure, namely:

- iCARDEA Certification authority
- iCARDEA Audit repository
- iCARDEA ID provider

In the following sections we elaborate the implementation of these components and mechanisms to secure the communication with this infrastructure.

## 4.1 AN ANALYSIS OF ICARDEA SECURITY INFRASTRUCTURE



**Figure 4 iCARDEA Security Infrastructure**

In Figure 4, the basics of iCARDEA Security architecture are presented. The interactions required ensuring security and privacy of the data exchanged between iCARDEA components are depicted in this figure, and elaborated through the use case definitions presented below.

### UC-1: Medical Professional Log-in for using iCARDEA Components

1. When a Medical Professional wants to access any iCARDEA web interface (Physician Portal, PHRs Portal, PIX Manager), s/he either directly enters his/her OpenID to the GUI or click "Authenticate through SALK Identity Provider" button. In the former case, the users should be provided with an OpenID beforehand.
2. After that the control is passed to Identity Provider which will perform the actual authentication. Any authentication mechanism can be used at this point. Simple username/password authentication is sufficient. If successful, the Identity Provider returns OpenID, name, surname, email, role, etc. of the user.
3. After that the user can use the component.

### UC-2: Care Plan Engine Subscribes to retrieve Patient Data from PHRs Portal and EHR Interoperability Framework

1. Prerequisite: Certificates for Care Plan Engine, PHRs Portal and EHR Interoperability Framework are created and shared beforehand.
2. Care Plan Engine sends subscription requests as PCC-09 messages to PHRs Portal and EHR Interoperability Framework. These messages are secured in conformance to ATNA Profile, using the agreed certificates.
3. In the PCC-09 subscription request, the identity and role of the Medical Professional currently logged in to the system is also sent through a SAML Assertion.

**UC-3: PHRs Portal and EHR Interoperability Framework sends Patient Data to Care Plan Engine**

1. Prerequisite: Certificates for Care Plan Engine, PHRs Portal and EHR Interoperability Framework are created and shared beforehand.
2. PHRs Portal /EHR Interoperability Framework sends PCC-10 messages to Care Plan Engine. These messages are secured in conformance to ATNA Profile, using the agreed certificates.
3. These are logged to ATNA Audit Repository.

**UC-4: CIED Information System sends CIED Data to Care Plan Engine**

1. Prerequisite: Certificates for Care Plan Engine, CIED Information System are created and shared beforehand.
2. CIED Information System sends PCD-09 messages to Care Plan Engine. These messages are secured in conformance to ATNA Profile, using the agreed certificates.
3. These are logged to ATNA Audit Repository.

**UC-5: Patient is registered to iCARDEA System by SALK Personnel**

1. SALK Personnel need to log in the PIX Manager Web Interface following the procedure described in UC-1 above.
2. Patient's HIS ID, Demographic data, CIED ID and Protocol ID is entered through PIX Manager Web Interface by SALK Personnel.
3. These are stored in the PIX Manager to answer PIX Queries to be received in the future.
4. Patient is given the Protocol ID, s/he will use this ID while signing up to the PHRs Portal.
5. All the above actions are logged to the ATNA Audit Repository.

**UC-6: Patient signs up to PHRs Portal**

1. Patient is requested to present an Open ID account. If s/he does not have an OpenID, the System directs him/her to a default OpenID provider.
2. Patient will also be asked to provide the Protocol ID provided to him.
3. PHRs Portal will create a unique PHRs ID for the patient, and will register the OpenID, PHRs ID, and the Protocol ID in its databases. It will also serve a service to return the PHRs ID, and/or the Protocol ID given the OpenID (which will be used by to Consent Management System).
4. PHRS Portal will send a HL7 ADT:A40 message to the PIX Manager to merge the PHRs ID with the Protocol ID

**UC-7: Patient signs in to PHRs Portal**

1. Patient signs in to the PHR Portal using his/her OpenID
2. The PHRs Portal will check whether this OpenID is registered as a Patient in the system
3. If the OpenID is available in PHRs System as a registered patient, s/he will be directed to the OpenID Provider so that s/he can confirm his OpenID login password, if successful, s/he will be redirected back to the PHRs Portal
4. If s/he is not available in PHRs System as a registered patient, s/he will be reminded about the Sign up procedure and will be directed to PHRs Portal Signup page.

**UC-8: An authorized Medical Professional wants to access Patient Data through PPM**

1. An authorized Medical Professional logs in to the iCardea Medical Professional Portal through its OpenID and click PPM's link.
2. The role information will be retrieved from the ID Provider.

3. When the user selects a patient (through a Protocol ID), and the EHR/PHR Sections s/he wants to view, the PPM will direct the query to the CarePlan DB, where the role of the user, the Protocol ID of the patient and the EHR/PHR Sections s/he want to access are specified.
4. The Care Plan DB will consult to Consent Manager (who acts as the Policy Decision Point), to be able to selectively return the requested information based on patient's consent.
5. PPM will log the accesses as an audit record to the ATNA Audit Repository.

**UC-9: An authorized Medical Professional wants to see potential patterns through DACT**

1. An authorized Medical Professional logs in to the iCardea Medical Professional Portal through its OpenID and click PPM's link.
2. Through the link provided Medical Professional is directed to DACT, which uses similar mechanisms with PPM to access the Care Plan DB.

**UC-10: An authorized Medical Professional wants to see Patient PHR data from PHRS Medical Professional Interface**

1. When a Medical Professional wants to access the PHRs Portal, s/he either directly enters his/her OpenID to the GUI or click "Authenticate through SALK Identity Provider" button. In the former case, the users should be provided with an OpenID beforehand.
2. After that the control is passed to Identity Provider which will perform the actual authentication. Any authentication mechanism can be used at this point. Simple username/password authentication is sufficient. If successful, the Identity Provider returns OpenID, name, surname, email, role, etc. of the user.
3. Following successful authentication, the user can use the component.
4. The user selects a patient and wants to view parts of his/her PHR Records, the PHRs Portal will query to the Consent Manager, where the role of the user, the ProtocolID of the patient and the PHR Sections s/he want to access are specified.
5. The Consent Manager (who acts as the Policy Decision Point), either grants or denies these access requests.
6. Based on the decision of Consent Manager, the PHRs Portal will be to be able to selectively present the requested information based on patient's consent.
7. The PHRs Portal will log the accesses as an audit record to the ATNA Audit Repository.

**UC-11: Import into EHR clinical data exported from the hospital information system**

1. Prerequisite: Certificates for EHR Interoperability Framework are created and shared beforehand.
2. HIS sends HL7 messages or EDF documents into EHR Interoperability Framework. EHR Listener receives these messages/documents, converts the clinical data into CDA formatted documents and stores them into XDS Repository. This is done by invoking the Provide and Register Document Set.b service of the XDS. These Provide and Register Document Set.b messages are secured in conformance to ATNA Profile, using the agreed certificates.
3. All the above actions are logged in the ATNA Audit Repository.

## **4.2 THE ICARDEA CERTIFICATION AUTHORITY**

The ATNA profile requires the use of TLS certificates and the related SSL/TLS encryption everywhere, in every cross-component IHE transaction. Normally in the "public" Web these

certificates need to be signed by some some “well-known” and trusted Certification Authorities (CA) like Verisign or Thawte. Unfortunately “official” signing costs a lot of money and it would be impractical for a research project such as the iCARDEA.

Another approach is to create “self-signed” certificates for each component, both the services and the end user ones. Unfortunately this also creates other problems such as the distribution of these certificates and the need for the users to deal with a lot of warnings about these certificates from their browsers and from the other hand the developers to lower the security level by not verifying peers in the SSL/TLS connections of their components.

A better approach though is to setup an iCARDEA specific CA for the needs of its platform. A drawback of using self-signed certificates is that browsers will still complain about the specific sites not being trusted. But this can change if the root certificate of CA is imported to the browsers so that all SSL/TLS protected web sites that have their certificates signed by the iCARDEA CA are subsequently considered trusted without further user intervention. At the pilot installation in SALK this root certificate of the iCARDEA CA can be installed by accessing <http://icardea-server.lksdom21.lks.local/CA/cacert.crt>. The certificate of this CA is shown next in the PEM (“Privacy Enhanced Mail”) format:

```
-----BEGIN CERTIFICATE-----
MIIEZTCCA02gAwIBAgIJAKfjzAzbybQyMA0GCSqGSIb3DQEEBQUAMH4xCzAJBgNV
BAYTAKdSMRIwEAYDVQQKEw1JQ1MtRk9SVEgxEDA0BgNVBAsTB21lDQVJERUExJjAk
BgNVBAMUHW1DQVJERUFFQ0EgQ2VydG1maWNhdGUgTWVzdGVyMSEwHwYJKoZIhvcN
AQkBFhJzc2Zha0BpY3MuZm9ydGguZ3IwHhcNMTEwMDIwMTEzMjUwWhcNMjExMDE3
MTEzMjUwWjB+MQswCQYDVQGEwJHUjESMBAGA1UEChMJSUJUNTLUZPULRIMRAwDgYD
VQQLewdpQ0FSREVBMSYwJAYDVQQDFB1pQ0FSREVBX0NBIENlcnRpZmljYXR1IE1h
c3RlcjEhMB8GCSqGSIb3DQEJARYSc3NmYWtAaWNzLmZvcnRoLmdyMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApyU0GW7Gulsc8izKog4bIOcBn7d8GS6E
3lRjPMPxkPeLCWmmjeVbV46CAiWDpUSdzcz+LP910fECBZOXQIJptqWBU8XKniEm
pfk+1RPtZtZ7p4V8Hzo/jHY7oy+xywyrn2nk1gxmpLd/00gh3kCuc2p9Bc0xFjg1
OPDJLrksV3T0kZf42gjjgBMB43xLlFEfFvcTrUiiecmTy+cXX+AS+IaU1HBS1xyey
RESnfuOf/bILX9e55R6FVLeeZ4YEWLKooOKydt5teOjNtn11/Jv1PYaBrFotM/Qj
OaBstuknb0ZyIKs+bWt6sE5FwTkooyX8+g7Y0eb+M160NVvGxOXbLwIDAQAB04H1
MIHiMB0GA1UdDgQWBQmjjg3sIiK2VbGy4aNdF22+OYaFTCBsgYDVR0jBIGqMIGn
gBQmjjg3sIiK2VbGy4aNdF22+OYaFaGBg6SBgDB+MQswCQYDVQGEwJHUjESMBAG
A1UEChMJSUJUNTLUZPULRIMRAwDgYDVQQLewdpQ0FSREVBMSYwJAYDVQQDFB1pQ0FS
REVBX0NBIENlcnRpZmljYXR1IE1hc3RlcjEhMB8GCSqGSIb3DQEJARYSc3NmYWtA
aWNzLmZvcnRoLmdyggkAp+OsDNvJtDIwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQUFAAOCAQEAePRn6nrtSL6oTSuRD8zj94KA2w135ttlHfOdj7fThnQRglQKQLWX
4t7bLRCRAKIoapoGo7RH0X7D383wNIqUtN809RhG3JquyNscgMDIqbb/VrendOdj
Wne4fxQFbn2dTTT7dq+eNKvtZYNbcNKeybWMqnpnk3z7svfzQSYpniOf6jBfm6CK
bQ2baxMFxIgeOj7x9uCI1b8hwqD7eYqGyCBAC9x2xXKOQp3AOFrvjzPFq4girXOa
5qbQHwmnwnhRKYtQEWUvmr1AFXetXpgK/4lmsXK2s0Cvzm8sK4VCQSLssNVRrzir
GrBZB9/nW8I1SBqsjzHb91p8chp9b5f5pA==
-----END CERTIFICATE-----
```

This iCARDEA CA is set to be trusted by all components of the iCARDEA platform and all these components and services will have their certificates signed by this CA.

### 4.3 THE ICARDEA AUDIT REPOSITORY

ATNA is an IHE security profile representing Audit Trail and Node Authentication, which was described in Section 3.2. OpenATNA<sup>1</sup> is an Open Source implementation of an Audit Record Repository supporting RFC 3881 audit messages [10] over BSD Syslog as well as RFC 5424-5426 (UDP and TLS).

<sup>1</sup> <https://www.projects.openhealthtools.org/sf/projects/openatna/>

In the iCARDEA system we use an OpenATNA installation as the central Audit Record Repository. The following are the EHR components and the relevant IHE transactions that require the submission of audit record events to the Audit Repository:

- *EHR Interoperability Framework (Patient Index)*: PIX Query (ITI-9) and Patient Demographics Query (ITI-21)
- *EHR Interoperability Framework (XDS)*: Retrieve Document Set (ITI-43), Stored Query (ITI-18), Provide and Register Document (ITI-41)
- *EHR Interoperability Framework (Update Broker)*: PCC-9 (QUPC\_IN043100UV) and PCC-10 (QUPC\_IN043200UV)
- *PHR Interoperability Framework (Update Broker)*: PCC-9 (QUPC\_IN043100UV) and PCC-10 (QUPC\_IN043200UV)
- *PHR Interoperability Framework*: PIX Query (ITI-9) and Patient Demographics Query (ITI-21)
- *Care Planner*: PIX Query (ITI-9) and Patient Demographics Query (ITI-21)
- *CIED Information System*: PIX Query (ITI-9) and Patient Demographics Query (ITI-21)
- *Care Planner*: PCC-9 (QUPC\_IN043100UV) and PCC-10(QUPC\_IN043200UV)
- *CIED Information System*: Send Observation (PCD-9)
- *Care Planner*: Send Observation (PCD-9)

The ATNA profile defines the “Record Audit Event” (ITI-20) transaction for sending audit trail information to the Audit Repository. The HL7 Security and Accountability SIG and DICOM WG 14 have jointly defined in the DICOM supplement 95<sup>2</sup> the base format of the payload for the SYSLOG message, as an extension/derivation of the XML schema defined in RFC 3881. A template XDS Provide and Register Document (ITI-41) audit record event message conforming to this XML format is shown in Figure 5 below.

In this audit message the following information is transmitted:

- The identification of the transaction (“ITI-41”) and the current timestamp. The *EventActionCode* is “C” which means that the transaction triggered the *creation* of a data resource in the receiving application.
- The identification for the client (where *RoleId* is “Source”), which includes its IP address and its SOAP Messaging information. Also in the *UserId* element the unique identifier for the user actively participating in the event can be filled in, if the client has provided this information.
- The identification of the server (where *RoleId* is “Destination”), i.e. the XDS Registry/Repository, which includes its IP address and its SOAP Messaging information.
- Information about the operation itself. In the case of ITI-41, this includes the Patient Identifier and the unique id of the XDS Submission Set. Using this information another application can retrieve all the submitted documents from the XDS Repository.

---

<sup>2</sup> [ftp://medical.nema.org/medical/dicom/final/sup95\\_ft.pdf](ftp://medical.nema.org/medical/dicom/final/sup95_ft.pdf)

```

<AuditMessage>
  <EventIdentification EventOutcomeIndicator="0"
    EventDateTime="{CURRENT_TIMESTAMP}" EventActionCode="C">
    <EventID codeSystemName="DCM" displayName="Import"
      code="110107"/>
    <EventTypeCode codeSystemName="IHE Transactions"
      displayName="Provide & Register Document Set-b"
      code="ITI-41"/>
  </EventIdentification>
  <ActiveParticipant NetworkAccessTypeCode="2"
    NetworkAccessPointID="{REMOTE_HOST_IP}" UserIsRequestor="true"
    UserID="http://www.w3.org/2005/08/addressing/anonymous">
    <RoleIDCode codeSystemName="DCM" displayName="Source"
      code="110153"/>
  </ActiveParticipant>
  <ActiveParticipant NetworkAccessTypeCode="2"
    NetworkAccessPointID="{XDS_SERVER_IP}" UserIsRequestor="false"
    UserID="{XDS_SOAP_URI}">
    <RoleIDCode codeSystemName="DCM" displayName="Destination"
      code="110152"/>
  </ActiveParticipant>
  <AuditSourceIdentification AuditSourceID="iCARDEA.XDS.b"
    AuditEnterpriseSiteID="iCARDEA.XDS.b"/>
  <ParticipantObjectIdentification ParticipantObjectTypeCodeRole="1"
    ParticipantObjectTypeCode="1" ParticipantObjectID="{PATIENT_ID}">
    <ParticipantObjectIDTypeCode code="2"/>
    <ParticipantObjectName>PatientIdentifier</ParticipantObjectName>
  </ParticipantObjectIdentification>
  <ParticipantObjectIdentification ParticipantObjectTypeCodeRole="20"
    ParticipantObjectTypeCode="2"
    ParticipantObjectID="{SUBMISSION_UID}">
    <ParticipantObjectIDTypeCode
      code="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd"/>
    <ParticipantObjectName>SubmissionSet</ParticipantObjectName>
  </ParticipantObjectIdentification>
</AuditMessage>

```

**Figure 5 A template audit record message for ITI-41**

The XML audit trail messages created using the format defined in Audit Trail Message Format Profile shall be transmitted to a collection point using the syslog over TLS mechanism, defined in RFC 5425. The XML audit trail message shall be inserted into the MSG portion of the SYSLOG-MSG element of the syslog message as defined in RFC 5424 "The Syslog Protocol". Should the XML audit message contain any Unicode characters they are encoded using the UTF-8 encoding rules. The following is an example of such SYSLOG message:

```

<85>1 2011-10-27T09:28:37Z example.com iCARDEA.XDS.b 8860 IHE+RFC-3881 -
\xef\xbb\xbf<AuditMessage>...</AuditMessage>

```

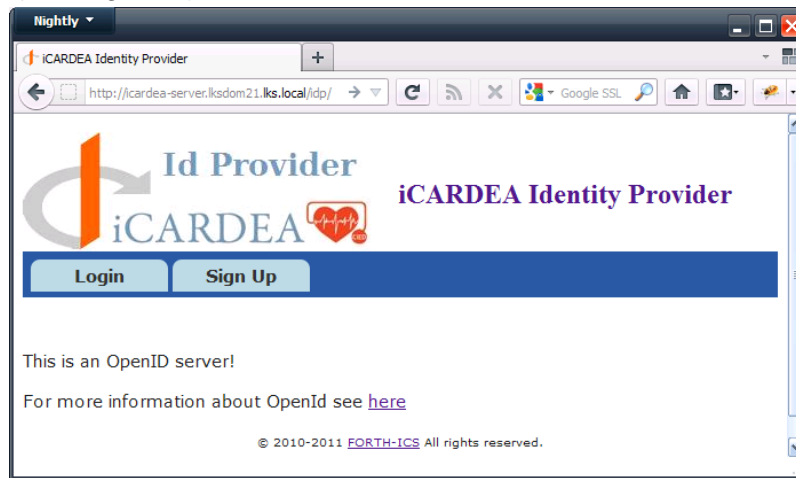
In this message there's again a timestamp, the hostname of the client (i.e. the "Secure Node" role in the ATNA profile), the application name ("iCARDEA.XDS.b" in the example), and the process id ("8860" in the example). All this information is entered in the SYSLOG Header while the XML audit trail payload comes in the MSG portion. Since this is encoded in UTF-8 format, the first three characters (shown as the byte sequence "\xef\xbb\xbf" in the example above, i.e. the hexadecimals 0xEF,0xBB,0xBF) represent the corresponding "byte order mark" (BOM) signifying this message as UTF-8 encoded.

## 4.4 THE ICARDEA ID PROVIDER

The idea behind the iCARDEA Id Provider is to have a single place where the authentication of the iCARDEA users happens so that the rest of the iCARDEA user applications do not bother storing passwords and other authentication information. From the technical side under the covers it uses the OpenID protocol but the user does not really need to know anything about it.

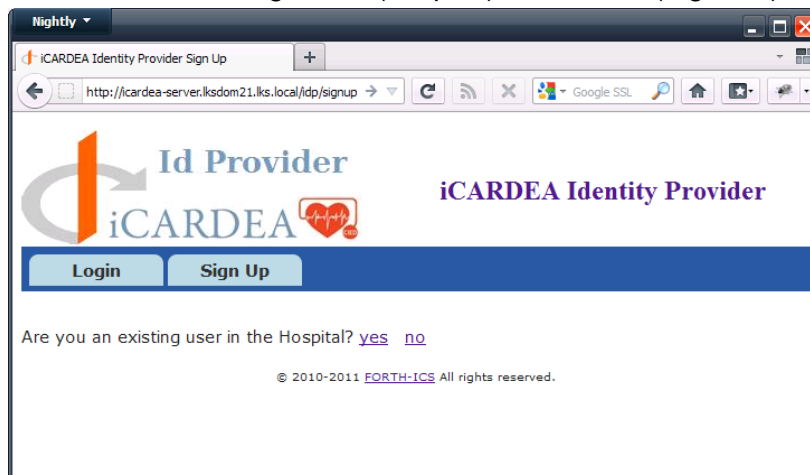
An additional requirement is to support the reuse of authentication provided by the Hospital computer network so that the existing hospital users need not to recreate any account or provide additional authentication (e.g. password) or other profile information. So from the end user point of view the registration of a new iCARDEA user is like the following<sup>3</sup>:

- A new user of iCARDEA needs first of all to visit the iCARDEA Id Provider at <http://icardea-server.lksdom21.lks.local/idp/> and select the “Sign Up” menu option (see Figure 6)



**Figure 6 The initial "welcome" page of the Id Provider**

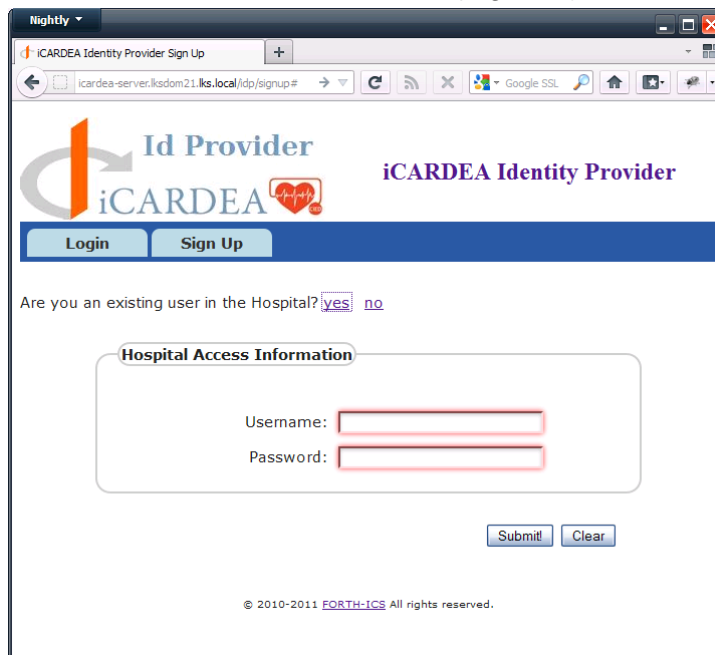
- After selecting the “sign up” menu option, at the next screen, she is asked whether she’s an existing SALK (hospital) user or not (Figure 7)



**Figure 7 "Signing up" to the Id Provider**

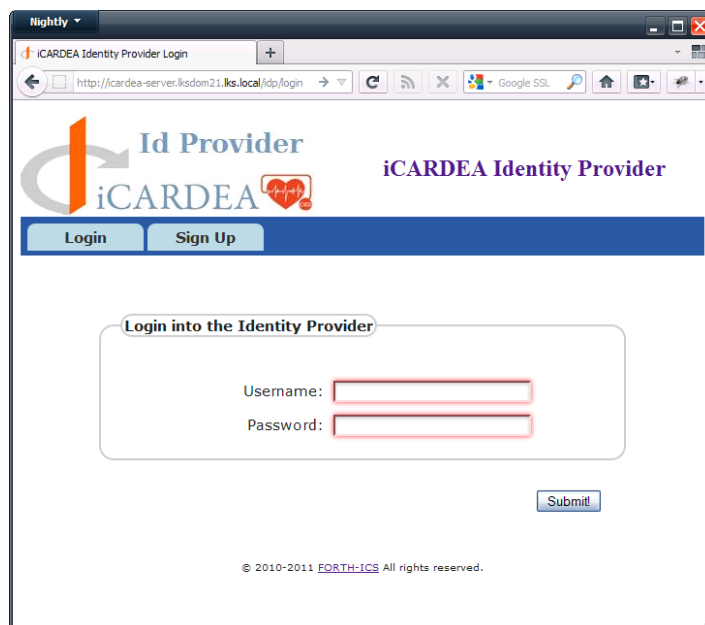
<sup>3</sup> For this description we use the SALK pilot installation as an example.

- When s/he declares that she's an existing Hospital user by choosing "yes", she is requested to give her user name and password i.e. the same credentials that she uses to log into the SALK windows machines (Figure 8)



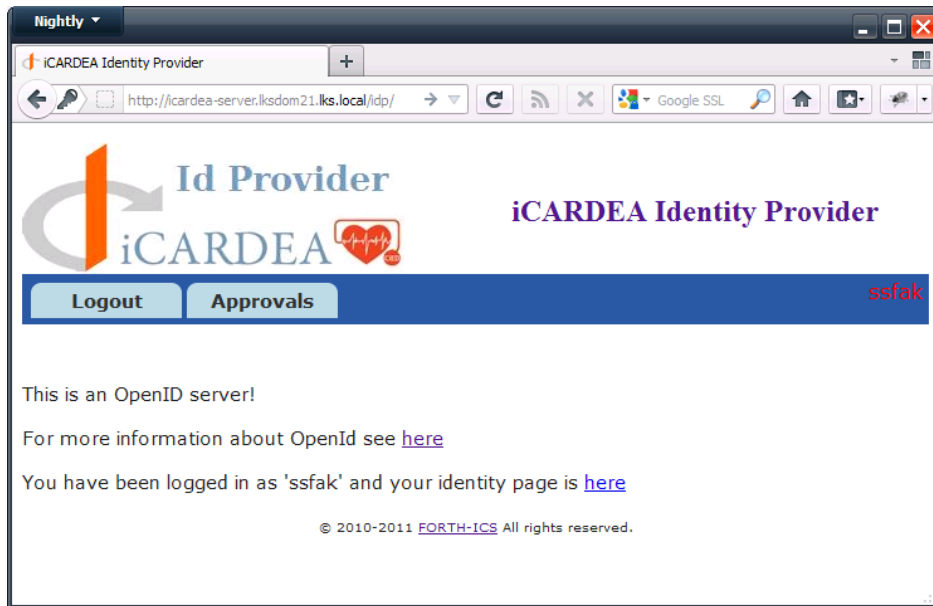
**Figure 8 The user is asked to give the same username and password that he/she uses for logging into the SALK MS Windows machines**

- After the successful validation of the SALK credentials the user is a valid iCARDEA user with his identifier constructed based on his windows user name, i.e. the iCARDEA username will be the same username the user has in the Hospital machines.
- The user can then log into the id provider giving his/her existing (SALK's) user name/ password information and use the rest of iCARDEA applications (Figure 9 **Error! Reference source not found.**)



**Figure 9 The login page of the Id Provider**

- After the successful login the user is presented with a page similar to the one shown in Figure 10. In the menu on the right side the user should see its username (ssfak as shown in the example figure above) but there are also some new menu options. The first is for “logging out” of the iCARDEA and the second one is about the current “Approvals”. Basically the “approvals” are the list of iCARDEA applications that the user has allowed to be silently “logged into” immediately. An example of this “approval” mechanism is shown in the next paragraph when we try to log into the PIX Manager.



**Figure 10** The initial page of the Id Provider after the user has successfully logged in.

Under the covers there’s a communication with the Windows “domain controller” in order to authenticate the users and also to get some information about their “profile”. The currently retrieved information is their (given and full) name, and the list of groups they belong to. This information is supplied to the “Relying Parties” through the use of the Simple Registration (SReg), where this is possible, and Attribute Exchange (AX) extensions as described in the following table:

Profile Information	SReg attribute	AX attribute type URI
<b>User name (alias)</b>	openid.sreg.nickname	<a href="http://openid.net/schema/namePerson/friendly">http://openid.net/schema/namePerson/friendly</a>
<b>First name</b>	-	<a href="http://openid.net/schema/namePerson/first">http://openid.net/schema/namePerson/first</a>
<b>Full name</b>	openid.sreg.fullname	<a href="http://schema.openid.net/namePerson">http://schema.openid.net/namePerson</a>
<b>Groups (multiple values)</b>	-	<a href="http://www.w3.org/2006/vcard/ns#role">http://www.w3.org/2006/vcard/ns#role</a>

Some notes are in order:

- We supply both the “given” (first) name and the “full” name because they serve different purposes. Both can be extracted in distinct forms from the MS Windows Active Directory server but the given name can be used to provide a more “friendly” user interface in the Relying Party’s web site while the full name is important for identification reasons<sup>4</sup>.
- SReg [8] supports strictly the following attributes: `nickname`, `email`, `fullname`, `dob`, `gender`, `postcode`, `country`, `language`, and `timezone`. So there’s no support for the “given” name or the “groups” information
- The AX extension is more generic than the Simple Registration because it allows an extensible set of attributes to be transmitted. The identification of the attributes is through the use of “type URIs” and there’s a (kind of) standard set of such attributes described in that we reuse here.
- Unfortunately there’s no attribute type URI for the group membership in [10]. But the vCard specification [12] defines the “Role” attribute “to specify the function or part played in a particular situation by the object the vCard represents” and there’s a W3C Submission [13] to build a vCard RDF ontology that provides URIs for all the vCard attributes. We have therefore reused the URI for the role attribute from this specification.

## 5 References

- [1] T. Dierks, E. Rescorla "The Transport Layer Security (TLS) Protocol, Version 1.2", RFC 5246, August 2008
- [2] E. Rescola: *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley Professional, Addison-Wesley Professional 2000, ISBN-13: 978-0201615982
- [3] ITU-T Recommendation X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks <http://www.itu.int/rec/T-REC-X.509/en>
- [4] F. Miao, Y. Ma, J. Salowey, IETF, Transport Layer Security (TLS) Transport Mapping for Syslog, <http://tools.ietf.org/html/rfc5425>
- [5] N. Ragouzis et al., Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS Committee Draft, March 2008. Document ID sstc-saml-tech-overview-2.0-cd-02 <http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf>
- [6] SAML V2.0 Interoperability Demonstration Scenarios, Guidelines & Final Report, RSA Conference 2005 February 14-17 San Francisco, CA: <http://www.oasis-open.org/committees/download.php/11915/RSA2005-saml-interop-final.pdf>
- [7] “OpenID Authentication 2.0 - Final,” August 2007, [http://openid.net/specs/openid-authentication-2\\_0.html](http://openid.net/specs/openid-authentication-2_0.html)
- [8] “Simple Registration Extension 1.0”, June 2006, [http://openid.net/specs/openid-simple-registration-extension-1\\_0.html](http://openid.net/specs/openid-simple-registration-extension-1_0.html)
- [9] “OpenId Attribute Exchange 1.0 - Final”, December 2007, [http://openid.net/specs/openid-attribute-exchange-1\\_0.html](http://openid.net/specs/openid-attribute-exchange-1_0.html)
- [10] G. Marshall “Security Audit and Access Accountability XML Message Data Definitions for Healthcare Applications”, RFC 3881, September 2004
- [11] “Attribute Properties for OpenID Attribute Exchange”, August 2006, [http://openid.net/specs/openid-attribute-properties-list-1\\_0-01.html](http://openid.net/specs/openid-attribute-properties-list-1_0-01.html)

---

<sup>4</sup> If anyone thinks that it’s easy to construct the full name from the given and the surname or that any such name splitting and joining is easy in international settings, he should read this: <http://www.w3.org/International/questions/qa-personal-names>

- [12] S. Perreault " vCard Format Specification", RFC 6350, August 2011
- [13] Renato Iannella, "Representing vCard Objects in RDF", W3C Submission, January 2010, <http://www.w3.org/Submission/vcard-rdf/>