



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 D4.4.1 Security and Privacy for Personalized Adaptive Care Planner

<i>Due Date:</i>	January 31, 2012
<i>Actual Submission Date:</i>	January 23, 2012
<i>Project Dates:</i>	Project Start Date : February 01, 2010 Project End Date : January 31, 2013 Project Duration : 36 months
<i>Leading Contractor Organization:</i>	SRDC

Document History:

Version	Date	Changes	From	Review
V01	January 04, 2012	Initial draft	SRDC	All partners
V02	January 23, 2012	Final Version	SRDC	All partners

Contributors

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

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)		
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	Robert Mulrenin	+43 (0)662 2288 403	+43 (0)662 2288 222	robert.mulrenin@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

PURPOSE	5
1.1 DEFINITIONS AND ACRONYMS.....	5
2 INTRODUCTION	5
3 STANDARDS.....	7
3.1 ATNA INTEGRATION PROFILE.....	7
3.1.1 <i>TLS and Digital Certificates</i>	8
3.2 OPENID	8
4 THE ICARDEA SECURITY INFRASTRUCTURE	9
4.1 POSITION OF ADAPTIVE CARE PLANNER IN ICARDEA SECURITY INFRASTRUCTURE.....	11
4.2 SECURITY REQUIREMENTS OF ADAPTIVE CARE PLANNER.....	11
5 OPENID IMPLEMENTATION FOR ADAPTIVE CARE PLANNER	13
5.1 OBTAIN THE USER-SUPPLIED IDENTIFIER	14
5.2 DISCOVERY.....	14
5.3 ASSOCIATION.....	15
5.4 AUTHENTICATION	15
5.5 VERIFICATION	15
5.6 PROCEED TO APPLICATION	16
6 THE ATNA PROFILE IMPLEMENTATION FOR ADAPTIVE CARE PLANNER	16
6.1 AUDIT TRAIL.....	16
6.2 NODE AUTHENTICATION	22
7 CONCLUSION	23

PURPOSE

This document aims to provide details on the design principles and the implementation of the security and privacy requirements for iCARDEA Personalized Adaptive Care Planner based on the security architecture established in Task 6.5. Its main focus is on the interactions and the communications between the Personalized Adaptive Care Planner and the other iCARDEA components and as well as the end user sessions.

1.1 DEFINITIONS AND ACRONYMS

Table 1 List of Abbreviations and Acronyms

Abbreviation/ Acronym	DEFINITION
ADT	Admission, Discharge and Transfer
ATNA	Audit Trail and Node Authentication
ARR	Audit Record Repository
AX	OpenID Attribute Exchange extension
CA	Certification Authority
CIED	Cardiovascular Implantable Electronic Device
CM	Care Management
CSR	Certificate Signing Request
DICOM	Digital Imaging and Communications in Medicine
EHR	Electronic Health Record
HL7	Health Level 7
HTTP	Hypertext Transfer Protocol
IdP	OpenId Identity Provider
IHE	Integrating the Healthcare Enterprise
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
PPM	Patient Parameter Monitor
RP	OpenId Relying Party
SSL	Secure Sockets Layer
SReg	OpenId Simple Registration extension
TLS	Transport Layer Security

2 Introduction

Security in information systems means protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. This concept 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. The following key concepts related to information security show some of these characteristics:

- **Confidentiality:** This is the term used to prevent the disclosure of information to unauthorized individuals or systems. This can be provided through authorization mechanisms, encryption and privacy techniques.
- **Integrity:** In information security respect, integrity means that data cannot be modified undetectably. This covers data in storage, during processing, and while in transit.
- **Authentication:** It is necessary to ensure that the data, transactions, communications or documents are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are. This can be done verification of the identity of user, process, or device.
- **Authorization:** In security information, authorization is to define access policy over the resources. The system must ensure that the resources are accessible only to those people who are authorised to do so.
- **Accountability:** This property generates the requirement for actions of an entity to be traced uniquely to that entity supporting non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action.
- **Privacy:** This concern exists wherever personally identifiable information is collected and stored. The challenge in data privacy is to share data while protecting personally identifiable information.

In this document we will focus on the way to meet these key concepts for the iCARDEA Adaptive Care Planner which is one of the main parts of iCARDEA architecture shown in Figure 1.

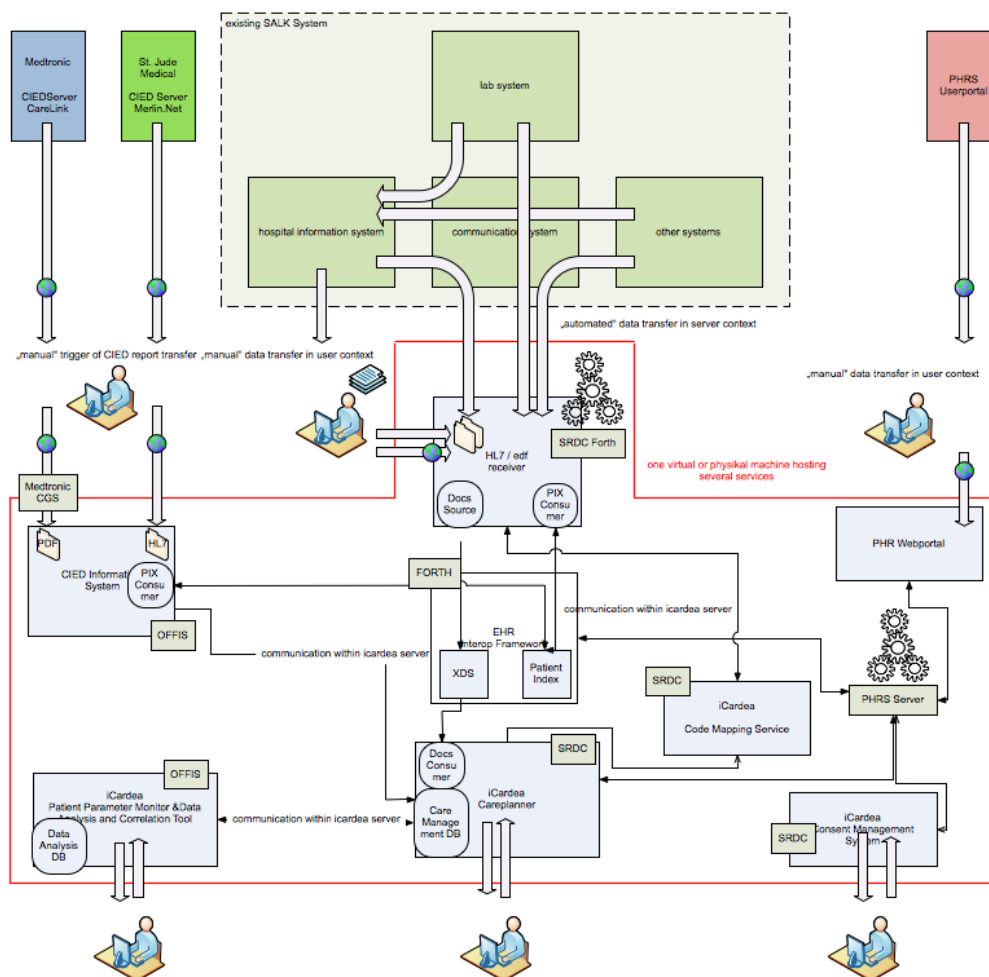


Figure 1 iCARDEA Deployment architecture

The communication between Adaptive Care Planner and the other iCARDEA components is provided over IHE specified “transactions” such as PCC-09 and PCC-10 for IHE CM profile, and PCD-09 for IHE-IDCO profile. IHE also provides another integration profile, IHE *Audit Trail and Node Authentication (ATNA)*, to ensure the adaptation of the necessary the security mechanisms for IHE based transactions. ATNA, references a set of standards for implementing the security mechanisms. ATNA profile and these common standards are explained in the following section.

In addition to this, OpenID standard is used for Adaptive Care Planner which describes how users can be authenticated in a decentralized manner. This web based solution to the Single Sign-On problem provides to reuse of the identities and credentials when signing up into multiple web sites. The details about this open standard is explained in section 3.2.

3 Standards¹

3.1 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)².

¹ Please note that these standards are also introduced in D6.5.1, however to have a self complete deliverable this section is repeated in this deliverable too.

² F. Miao, Y. Ma, J. Salowey, IETF, Transport Layer Security (TLS) Transport Mapping for Syslog, <http://tools.ietf.org/html/rfc5425>

3.1.1 TLS and Digital Certificates

Transport Layer Security (TLS)³ and its predecessor, Secure Sockets Layer (SSL)⁴, 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.509⁵ *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 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).

³ T. Dierks, E. Rescorla "The Transport Layer Security (TLS) Protocol, Version 1.2", RFC 5246, August 2008

⁴ E. Rescorla: SSL and TLS: Designing and Building Secure Systems, Addison-Wesley Professional, Addison-Wesley Professional 2000, ISBN-13: 978-0201615982

⁵ 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>

⁶ "OpenID Authentication 2.0 - Final," August 2007, http://openid.net/specs/openid-authentication-2_0.html

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 Registration⁷, while a more modern and extensible way is the one specified by the Attribute Exchange⁸.

4 The iCARDEA Security Infrastructure

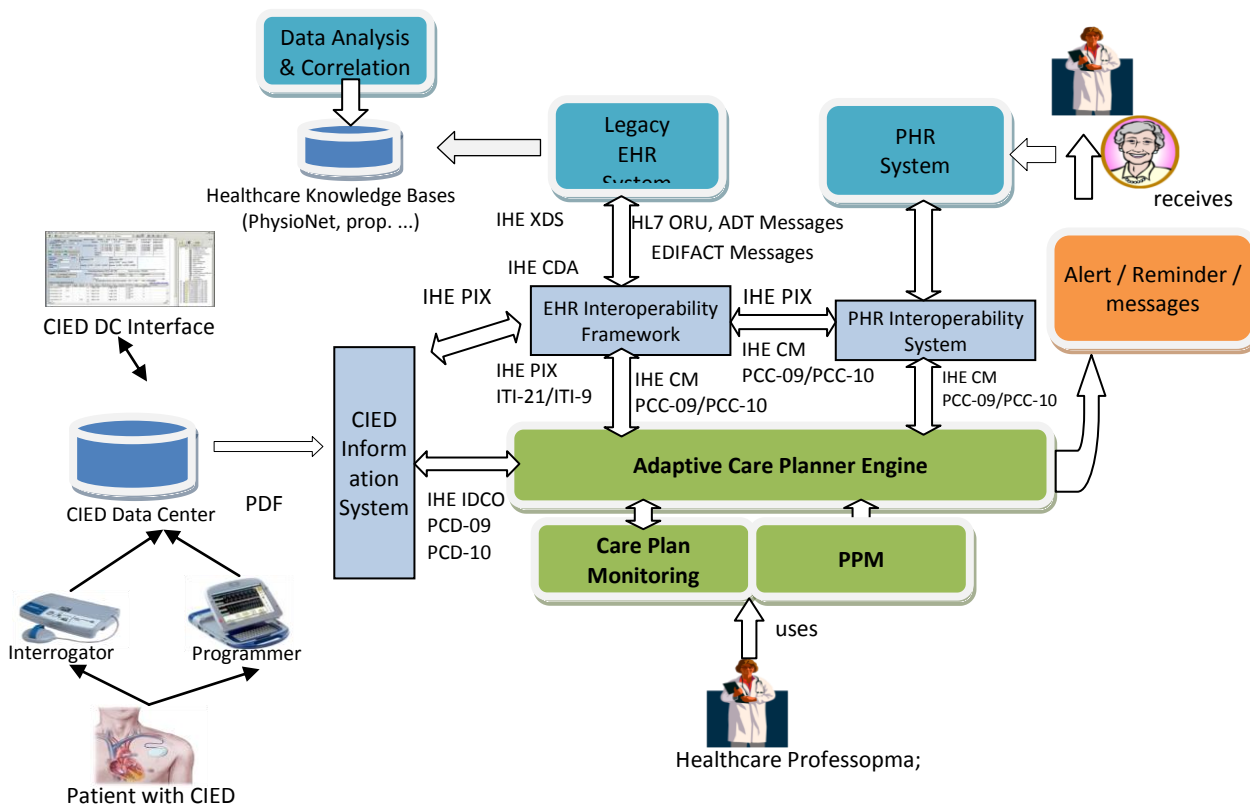


Figure 2: iCARDEA Interoperability Infrastructure – IHE Integration Profiles /Transactions

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

⁷ “Simple Registration Extension 1.0”, June 2006, http://openid.net/specs/openid-simple-registration-extension-1_0.html

⁸ “OpenId Attribute Exchange 1.0 - Final”, December 2007, http://openid.net/specs/openid-attribute-exchange-1_0.html

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 encrypts the messages exchanged through TLS and digital certificates. Implementation also ensures accountability, as ATNA Audit Trails are also 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 Deliverable 5.4.1.

In Task 6.5, the general security and privacy requirements of iCARDEA architecture are analyzed and based on this analysis, the core components of iCARDEA Security Infrastructure are implemented as explained in Deliverable D6.5.1. These components are:

- **iCARDEA Certification authority:** This CA is setup for the needs of verifying peers in the SSL/TLS connections of the iCARDEA components that the IHE ATNA profile requires. This iCARDEA CA is set to be trusted by all components of the iCARDEA platform and all these components and services have their certificates signed by this CA.
- **iCARDEA Audit record repository:** ATNA is an IHE security profile representing Audit Trail and Node Authentication, which was described in Section 3.1. OpenATNA⁹ is an Open Source implementation of an Audit Record Repository supporting RFC 3881 audit messages¹⁰ over BSD Syslog as well as RFC 5424-5426 (UDP and TLS). For the Care Planner, the following are the relevant IHE transactions that require the submission of audit record events to this Audit Record Repository (ARR).
 - PIX Query (ITI-9) and Patient Demographics Query (ITI-21)
 - PCC-9 (QUPC_IN043100UV) and PCC-10(QUPC_IN043200UV)
 - Send Observation (PCD-9)
- **iCARDEA ID provider:** This component provides 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. It uses the OpenID protocol and supports 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 or other profile information.

As stated in Deliverable 6.5.1, there is a communication with the Windows “domain controller” in order to get some information about their “profile” by supplying to the “Relying Parties” through the use of the Simple Registration (SReg) and Attribute Exchange (AX) extensions.

In the following sections, we will first of all revisit the analysis of security requirements for iCARDEA architecture to highlight the security requirements particularly for iCARDEA Personalized Adaptive Care Planner security implementation through use cases. Then, the security of privacy implementation of iCARDEA Personalized Adaptive Care Planner will be explained, detailing how it builds upon the core components of iCARDEA Security and privacy architecture.

⁹ OpenATNA: <https://www.projects.openhealthtools.org/sf/projects/openatna/>

¹⁰ G. Marshall “Security Audit and Access Accountability XML Message Data Definitions for Healthcare Applications”, RFC 3881, September 2004

4.1 POSITION OF ADAPTIVE CARE PLANNER IN ICARDEA SECURITY INFRASTRUCTURE

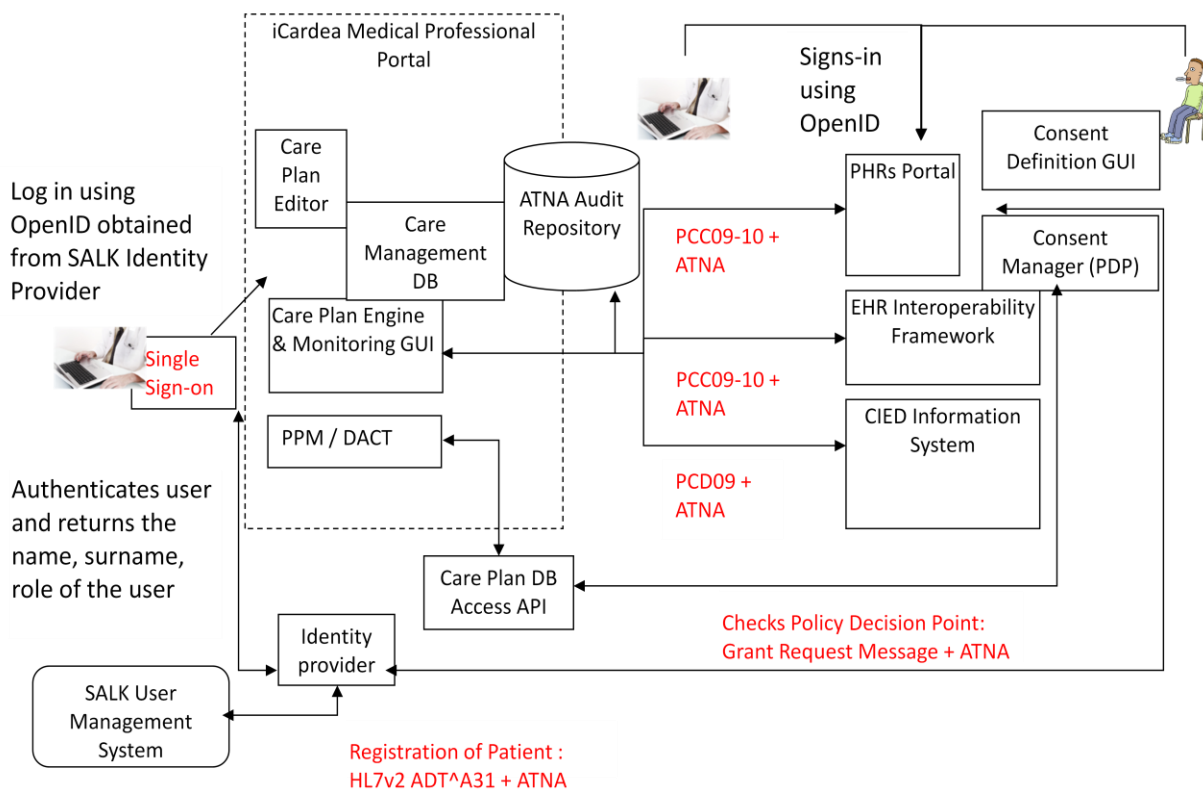


Figure 3: iCARDEA Security Infrastructure

In Figure 3, the basics of iCARDEA Security architecture are presented. In this figure, the interactions marked with red colour show the target transactions of the security and privacy implementation of Adaptive Care Planner. These interactions are elaborated through the use case definitions presented in section 4.2.

4.2 SECURITY REQUIREMENTS OF ADAPTIVE CARE PLANNER

Security requirements of Adaptive Care Planner focuses on implementation of OpenID protocol in order to authenticate medical professional before accessing Adaptive Care Planner and implementation of IHE ATNA Profile for sending and receiving messages securely over TLS and logging all the events to ATNA Audit Repository. The requirements in conformance with the Deliverable D6.5.1 (use case numbers) are explained step by step in the following subsections:

UC-1: Medical Professional Log-in for using iCARDEA Adaptive Care Planner with OpenID standard

1. When a Medical Professional wants to access any Adaptive Care Planner web interface, 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 OpenID Identity Provider (IdP) 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 by using convenient extensions of this profile.
 3. After successful authentication, the user can use Adaptive Care Planner.

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 and they are sent over TLS to the related end points of this external systems.
3. These are logged to ATNA Audit Repository.

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 and they are sent over TLS to the end point of Care Plan Engine.
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 and they are sent over TLS to the end point of Care Plan Engine.
3. These are logged to ATNA Audit Repository.

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

1. Prerequisite: Certificates for Care Plan Engine and EHR Interoperability Framework are created and shared beforehand.
2. SALK Personnel need to log in the PIX Manager Web Interface following the procedure described in UC-1 above.
3. Patient’s HIS ID, Demographic data, CIED ID and Protocol ID is entered through PIX Manager Web Interface by SALK Personnel.
4. These are stored in the PIX Manager to answer PIX Queries to be received in the future.
5. When PIX Manager stores these information, HL7v2 ADT^A31 message is sent to Care Plan Engine as Update Person Information.
6. All the above actions are logged to the ATNA Audit Repository.

UC-8: An authorized Medical Professional wants to access Patient Data through Patient Parameter Monitor(PPM)

1. An authorized Medical Professional logs in to the iCardea Medical Professional Portal through its OpenID (UC-1) 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. These are logged to ATNA Audit Repository.

5 OpenID Implementation for Adaptive Care Planner

As stated in section 3.2, OpenID is an open standard that describes how users can be authenticated in a decentralized manner defining 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.

As stated in Deliverable 6.5.1 Security and Privacy of the Interoperability Layer, Identity Provider was implemented to authenticate the users before accessing the iCARDEA components. For Adaptive Care Planner, a Relying Party (RP) is implemented communicating this Identity Provider as a "Consumer" by using openid4java¹¹ library allowing creation of Open ID enabled java web applications.

As a brief introduction to this process, the whole point of authentication is for the user to prove his/her identity. Once the user has proved his/her identity, Identity Provider decides whether or not to grant him/her access to the desired resource and return the response to the relying party. Basic steps for this process are:

1. **Obtain the User-Supplied Identifier:** The RP gets the user's OpenID identifier.
2. **Discovery:** The RP normalizes this identifier to determine which IdP to contact for authentication and how to contact it.
3. **Association:** As an optional step, RP and IdP may establish a secure communication channel.
4. **Authentication request:** The RP asks the IdP to authenticate the user.
5. **Verification:** The RP requests userid verification from the IdP and ensures the communication has not been tampered with.
6. **Proceed to application:** Following authentication, the RP directs the user to the resource he/she initially requested.

¹¹ "openid4java": <http://code.google.com/p/openid4java/>

5.1 OBTAIN THE USER-SUPPLIED IDENTIFIER

In this phase, user enters his/her identifier registered to Identity Provider before and clicks "Verify" button in order to access the application after authenticating by IdP (Figure 4).

After retrieving user identifier, three steps should be followed in the order of:

- Performing discovery on the User-Supplied Identifier
- Creating the openid4java AuthRequest object that will be used to make the authentication request
- Redirecting the browser to the OpenID provider

After redirecting the browser, this phase is done and control is in the hands of the IdP.

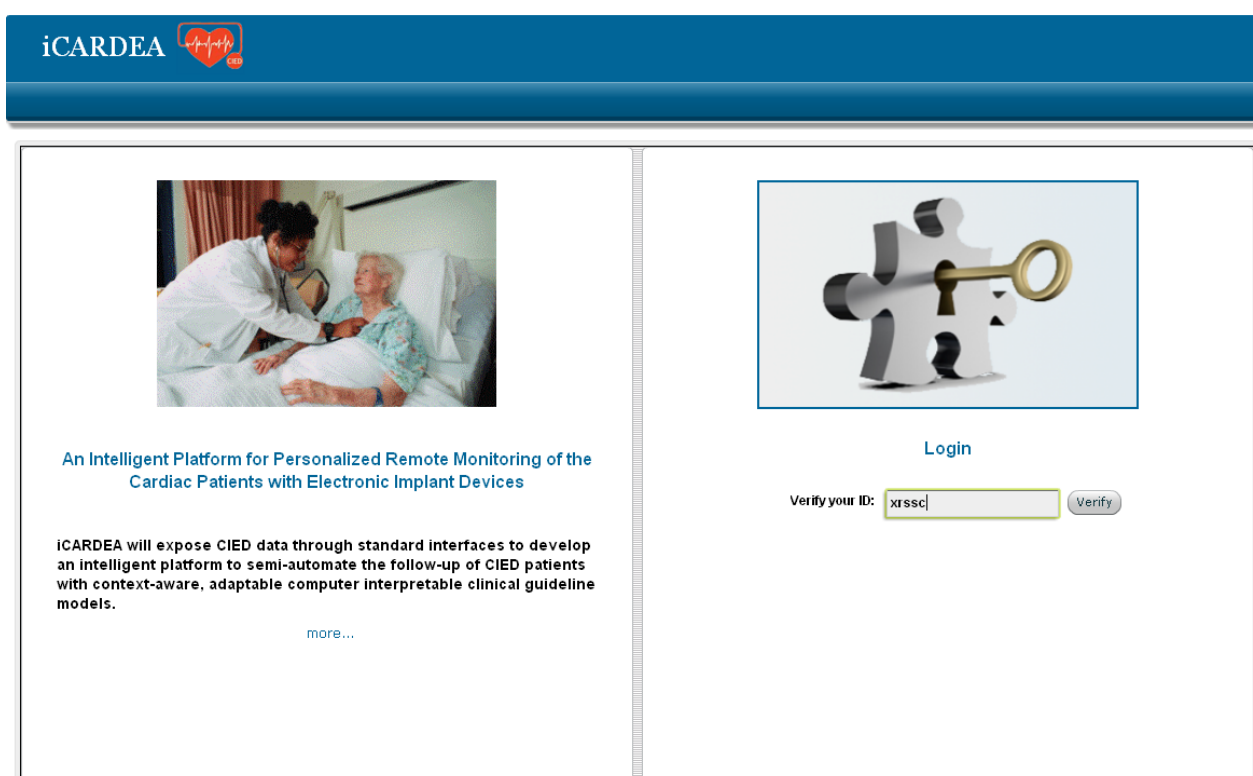


Figure 4: Obtain Identifier for Care Planner

5.2 DISCOVERY

The RP takes the User-Supplied Identifier and converts it to a form that can be used to determine two things: who the Identity Provider (IdP) is and how to contact the IdP.

The process of discovery is used by the RP to determine how to make requests of the IdP, and the key is the User-Supplied Identifier. To perform discovery on this identifier, ConsumerManager class is used through the getConsumerManager() method. What is returned is a java.util.List of DiscoveryInformation objects which are treated as opaque objects kept for association with the IdP.

5.3 ASSOCIATION

Association is a way for the RP and the IdP to establish a shared secret to make their interactions more trusted and secure. Association is not required by the OpenID specification. Association is performed from the RP code with a single call to the `associate()` method on `ConsumerManager`.

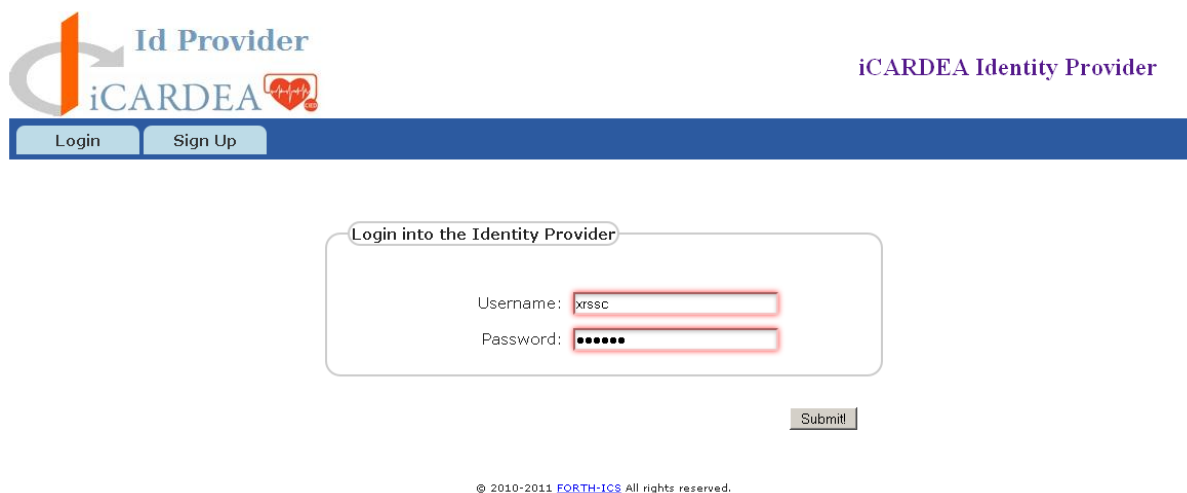
This method returns the `DiscoveryInformation` object that describes the results of the discovery. This object is going to be used to make the authentication request.

5.4 AUTHENTICATION

After the RP has successfully performed discovery on the User-Supplied Identifier, it's time to authenticate the user. `ConsumerManager` is asked to build a special object called `AuthRequest` that will be used by the IdP to process the authentication request.

During this interaction, the IdP will be asked to make use of an OpenID extensions called `SimpleRegistration (SReg)` and `Attribute Exchange (AX)` enabling the RP to request that certain attributes from the user's profile with the IdP to be returned in the response.

At this point, the browser is directed to the OpenID Provider that is responsible for authenticating the user, where the user will enter his or her password. In Figure 5, Identity Provider is authenticating a request.



Id Provider
iCARDEA

iCARDEA Identity Provider

Login Sign Up

Login into the Identity Provider

Username: xrssc

Password: ●●●●●●

Submit!

© 2010-2011 FORTH-ICS All rights reserved.

Figure 5: Authentication of request by Identity Provider

5.5 VERIFICATION

In this phase, the main purpose is to find out whether a request has come from the IdP. If it has, there will be a parameter, `is_return`, whose value is true. If this is the case, then `openid4java` is used to verify the request which is a response from the IdP and pull out the attributes that are requested with OpenID extensions.

After getting the intended attributes when successful verification is done, application can proceed with its intended function.

5.6 PROCEED TO APPLICATION

If the response to the authentication request is successfully verified, the user is granted access to whatever resource was being protected by the RP through OpenID. In the case of the Care Planner, this is the process of registration. After successful verification, main page of Care Planner is opened and ready to use by the authenticated user (Figure 6).

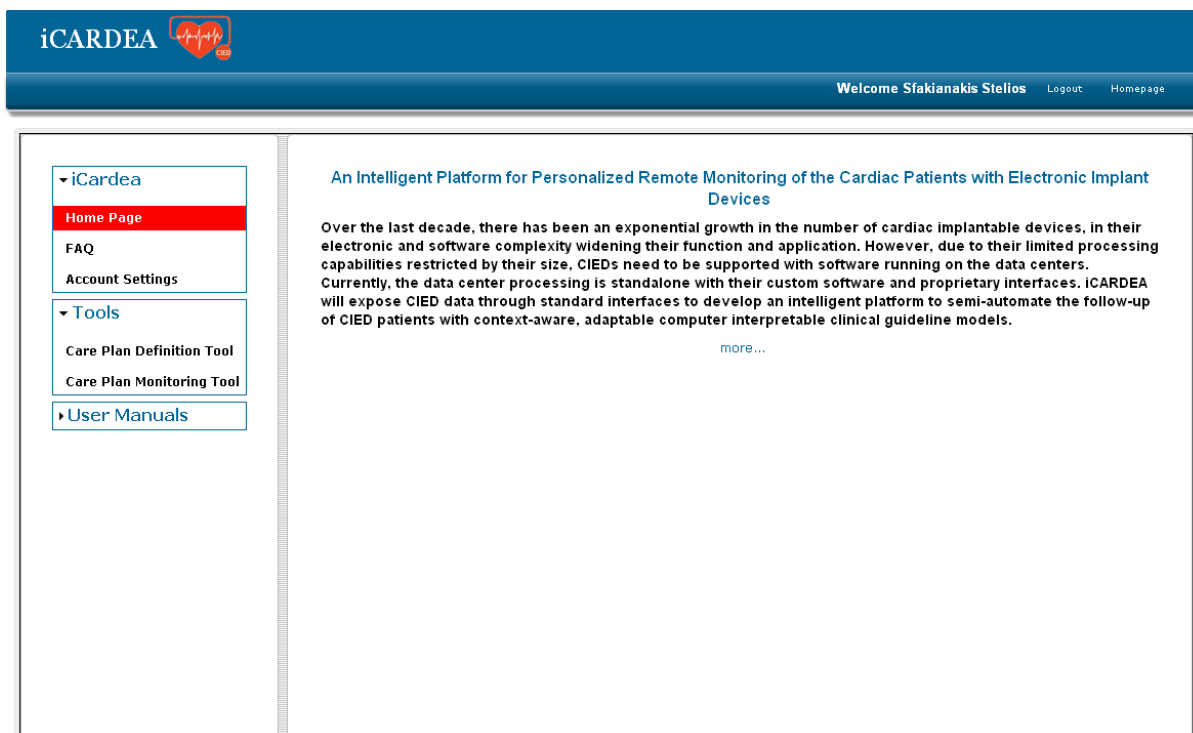


Figure 6: Care Planner after successful verification

6 IHE ATNA Profile Implementation for Adaptive Care Planner

As stated in section 3.1, IHE ATNA(Audit Trail and Node Authentication) Profile provides secure exchange of healthcare information and the auditing of events related to the access, production or modification of healthcare information. In order to achieve secure exchange of information between Care Planner and the other components as well as auditing all transactions, two parts of this profile is implemented separately for Care Planner, namely Audit Trail and Node Authentication.

6.1 AUDIT TRAIL

For the Audit Trail part of IHE ATNA profile, ITI-20 Record Audit Event transaction is used to store an audit record in the Audit Log for any “important” interaction. For this transaction,

Audit Record format is compatible with IHE Audit Trail XML format which covers RFC 3881¹² standard and IHE codes. This format has the following structure shown in Figure 7.

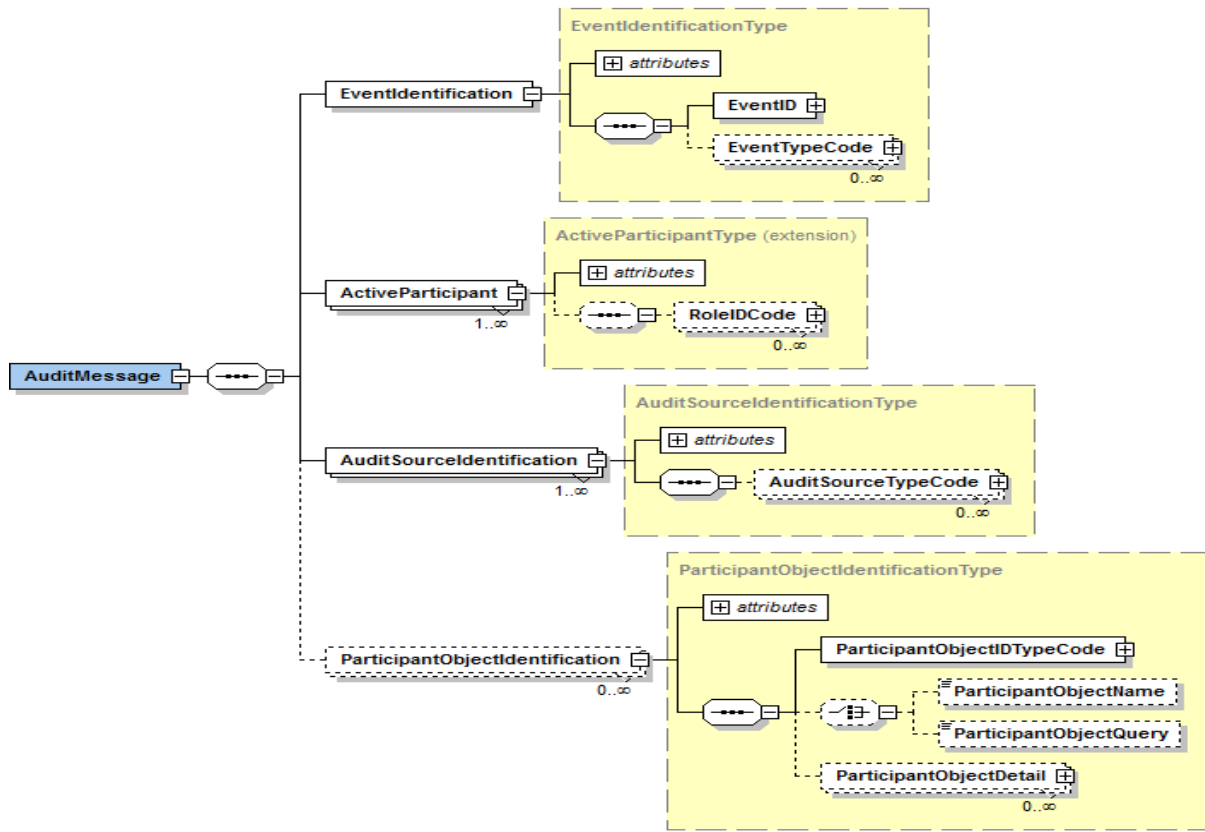


Figure 7: RFC 3881 Audit Record format

In this format, Event Action Code and Event Outcome Indicator attributes in Event Identification can be the one of the predefined values as follows:

Value	Meaning	Examples
C	Create	Create a new database object, such as Placing an Order
R	Read/View/Print/Query	Display or print data, such as a Doctor Census
U	Update	Update data, such as Revise Patient Information
D	Delete	Delete items, such as a doctor master file record
E	Execute	Perform a system or application function such as log-on, program execution, or use of an object's method

Figure 8: Event Action Code values

¹² G. Marshall "Security Audit and Access Accountability XML Message Data Definitions for Healthcare Applications", RFC 3881, September 2004

Value	Meaning
0	Success
4	Minor failure; action restarted, e.g., invalid password with first retry
8	Serious failure; action terminated, e.g., invalid password with excess retries
12	Major failure; action made unavailable, e.g., user account disabled due to excessive invalid log-on attempts

Figure 9: Event Outcome Indicator values

In addition to these, to define Event Identification properly, we need to define Event IDs and Event Type Codes for auditing Care Planner transactions with a suitable manner. The values of these elements are:

```
<CodeType name="EventId">
  <!-- icardea start -->
  <Code code="COBSCAT" codingScheme="IHE" display="All Vital Signs"/>
  <Code code="MEDCCAT" codingScheme="IHE" display="All problem entries"/>
  <Code code="CONDLIST" codingScheme="IHE" display="All Concern Entries"/>
  <Code code="PROBLIST" codingScheme="IHE" display="All Problem Concerns"/>
  <Code code="INTOLIST" codingScheme="IHE" display="All Allergy Concerns"/>
  <Code code="RISKLIST" codingScheme="IHE" display="All Risks"/>
  <Code code="LABCAT" codingScheme="IHE" display="All Lab Results"/>
  <Code code="DICAT" codingScheme="IHE" display="All Imaging Results"/>
  <Code code="RXCAT" codingScheme="IHE" display="All Medications"/>
  <Code code="MEDLIST" codingScheme="IHE" display="All Medications"/>
  <Code code="CURMEDLIST" codingScheme="IHE" display="All active medications"/>
  <Code code="DISCHMEDLIST" codingScheme="IHE" display="Discharge Medications"/>
  <Code code="HISTMEDLIST" codingScheme="IHE" display="All Historical Medications"/>
  <Code code="IMMUCAT" codingScheme="IHE" display="All Immunizations"/>
  <Code code="PSVCCAT" codingScheme="IHE" display="All professional service entries"/>
  <Code code="CIED" codingScheme="IHE" display="Cardiac Implantable Electronic Device"/>
  <Code code="{resource}" codingScheme="IHE" display="Grant Request Message"/>
  <!-- icardea end-->
</CodeType>
<CodeType name="EventType">
  <!-- icardea start -->
  <Code code="PCC-9" codingScheme="IHE Transactions"/>
  <Code code="PCC-10" codingScheme="IHE Transactions"/>
  <Code code="PCD-9" codingScheme="IHE Transactions"/>
  <Code code="ADT-01" codingScheme="IHE Transactions"/>
  <Code code="Consent Request" codingScheme="IHE Transactions"/>
  <!-- icardea end -->
</CodeType>
<CodeType name="ObjectIdType">
  <!-- icardea start -->
  <Code code="iCardea" display="Patient ID"/>
  <!-- icardea end -->
</CodeType>
```

Figure 10: Event ID and Event Type values for Care Planner transactions

These values are used to define related Audit Record messages for Care Planner which interacts with EHR, PHR and CIED Data Exposure systems shown in red in the Figure 3: iCARDEA Security Infrastructure.

For this purpose, five types of Audit Record message templates are prepared to send them to Audit Record Repository when any transaction is done with the participation of Care Planner. These messages are presented between Figure 11 and Figure 15.

In Figure 11, the audit record message represents PCC-09 transaction between Care Planner and EHR system. This is read action and this transaction takes place from Care Planner to EHR system. For the same action, the audit message for this transaction is the same for PHR system.



Figure 11: Audit Record Message for PCC-09 transaction

In Figure 12, the audit record message represents PCC-10 transaction between Care Planner and PHR system. This is create action and this transaction takes place from PHR system to Care Planner. For the same action, the audit message for this transaction is the same for EHR system.

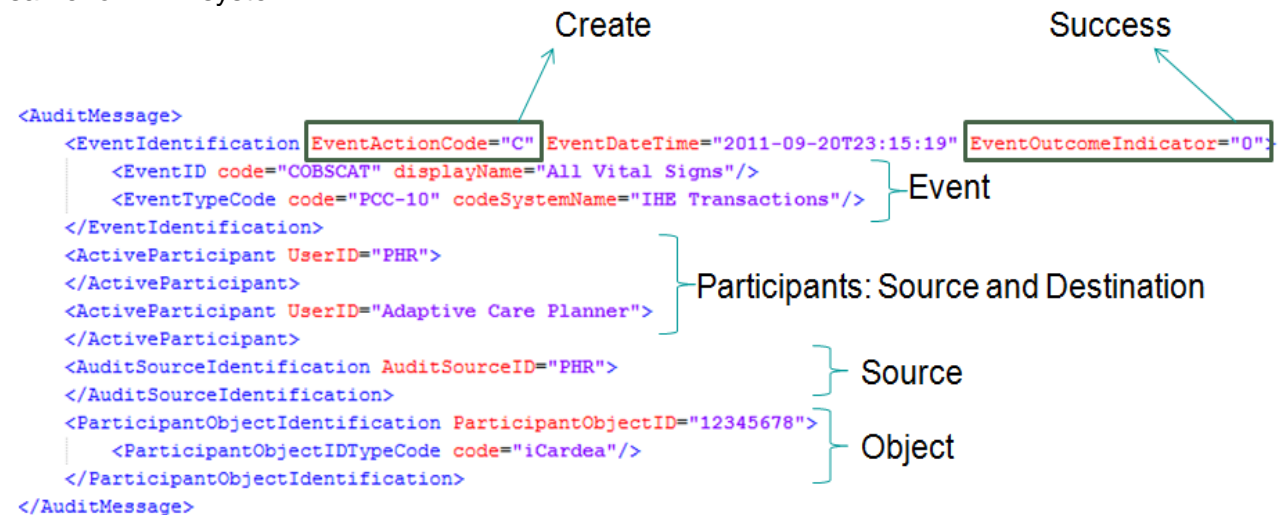


Figure 12: Audit Record Message for PCC-10 transaction

In Figure 13, the audit record message represents PCD-09 transaction between Care Planner and CIED Data Exposure system. This is create action and this transaction takes place from CIED Data Exposure system to Care Planner.

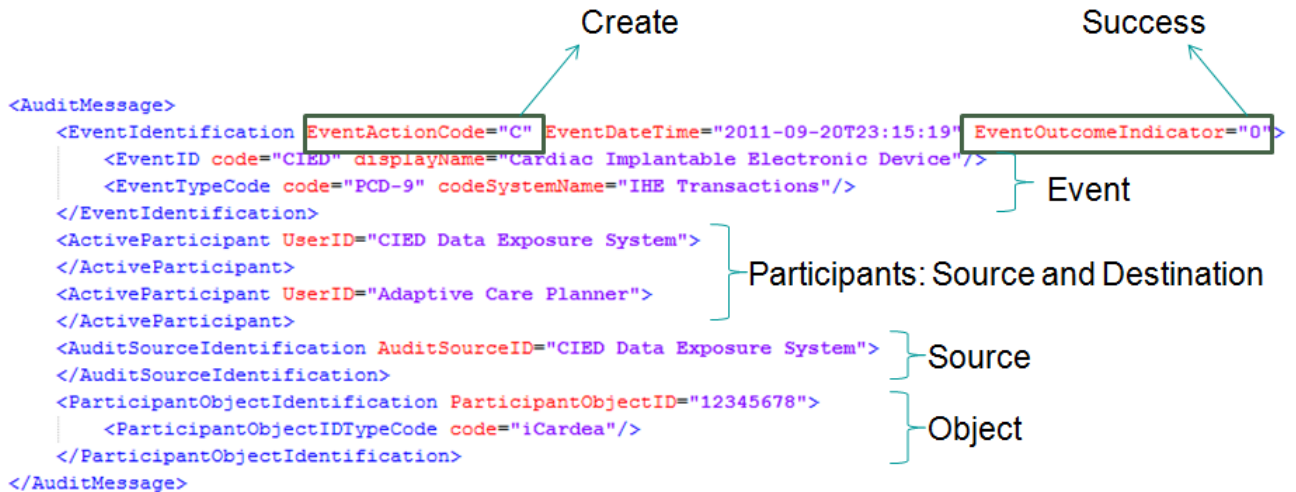


Figure 13: Audit Record Message for PCD-09 transaction

In Figure 14, the audit record message represents HL7v2 ADT^A31 transaction using HL7's generic 'Update Person Information' message to communicate the patient-centric information between Care Planner and Patient Identifier Cross-reference (PIX) Manager. This is create action and this transaction takes place from PIX Manager to Care Planner when a new patient is registered to the iCARDEA system.

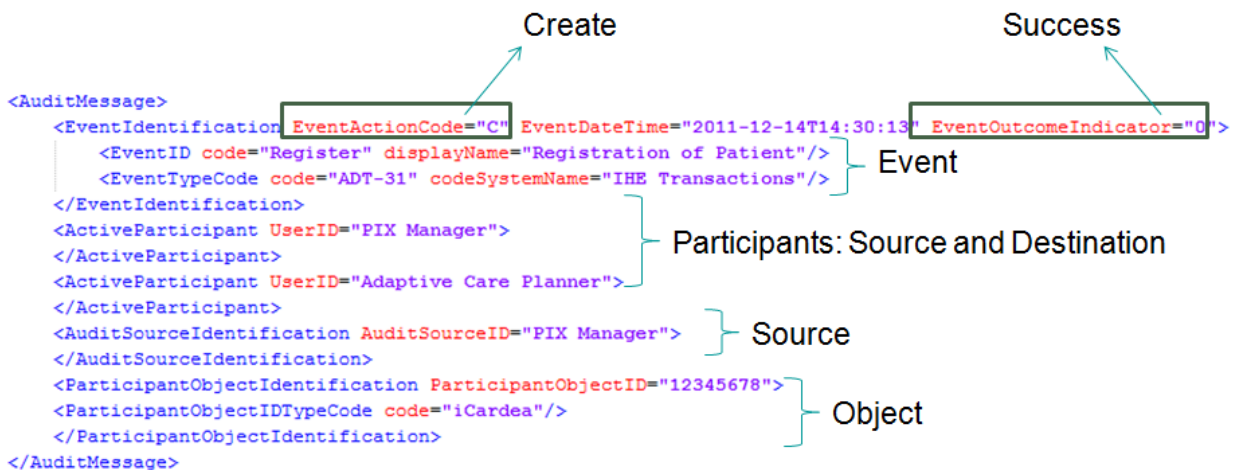


Figure 14: Audit Record Message for HL7v2 ADT^A31 transaction

In Figure 14, the audit record message represents Consent Request between Care Management DB and any resource which user wants to access via Consent Manager. This is read action and this request takes place from Care Management DB to the requested resource.

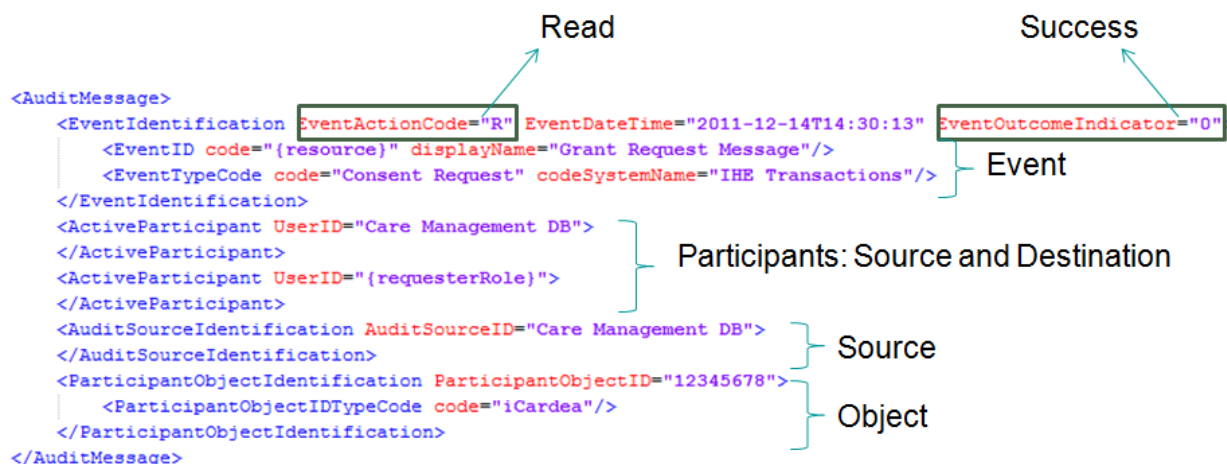


Figure 15: Audit Record Message for Consent Request

In these messages, apart from the Event Identification attributes mentioned above, participants objects as "Source" and "Destination" are defined to know the transaction end-points and as well as Participant Object (in this case, it is the patient iCARDEA ID) which is necessary to audit for which patient this transaction is done.

After preparing suitable Audit Record messages, the transportation of these messages come up. The transport of the transaction of Audit Record messages can be done in 2 ways:

- Syslog Messages (RFC 5424¹³) over TLS (RFC 5425¹⁴)
- Syslog messages (RFC 5424) over UDP (RFC 5426¹⁵)

TLS on top of TCP is reliable and secure but also less efficient. On the other side, UDP is easier (no certificates etc) and faster. Additionally, in the SALK installation where all iCARDEA components are deployed, components communicate over localhost meaning less security threats and big Maximum Transition Units (MTUs), better guarantees for delivery. In iCARDEA Security architecture, UDP is decided to be used for Audit Messages as long as we secure actual messages with TLS while sending them to the end points of the external systems. Therefore, UDP is used for the Care Planner to send Audit messages to Audit Record Repository (ARR) installed in SALK machine.

When the related messages are sent to the Audit Record Repository, these logs can be seen from both ARR server from terminal and simple graphical user interface of ARR running at <http://localhost:8081/atna>. Sample logs can be seen in Figure 16.

¹³ The Syslog Protocol, <http://tools.ietf.org/html/rfc5424>

¹⁴ F. Miao, Y. Ma, J. Salowey, IETF, Transport Layer Security (TLS) Transport Mapping for Syslog, <http://tools.ietf.org/html/rfc5425>

¹⁵ Transmission of Syslog Messages over UDP, <http://tools.ietf.org/html/rfc5426>

OpenATNA Audit Message Viewer

Error Viewer

Constraints

At least one constraint must be specified.
A '' can be used for Ids and Type Codes as a wildcard at the beginning and end of values.*

Event Id Code : Event Type Code : Start Date :

Event Time : Audit Source Id : Start Time : :

Event Outcome : Participant Object Id : End Date :

Event Action : Active Participant Id : End Time : :

Source Type Code : Participant Type Code : Object Type Code :

Source IP :

Event Time	Event Action	Event Outcome	Event ID	
2011-12-19 04:56:03.0	C	0	LABCAT	+
2011-12-19 04:56:27.0	C	0	MEDLIST	+
2011-12-19 04:56:51.0	C	0	MEDCCAT	+
2011-12-19 04:57:14.0	C	0	COBSCAT	+
Event Time	Event Action	Event Outcome	Event ID	

Figure 16: Sample view of Audit Message Viewer

6.2 NODE AUTHENTICATION

For the Node Authentication part of IHE ATNA profile, ITI-19 Node Authentication transaction is used to authenticate services and secure their communication over TLS which meets the requirements of mutual authentication with optional confidentiality protections.

This transaction uses RFC 2246 Transport Layer Security (TLS) 1.0¹⁶ standard for node authentication which includes X.509 certificates for node identity and keys. As noted in Section 3.1.1, these certificates are usually issued by a *certification authority* (CA) and contain identification information, a validity period, a public key, a serial number, and the digital signature of the issuer. In order to achieve this, iCARDEA CA is created as explained in section 4 and in Deliverable 6.5.1. Therefore, Care Planner certificate is signed by this CA which is trusted by all components as the root CA.

For the Care Planner first a new certificate and Certificate Signing Request(CSR) were created by using keytool¹⁷, then iCARDEA CA signed this CSR and this signed certificate was imported to local keystore which contains private keys, and the certificates with their corresponding public keys and CA certificate was imported to the local truststore which contains certificates from other parties that we expect to communicate with, or from Certificate Authorities that we trust to identify other parties.

The self-signed certificate created first and related CSR can be seen in the following format:

¹⁶ The TLS Protocol version 1.0, <http://tools.ietf.org/html/rfc2246>

¹⁷ keytool: Key and Certification Management Tool
<http://docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html>

