

eHealth Framework

How to Comply with ATNA Connection Authentication

Imprint

InterComponentWare AG
Altrottstraße 31
69190 Walldorf
Tel.: +49 (0) 6227 385 0
Fax.: +49 (0) 6227 385 199

© Copyright 2010 InterComponentWare AG. All rights reserved.

Document ID:
Document version: 0.3
Document Language: en (US)
Security Level: Public
Document Status: Approved
Product Name: eHealth Framework
Product Version: 2.9
Last Change: 23.07.2010

Document Version History

| Version | Date | Name | Sections Changed | Change Description |
|---------|------------|------|------------------|--------------------|
| 0.01 | 12.07.2010 | YUD | All | Started content. |
| 0.02 | 22.07.2010 | KKL | All | Functional review. |
| 0.03 | 23.07.2010 | SGR | all | Editorial review. |

Contents

1 Overview..... 1

2 Terminology 2

3 Compliance with ATNA Connection Authentication 4


4 How to Configure eHF-based Applications for ATNA Compliance.....5


1 Overview


Applications based on the eHealth Framework (eHF) interact with the ICW products Master Key Provider and the Terminology Server, to ensure security and semantic interoperability respectively. This document describes how to configure the interactions between them, in order to support ATNA connection authentication. At first, we introduce the relevant terminology from the [Audit Trail and Node Authentication \(ATNA\) Integration Profile](#) of [Integrating the Healthcare Enterprise \(IHE\)](#). Then, we describe the requirements in order to claim for compliance with the ATNA connection authentication. [How to Configure eHF-based Applications for ATNA Compliance](#) on page 5 provides information about configuring eHF-based applications for ATNA compliance.

2 Terminology

This chapter briefly introduces the relevant terminology from IHE, in particular Secure Node, Secure Application, Authentication Node transaction and Connection Authentication.


[Integrating the Healthcare Enterprise \(IHE\)](#)  is an initiative designed to stimulate the integration of the information systems that support modern healthcare institutions. Its fundamental objective is to ensure that in the care of patients all required information for medical decisions is both, correct and available to healthcare professionals. IHE defines a set of technical frameworks for the implementation of established messaging standards (e.g. HL7, DICOM and OASIS) to achieve specific clinical goals.

The [IT Infrastructure Technical Framework](#)  of IHE identifies a subset of the functional components of the healthcare enterprise that produce, manage or act on categories of information, required by operational activities, called IHE *actors*, and specifies their interactions in terms of a set of coordinated, standards-based *transactions*. The transactions are organized into functional units called *integration profiles* that highlight their capacity to address specific IT Infrastructure requirements.

The [Audit Trail and Node Authentication \(ATNA\) Integration Profile](#)  in the IT Infrastructure Technical Framework establishes security measures which, together with the security policy and procedures, provide patient information confidentiality, data integrity and user accountability.

Secure Node and Secure Application

The ATNA profile defines a *Secure Node* actor and a *Secure Application* actor. The characteristics of a secure node are the following:

1. It describes the security environment (user identification, authentication, authorization, access control, etc.) for the node.
2. It defines basic auditing requirements for the node.
3. It defines basic security requirements for the communication of the node using the [Transport Layer Security \(TLS\)](#)  protocol or equivalent functionality.
4. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information.
5. It defines a Secure Application actor for describing product configurations that are *not* able to meet all of the requirements of a Secure Node.

As mentioned in the [IT Infrastructure Technical Framework Volume 1](#)  "The difference between the Secure Node and the Secure Application is the extent to which the underlying operating system and other environment are secured. A Secure Node includes all aspects of user authentication, file system protections, and operating environment security. The Secure Application is a product that does not include the operating environment." The Secure Application provides security features only for the application features.

A web server application consists of an operating system, a web server framework, and individual web applications. Each of these components has a role in performing security related tasks. If an application product claims to be only a secure application actor, the system integrator can determine what additional products or integration work will be needed to establish the functionality provided by a secure node actor.

Authenticate Node Transaction

Transactions are interactions between actors that communicate the required information through standards-based messages. [IT Infrastructure Technical Framework Volume](#)

2 ➤ defines these transactions. The *Record Audit Event*, the *Maintain Time* and the *Authenticate Node* transactions are relevant for the ATNA profile.

For a secure node to claim support of the ATNA integration profile, it is mandatory to perform both, the *Authenticate Node* and the *Maintain Time* transaction, while for a secure application both transactions are optional.

The *Authenticate Node* transaction consists of user authentication and connection authentication:

- *User authentication*: The ATNA profile "requires only local user authentication. The profile allows each secure node to use the access control technology of its choice to authenticate users".
- *Connection authentication*: The ATNA profile "requires the use of bi-directional certificate-based node authentication for connections to and from each node. [...] 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" personal health information.

The connection authentication defines the security requirements for the communications among the secure nodes. It is concerned with the third characteristic of a secure node and this is the focus of this document.

3 Compliance with ATNA Connection Authentication

The ATNA profile mandates the use of the Transport Layer Security (TLS) security negotiation mechanism for all communications between secure nodes. IHE does not mandate the use of encryption during transmission. To allow installation of IHE secure nodes into environments where the network is not otherwise secured, it permits the negotiation of encryption if both nodes are configured to request and support encryption.

If a secure node claims to support the ATNA Connection Authentication, it must fulfill the following requirements:

- *Mutual authentication:* Bi-directional certificate-based node authentication is required.
- *Certificate requirements:* The certificates used for mutual authentication shall be X.509 certificates. "The healthcare enterprise should define the maximum expiration time for certificates in its security policy. The IHE Technical Framework recommends a maximum expiration time of 2 years."
- *Certificate validation:* When authenticating the remote secure node, the local secure node shall be able to perform certificate validation based on either (1) signatures by a trusted CA, or (2) a set of trusted certificates. The local secure node can make the choice of which mode or a mixture of both is used.
- *DICOM and HL7 connections:* All secure nodes shall be configurable for use on a physical secured network or on a not physical secured network.
 - a. On a physical secured network, a non-TLS protocol may be used. DICOM recommends using the port 2762. HL7 does not specify port numbers.
 - b. If the network is not physical secured, TLS shall be used. Either the `TLS_RSA_WITH_NULL_SHA` or the `TLS_RSA_WITH_AES_128_CBC_SHA` ciphersuite shall be supported, depending whether confidentiality is required. DICOM recommends using the port 104. HL7 does not specify port numbers. In general, different ports shall be used for physical secured and not physical secured networks.
- *HTTP connections:*
 - a. HTTP communications shall require the encryption option. The `TLS_RSA_WITH_AES_128_CBC_SHA` ciphersuite shall be supported.
 - b. The port number shall be configurable.

4 How to Configure eHF-based Applications for ATNA Compliance

Applications based on the eHealth Framework (eHF) interact with the ICW products Master Key Provider and the Terminology Server to ensure security with encryption and semantic interoperability respectively. As illustrated in [Figure 1](#) an eHF-based application, the Master Key Provider (MKP) and the Terminology Server (TS) are all web applications which run on a web server framework. In particular, we recommend using an Apache Web Server in front of one or multiple Apache Tomcat Application Servers which host the web application.

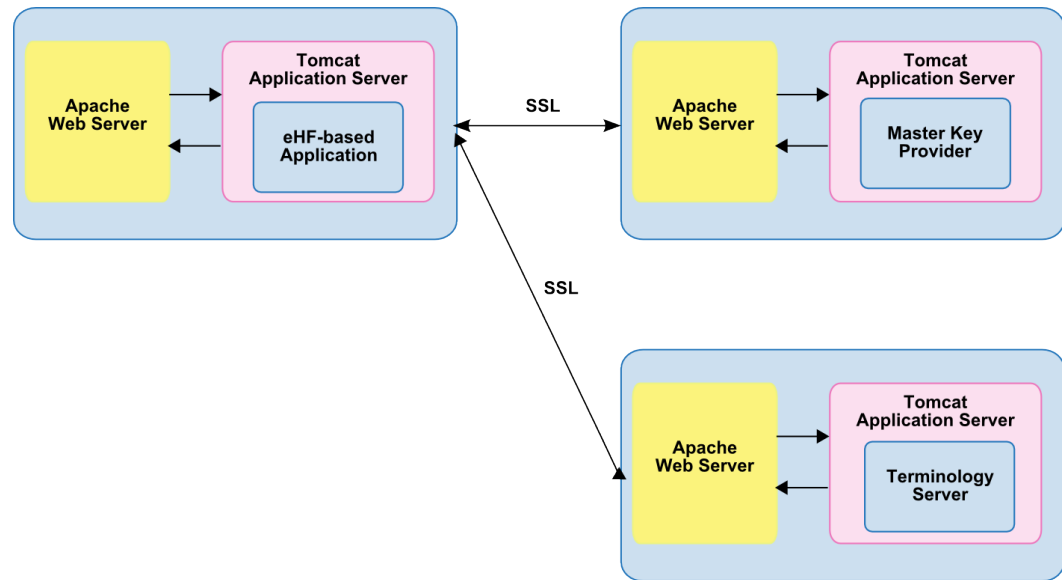


Figure 1: Communications among an eHF-based application, MKP and TS

Both, communications between an eHF-based application and the Master Key Provider and communications between an eHF-based application and the Terminology Server are based on the TLS protocol. During the interactions, the eHF-based application plays the role of a client, while the Master Key Provider and the Terminology Server play the role of a server. To claim for compliance with ATNA connection authentication, both the client and the server must be configured appropriately.

At the server side, the requirements for compliance as defined in [Compliance with ATNA Connection Authentication](#) on page 4 are not concerned with the web application, but rather with certificate handling and configuration of the Apache Web Server and the Apache Tomcat Application Server.

Integrating with the Master Key Provider

At the server side, the Master Key Provider is delivered with a set of basic configurations which are designed for ATNA compliance. Please refer to the installation manual of the Master Key Provider for detailed configuration information.

At the client side, please refer to the chapter "Configuring the Master Key Provider" of "How to configure an Assembly for Encryption" for detailed information.