HITSP Secured Communication Channel Transaction

HITSP/T17

Submitted to:
Healthcare Information Technology Standards Panel

Submitted by:
Security, Privacy and Infrastructure Domain Technical Committee
(Formerly Security and Privacy Technical Committee)
## DOCUMENT CHANGE HISTORY

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Description of Change</th>
<th>Name of Author</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Review Copy</td>
<td>Security and Privacy Technical Committee</td>
<td>July 20, 2007</td>
</tr>
<tr>
<td>1.0.1</td>
<td>Review Copy</td>
<td>Security and Privacy Technical Committee</td>
<td>October 5, 2007</td>
</tr>
<tr>
<td>1.1</td>
<td>Released for Implementation</td>
<td>Security and Privacy Technical Committee</td>
<td>October 15, 2007</td>
</tr>
<tr>
<td></td>
<td>Template Updated to V2.4</td>
<td>Project Team</td>
<td>July 31, 2008</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>August 20, 2008</td>
</tr>
<tr>
<td>1.2</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>August 27, 2008</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>December 10, 2008</td>
</tr>
<tr>
<td>1.3</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>December 18, 2008</td>
</tr>
<tr>
<td></td>
<td>Template V2.5</td>
<td>Project Team</td>
<td>June 30, 2009</td>
</tr>
<tr>
<td>1.3.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>June 30, 2009</td>
</tr>
<tr>
<td>1.4</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>July 8, 2009</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1.0 INTRODUCTION ................................................................................................................................. 5  
1.1 Overview ........................................................................................................................................... 5  
1.2 Copyright Permissions ....................................................................................................................... 5  
1.3 Reference Documents ...................................................................................................................... 5  
1.4 Conformance .................................................................................................................................... 5  
  1.4.1 Conformance Criteria ................................................................................................................. 5  
  1.4.2 Conformance Scoping, Subsetting and Options ........................................................................... 6  
2.0 TRANSACTION DEFINITION ............................................................................................................. 7  
  2.1 Context Overview ............................................................................................................................. 7  
    2.1.1 Transaction Constraints ............................................................................................................. 7  
    2.1.2 Interfaces ................................................................................................................................. 7  
    2.1.3 Interface Interactions ............................................................................................................... 8  
    2.1.4 Pre-conditions ........................................................................................................................... 8  
      2.1.4.1 Process Triggers .................................................................................................................. 9  
    2.1.5 Post-conditions ....................................................................................................................... 9  
      2.1.5.1 Required Outputs .............................................................................................................. 9  
    2.1.6 Data Flows .............................................................................................................................. 9  
  2.2 List of HITSP Constructs ................................................................................................................... 9  
    2.2.1 Construct Dependencies .......................................................................................................... 9  
    2.2.2 Additional Constraints on Required Constructs ..................................................................... 10  
  2.3 Standards ....................................................................................................................................... 10  
    2.3.1 Regulatory Guidance .............................................................................................................. 10  
    2.3.2 Selected Standards .................................................................................................................. 10  
    2.3.3 Informative Reference Standards ......................................................................................... 10  
3.0 APPENDIX ....................................................................................................................................... 11  
4.0 DOCUMENT UPDATES ...................................................................................................................... 12  
  4.1 October 5, 2007 ............................................................................................................................... 12  
  4.2 October 15, 2007 ............................................................................................................................ 12  
  4.3 July 11, 2008 .................................................................................................................................. 12  
  4.4 August 20, 2008 ............................................................................................................................. 12  
  4.5 August 27, 2008 ............................................................................................................................. 12  
  4.6 December 10, 2008 ........................................................................................................................ 12  
  4.7 December 18, 2008 ........................................................................................................................ 12  
  4.8 June 30, 2009 .................................................................................................................................. 12  
  4.9 July 8, 2009 ................................................................................................................................... 13
FIGURES AND TABLES

Figure 2-1 Interface Interactions ................................................................................................................... 8

Table 1-1 Reference Documents .................................................................................................................. 5
Table 2-1 Transaction Constraints ................................................................................................................ 7
Table 2-2 Interfaces ...................................................................................................................................... 7
Table 2-3 Pre-conditions ............................................................................................................................... 8
Table 2-4 Process Triggers ........................................................................................................................... 9
Table 2-5 Post-conditions ............................................................................................................................. 9
Table 2-6 Required Output ............................................................................................................................ 9
Table 2-7 List of HITSP Constructs .............................................................................................................. 9
Table 2-8 Construct Dependencies .............................................................................................................. 9
Table 2-9 Additional Constraints on Required Constructs ................................................................. 10
Table 2-10 Regulatory Guidance ............................................................................................................... 10
Table 2-11 Selected Standards .................................................................................................................... 10
Table 2-12 Informative Reference Standards .......................................................................................... 10
1.0 INTRODUCTION

1.1 OVERVIEW

The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transmissions, and the mutual trust between communicating parties. Its objectives include providing:

- Mutual node authentication to assure each node of the others’ identity
- Transmission integrity to guard against improper information modification or destruction while in transit
- Transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes

This Secured Communication Channel Transaction supports application credentials, machine credentials, and user machines (user nodes). Details of how a user authenticates to a node or application is beyond the scope of this construct.

Practical examples of this Transaction are a secured communication channel between a Personal Health Record (PHR) system and an Electronic Health Record (EHR) system, or between an EHR system and a laboratory.

1.2 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2009 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI’s copyright is clearly noted.

1.3 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material.

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from www.hitsp.org.

<table>
<thead>
<tr>
<th>Reference Document</th>
<th>Document Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HITSP Acronyms List</td>
<td>Lists and defines the acronyms used in this document</td>
</tr>
<tr>
<td>HITSP Glossary</td>
<td>Provides definitions for relevant terms used by HITSP documents</td>
</tr>
<tr>
<td>TN900 - Security and Privacy</td>
<td>TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs</td>
</tr>
</tbody>
</table>

1.4 CONFORMANCE

This section describes the conformance criteria, which are objective statements of requirements that can be used to determine if a specific behavior, function, interface, or code set has been implemented correctly.

1.4.1 CONFORMANCE CRITERIA

In order to claim conformance to this construct specification, an implementation must satisfy all the requirements and mandatory statements listed in this specification, the associated HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected
base and composite standards. A conformant system must also implement all of the required interfaces within the scope, subset or implementation option that is selected from the associated Interoperability Specification.

Claims of conformance may only be made for the overall HITSP Interoperability Specification or Capability with which this construct is associated.

1.4.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification must be implemented in its entirety for an implementation to claim conformance to the specification. HITSP may define the permissibility for interface scoping, subsetting or implementation options by which the specification may be implemented in a limited manner. Such scoping, subsetting and options may extend to associated constructs, such as this construct. This construct must implement all requirements within the selected scope, subset or options as defined in the associated Interoperability Specification to claim conformance.
2.0 TRANSACTION DEFINITION

2.1 CONTEXT OVERVIEW

The scope of the Secured Communication Channel Transaction is limited to a session oriented, synchronous, and point-to-point communication channel. The focus is on the establishment of a secure path through which data can be transmitted, and not on the content of the data being transmitted. In addition, this Transaction does not include local user authentication in its scope.

The following are the requirements derived from the initial Use Cases for this Transaction:

1. Session used to transmit data has mutual authentication of the nodes involved
2. Data are transmitted with confidentiality and transmission integrity

This construct utilizes the Authenticate Node Transaction from the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Audit Trail and Node Authentication (ATNA) Integration Profile (IHE-ITI-TF ATNA), Section 9.1.

2.1.1 TRANSACTION CONSTRAINTS

<table>
<thead>
<tr>
<th>Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only communications requiring the attributes of transmission authenticity, transmission confidentiality, and transmission integrity need to utilize this construct for session oriented, synchronous, and point-to-point communication channels</td>
</tr>
</tbody>
</table>

Consistent with this constraint, those communications that require the attributes of transmission authenticity, confidentiality, and integrity shall either be prohibited, or designed and verified to prevent access to Protected Health Information (PHI) if they are not communicated through connections that provide session oriented, synchronous, and point-to-point communication channels¹.

2.1.2 INTERFACES

All Interfaces for this Transaction are described further in the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework, Volume 2, Section 3.19 (IHE ITI-TF-2).

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Used in Component/Composite Standard</th>
<th>Required = R</th>
<th>Optional = O</th>
<th>Conditional = C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>The originating or terminating point of information or signal flow in a telecommunications network. This interface is equivalent to the Secure Node in the IHE-ITI-TF ATNA Transaction</td>
<td>IHE-ITI-TF ATNA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ When there is a known security mechanism connecting two secured networks (e.g., physical isolation or VPN), this construct may be determined by the local security administrators to be unnecessary. The Node shall be configurable to disable the use of this construct.
2.1.3 INTERFACE INTERACTIONS

Figure 2-1 Interface Interactions

Figure 2-1 illustrates the mutual authentication of nodes producing a secured communication channel. The detailed interface interactions for authentication are deliberately omitted from the diagram and are incorporated by reference through IHE-ITI-TF2, Section 3.19.

The act of node authentication precedes all Transactions for HITSP interoperability constructs that require a secured communication channel. Once the secured communication channel is established, the HITSP Transactions continue inside the channel according to the Interoperability Specification.

2.1.4 PRE-CONDITIONS

Table 2-3 Pre-conditions

<table>
<thead>
<tr>
<th>Pre-condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A policy defining what is to be audited exists</td>
</tr>
<tr>
<td>Audit record repository is active and designated as the destination for recorded audit events</td>
</tr>
<tr>
<td>Audit record source is initialized to the audit policy</td>
</tr>
<tr>
<td>Consistent Time construct is a pre-requisite for this Transaction</td>
</tr>
<tr>
<td>Existence of active and network accessible nodes</td>
</tr>
<tr>
<td>Identities are managed</td>
</tr>
<tr>
<td>Policy defining the protection of the log and audit exists and is being enforced</td>
</tr>
<tr>
<td>There is a mutually agreed upon set of policies and procedures for establishment of mutually acceptable identity credentials</td>
</tr>
</tbody>
</table>
2.1.4.1 PROCESS TRIGGERS

Table 2-4 Process Triggers

<table>
<thead>
<tr>
<th>Process Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Secured Communication Channel Transaction is triggered when a secured information exchange between two nodes is requested. The node interface represented in this Transaction is equivalent to the secure node interface in the IHE-ITI-TF ATNA Transaction. All triggers associated with this Transaction are specified in the IHE-ITI-TF ATNA Transaction.</td>
</tr>
</tbody>
</table>

2.1.5 POST-CONDITIONS

Table 2-5 Post-conditions

<table>
<thead>
<tr>
<th>Post-condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A secured communication channel providing transmission confidentiality, transmission integrity, and session authenticity is established between the two nodes. This secured communication channel will be used for all future secure transmissions between the two nodes.</td>
</tr>
</tbody>
</table>

2.1.5.1 REQUIRED OUTPUTS

Table 2-6 Required Output

<table>
<thead>
<tr>
<th>Required Output</th>
<th>Format/Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable node to record an audit event to indicate successful connection from nodes that are mutually authenticated</td>
<td>See HITSP/T15 - Collect and Communicate Security Audit Trail</td>
</tr>
<tr>
<td>Require node to record an audit event to indicate attempted connections from nodes that are not mutually authenticated</td>
<td>See HITSP/T15 - Collect and Communicate Security Audit Trail</td>
</tr>
</tbody>
</table>

2.1.6 DATA FLOWS

This is an IHE ATNA Node Authentication Transaction, which in turn calls on various standards, such as TLS and RSA certificates. Please refer to IHE-ITI-TF2, Section 3.19 Authenticate Node for details on data flow.

2.2 LIST OF HITSP CONSTRUCTS

Table 2-7 List of HITSP Constructs

<table>
<thead>
<tr>
<th>Construct Name</th>
<th>Description</th>
<th>Event/Action Code</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>HITSP/T15 - Collect and Communicate Security Audit Trail</td>
<td>Provides a means to ensure that security policies are being enforced and that risks are being mitigated</td>
<td>Various (HITSP Use Case dependent)</td>
<td>Identification and management of audit trigger events and audit event outputs</td>
</tr>
</tbody>
</table>

2.2.1 CONSTRUCT DEPENDENCIES

Table 2-8 Construct Dependencies

<table>
<thead>
<tr>
<th>Construct</th>
<th>Depends On (Name of Component that it depends on)</th>
<th>Dependency Type (Pre-condition, post-condition, general)</th>
<th>Purpose (Reason for this dependency)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HITSP/T17 - Secured Communication Channel</td>
<td>HITSP/T15 - Collect and Communicate Security Audit Trail</td>
<td>General</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identification and management of audit trigger events and audit event outputs</td>
</tr>
</tbody>
</table>
2.2.2 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

Table 2-9 Additional Constraints on Required Constructs

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Construct</th>
<th>Constraint</th>
<th>Constraint Type (Pre-condition, post-condition, general)</th>
<th>Purpose (Reason for this constraint)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable constraints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3 STANDARDS

2.3.1 REGULATORY GUIDANCE

Table 2-10 Regulatory Guidance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable regulatory guidance</td>
<td></td>
</tr>
</tbody>
</table>

2.3.2 SELECTED STANDARDS

Table 2-11 Selected Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication</td>
<td>Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially interface specific requirements. The latest version of the IHE Technical Framework is available at <a href="http://www.ihe.net">www.ihe.net</a></td>
</tr>
</tbody>
</table>

2.3.3 INFORMATIVE REFERENCE STANDARDS

Table 2-12 Informative Reference Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable informative reference standards</td>
<td></td>
</tr>
</tbody>
</table>
3.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.
4.0 DOCUMENT UPDATES

The following sections provide the history of all changes made to this document since the last publication.

4.1 OCTOBER 5, 2007

The changes in this cycle address the following comments received during the Public Comment and Inspection Testing period (July 23, 2006 - August 17, 2007):

1205, 1239, 1240, 1261

The full text of the comments along with the Technical Committee’s disposition can be reviewed on the HITSP Public Web Site.

4.2 OCTOBER 15, 2007

Upon approval by the HITSP Panel on October 15, 2007, this document has been moved to Version 1.1. This document is now Released for Implementation.

4.3 JULY 11, 2008

Updated to place standards into 3 categories: Regulatory, Selected, and Informative References. Also provided clarifications for VPN use.

4.4 AUGUST 20, 2008

This document has been modified to reflect the updated HITSP approach to categorizing standards as Regulatory Guidance, Selected Standards, and Informative References.

The following standard was added as selected, as a more specific standard reference to ATNA Profile:

- Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile

4.5 AUGUST 27, 2008

Upon approval by the HITSP Panel on August 27, 2008, this document is now Released for Implementation.

4.6 DECEMBER 10, 2008

This document has been edited to incorporate the updated version of the IHE ATNA standard to IHE ITI-TF Revision 5.0.

Minor editorial changes were made to this document.

4.7 DECEMBER 18, 2008

Upon approval by the HITSP Panel on December 18, 2008, this document is now Released for Implementation.

4.8 JUNE 30, 2009

Minor editorial changes were made to this document. Boilerplate text was removed for simplification. The term "actor" was replaced with "interface".
4.9 JULY 8, 2009

Upon approval by the HITSP Panel on July 8, 2009, this document is now Released for Implementation.