

HITSP Secured Communication Channel Transaction

HITSP/T17



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security and Privacy Technical Committee



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Security and Privacy Technical Committee	July 20, 2007
1.0.1	Review Copy	Security and Privacy Technical Committee	October 5, 2007
1.1	Released for Implementation	Security and Privacy Technical Committee	October 15, 2007



TABLE OF CONTENTS

1.0	INTRODUCTION	5
1.1	Overview	5
1.2	Transaction Construct Roadmap	5
1.3	Copyright Permissions	6
1.4	Reference Documents	6
2.0	TRANSACTION DEFINITION	8
2.1	Context Overview	8
2.1.1	Transaction Constraints	8
2.1.2	Technical Actors	9
2.1.3	Actor Interactions	9
2.1.4	Pre-conditions	10
2.1.4.1	Process Triggers	11
2.1.5	Post-conditions	11
2.1.5.1	Required Outputs	11
2.1.6	Data Flows	12
2.2	List of HITSP Constructs	12
2.2.1	Construct Dependencies	12
2.2.2	Additional Constraints on Required Constructs	12
2.3	List of Standards	13
3.0	TECHNICAL IMPLEMENTATION	14
3.1	Conformance	14
3.1.1	Conformance Criteria	14
3.1.2	Conformance Scoping, Subsetting and Options	14
4.0	APPENDIX	15
5.0	CHANGE HISTORY	16
5.1	October 5, 2007	16
5.2	October 15, 2007	16



FIGURES AND TABLES

Figure 1.2-1 Transaction Construct Roadmap.....	6
Figure 2.1.3-1 Technical Actor Interactions	10
Table 2.1.1-1 Transaction Constraints.....	8
Table 2.1.2-1 Technical Actors	9
Table 2.1.4-1 Pre-conditions	10
Table 2.1.4.1-1 Process Triggers.....	11
Table 2.1.5-1 Post-conditions	11
Table 2.1.5.1-1 Required Output	11
Table 2.2-1 List of HITSP Constructs	12
Table 2.2.1-1 Construct Dependencies	12
Table 2.2.2-1 Additional Constraints on Required Constructs.....	13
Table 2.3-1 List of Standards.....	13



1.0 INTRODUCTION

As an introduction to the HITSP Secured Communication Channel Transaction, this section provides a high level overview of the information sharing scenario enabled by following this specification, provides a document map of the construct relationships for this specification, acknowledges the copyright protections that pertain, and provides links to key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Transaction Definition.

1.1 OVERVIEW

This section describes the contents of this specification and provides a high level definition of this Transaction and background information about the underlying Components that the Transaction is based on.

The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of Transactions, 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; and
- Transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes

This Secured Communications Channel Transaction supports both application and 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.

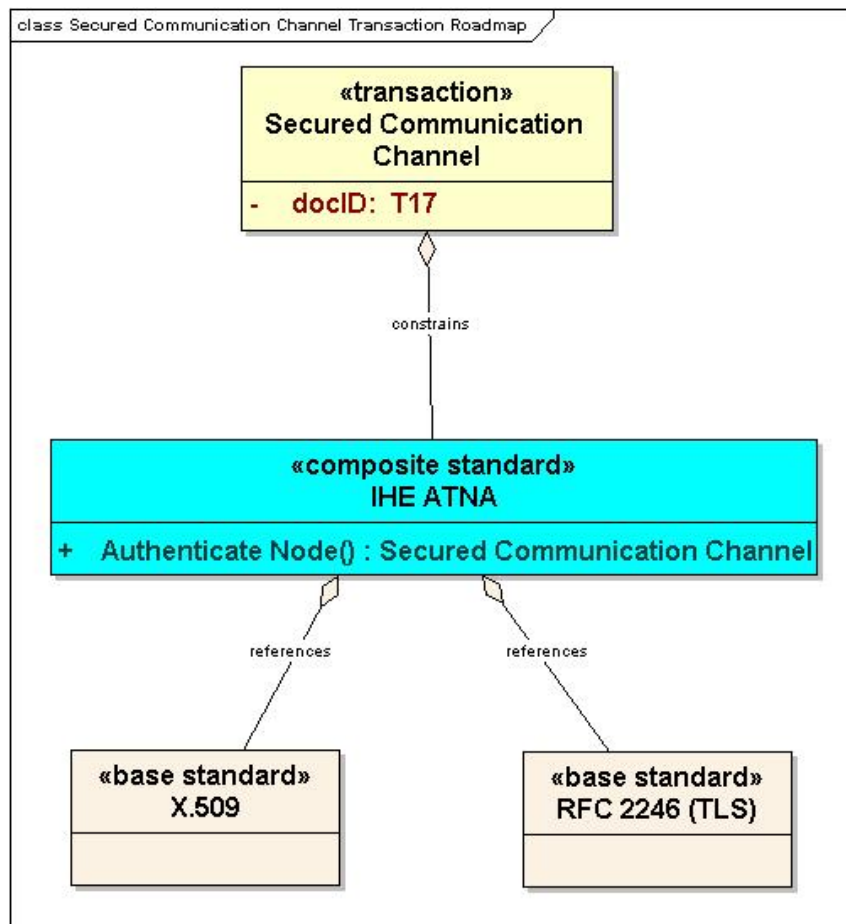
Practical examples of this Transaction are a secured communication channel between a Personal Health Record (PHR) system and an Electronic Health Record (EHR) system, or between an EHR system and a laboratory.

1.2 TRANSACTION CONSTRUCT ROADMAP

Each HITSP specification is comprised of a suite of constructs that, taken as a whole, provide a detailed map to existing standards and specifications that will satisfy the requirements for the HITSP construct. The specification identifies and constrains standards where necessary, and creates groupings of specific actions and actors to further describe the relevant contexts using Transactions and Components depicted in the diagram below. The most effective way to see the construct breakdown for any HITSP specification is to begin with the document indicated at the top of the diagram.



Figure 1.2-1 Transaction Construct Roadmap



1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2007 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.

IHE materials used in this document have been extracted from relevant copyrighted materials with permission of Integrating the Healthcare Enterprise (IHE). Copies of this standard may be retrieved from the IHE Web Site at www.ihe.net.

1.4 REFERENCE DOCUMENTS

This section contains links to key reference documents and background material.

The HITSP Interoperability Specification Overview provides the background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The



document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT product development or product refinement.

The conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications are contained in the HITSP Conventions List.

The acronyms used in this document are contained in the HITSP Acronyms List.

The HITSP Harmonization Framework describes the current framework within which the Interoperability Specifications are built.

A Technical Note, TN900 - Security and Privacy, has been developed as a reference document to provide the overall context for use of the HITSP Security and Privacy constructs. It includes the following:

- The scope, reference policy background, and Security and Privacy principles used in the development of the constructs
- A detailed description and schematics of the conceptual relationship between the Security and Privacy constructs
- A mapping of existing standards and constructs to be used in meeting the stated requirements of the AHIC Use Cases
- A list of identified gaps and the recommended approaches to resolving those gaps
- A roadmap for how the Security and Privacy constructs will evolve and eventually align with other HITSP Interoperability Specifications
- A conceptual framework for Security and Privacy management, including reference information on privacy policies, risk assessment, and risk management
- A glossary of terms used in all the Security and Privacy construct documents
- A description of the application of the Security and Privacy constructs to the HITSP Interoperability Specifications for the three initial AHIC Use Cases – Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment

HITSP will periodically update this Technical Note as required by the introduction of new contexts for use.



2.0 TRANSACTION DEFINITION

Transactions are a logical grouping of actions, including necessary content and context that must all succeed or fail as a group.

2.1 CONTEXT OVERVIEW

This section provides a general description of the Transaction. It includes a detailed definition of the Transaction and the reason for its use. It also provides all the necessary background information that further describes the context in which the Transaction is needed, and the Components or composite standards that the Transaction is based on.

The scope of the Secured Communication Channel Transaction is limited to a session oriented, synchronous, point-to-point communication channel based on the requirements identified in the initial Use Cases. 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 V4.0).

2.1.1 TRANSACTION CONSTRAINTS

This section describes the constraints that limit the context in which the Transaction construct may be used. A constraint describes a rule that limits the use of the actors, actions or data within the given context, or to which the interactions must conform to be used within the described context. It is a description of the limits and scope of the interactions and can describe actions or events that are not part of the initial definition for the context.

Table 2.1.1-1 Transaction Constraints

Constraint
Only communications requiring the attributes of transmission authenticity, transmission confidentiality, and transmission integrity need utilize this construct for session oriented, synchronous, point-to-point communication channels.

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, point-to-point communication channels.

2.1.2 TECHNICAL ACTORS

This section describes the technical actors that need to be integrated in order to meet the interoperability requirements for this Transaction. A Technical Actor represents an entity internal to a software application, which is engaged in one or more specific Transactions to support a specific aspect of a real world information interchange (e.g. set of message exchanges). The table below lists the technical actors involved, the relevant definition of their roles, and an indication of their requirements for the Transaction.

Table 2.1.2-1 Technical Actors

Actor	Description	Used in Component/ Composite Standard	Required = R Optional = O Conditional = C
Node	The originating or terminating point of information or signal flow in a telecommunications network. This actor is equivalent to the <i>Secure Node</i> in the IHE-ITI-TF ATNA Transaction.	IHE-ITI-TF ATNA	R

2.1.3 ACTOR INTERACTIONS

The following sections document the content of the Transaction and the basic process flows that are supported by the Transaction. They describe the underlying events that fulfill the Transaction, the sequence and timing of the events, and the specific actors involved. Process flow diagrams are provided to illustrate the process relationships.



Figure 2.1.3-1 Technical Actor Interactions

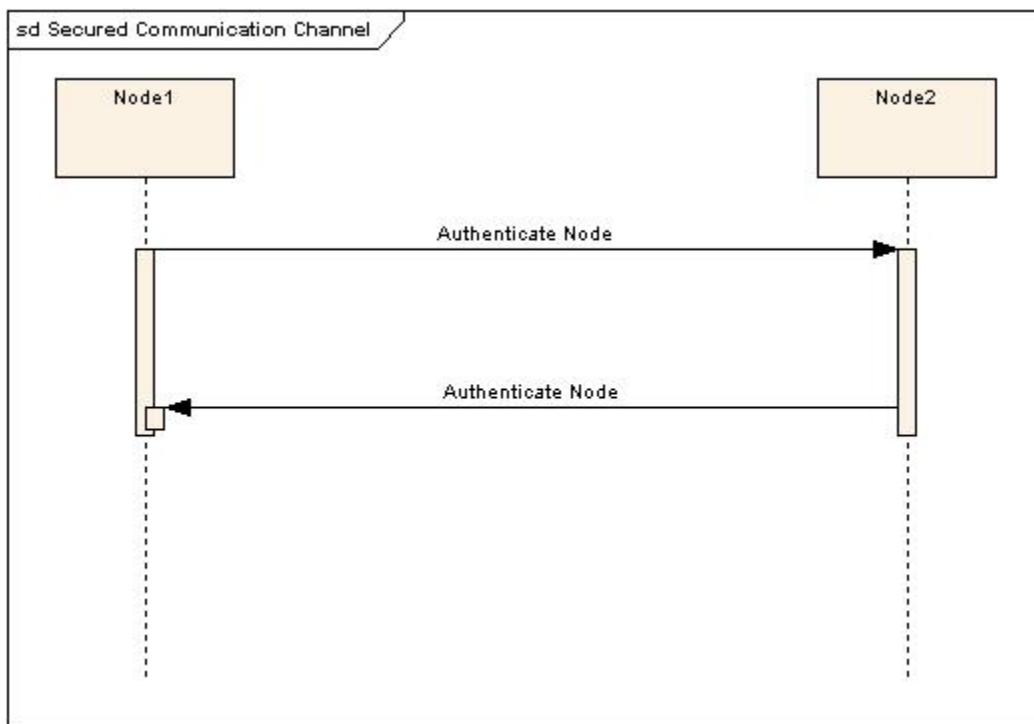


Figure 2.1.3-1 illustrates the mutual authentication of nodes producing a secure communications channel. The detailed actor interactions for authentication are deliberately omitted from the diagram and are incorporated by reference through IHE-ITI-TF ATNA V4.0.

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

This section describes the necessary conditions that must be in place prior to the start of the workings of the Transaction. The pre-conditions are used to convey any conditions that must be true at the outset of a Transaction. They describe the context that must be established before the Transaction is executed. They are not however the triggers that initiate the Transaction. Where one or more pre-conditions are not met, the behavior of the Transaction should be considered uncertain.

Table 2.1.4-1 Pre-conditions

Pre-condition
There is a mutually agreed upon set of policies and procedures for establishment of mutually acceptable identity credentials.
Existence of active and network accessible nodes.
Consistent Time construct is a pre-requisite for this Transaction



Pre-condition
Secure Nodes is a pre-condition to this Transaction
A policy defining what is to be audited exists
Audit record source is initialized to the audit policy
Audit record repository is active and designated as the destination for recorded audit events
Policy defining the protection of the log and audit exists and is being enforced
Identities are managed

2.1.4.1 Process Triggers

This section describes the triggers, including actors and/or processes, which are necessary to start the Transaction. They can invoke an automatic or manual process or result that in turn starts off the Transaction. A trigger is not the same as a pre-condition that describes a context that needs to be in place at the start of the event.

Table 2.1.4.1-1 Process Triggers

Process Trigger
The Secured Communication Channel Transaction is triggered when a secured information exchange between two nodes is requested. The node actor represented in this Transaction is equivalent to the secure node actor in the IHE-ITI-TF ATNA Transaction. All triggers associated with this Transaction are specified in the IHE-ITI-TF ATNA Transaction.

2.1.5 POST-CONDITIONS

This section provides an overview of the conditions or results that must occur at the end of the Transaction in order for the Transaction to be deemed successfully completed. This includes any required outputs from the Transaction, or specific actor states.

Table 2.1.5-1 Post-conditions

Post-condition
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 Transactions between the two nodes.

2.1.5.1 Required Outputs

This section identifies the required outputs that must be produced at the end of the Transaction in order for the Transaction to be deemed successfully completed. This includes the format and usage of the required output.

Table 2.1.5.1-1 Required Output

Required Output	Format/Usage
Require node to record an audit event to indicate attempted connections from nodes that are not mutually authenticated.	See HITSP/T15 - Collect and Communicate Security Audit Trail



Required Output	Format/Usage
Enable node to record an audit event to indicate successful connection from nodes that are mutually authenticated.	See HITSP/T15 - Collect and Communicate Security Audit Trail

2.1.6 DATA FLOWS

This section describes the basic data flows that are supported by this Transaction. It also describes the format of the data, the data sources, and the relevant actors involved in the successful flow of data for the Transaction. Any prevailing pre and post conditions are identified, as well as the purpose of each data post-condition associated with each Transaction. Any data that need to be made available to particular actors are highlighted, as well as the conditions and processes that will use the data to achieve the stated post-conditions.

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-TF ATNA *Authenticate Node Transaction* for details on data flow.

2.2 LIST OF HITSP CONSTRUCTS

The following list of constructs and their definitions are used by the Transaction specification.

Table 2.2-1 List of HITSP Constructs

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

2.2.1 CONSTRUCT DEPENDENCIES

The following table shows a list of Components with their existing dependencies. Dependencies usually exist when there are some additional pre-requisites for a specific construct:

Table 2.2.1-1 Construct Dependencies

Construct	Depends On (Name of Component that it depends on)	Dependency Type (Pre-condition, post-condition, general)	Purpose (Reason for this dependency)
HITSP/T17 - Secured Communication Channel	HITSP/T15 - Collect and Communicate Security Audit Trail	General	Identification and management of audit trigger events and audit event outputs

2.2.2 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

This section describes the constraints that further limit the constructs that are used by this Transaction.



Table 2.2.2-1 Additional Constraints on Required Constructs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, post-condition, general)	Purpose (Reason for this constraint)
No applicable constraints				

2.3 LIST OF STANDARDS

It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts. The following standards are used to implement this Transaction specification:

Table 2.3-1 List of Standards

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement 2004 - 2005 – Audit Trail and Node Authentication Profile (ATNA)	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 actor specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net



3.0 TECHNICAL IMPLEMENTATION

3.1 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.

3.1.1 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 be constrained as specified in table 2.1.1-1, and implement all of the required actors from table 2.1.2-1, 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 with which this construct is associated.

3.1.2 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 actor 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.



4.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.

RELEASED FOR IMPLEMENTATION



5.0 CHANGE HISTORY

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

5.1 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.

5.2 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.

