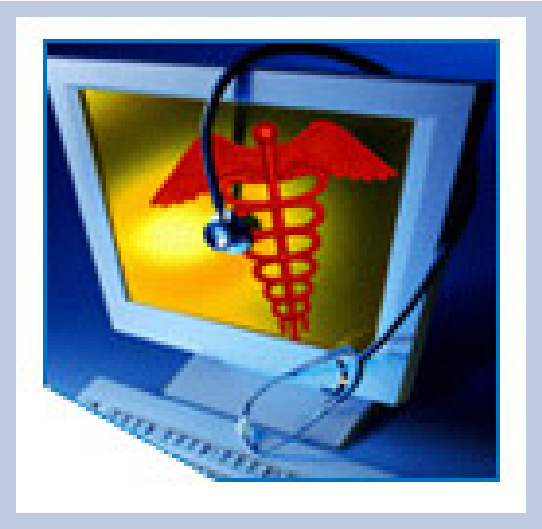
October 15, 2007
Version 1.1

HITSP Nonrepudiation of Origin Component

HITSP/C26



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security and Privacy Technical Committee

RELEASED FOR IMPLEMENTATION

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	Release for Implementation	Security and Privacy Technical Committee	October 15, 2007

RELEASED FOR IMPLEMENTATION

TABLE OF CONTENTS

RELEASED FOR IMPLEMENTATION

FIGURES AND TABLES

RELEASED FOR IMPLEMENTATION

1.0 INTRODUCTION

As an introduction to the HITSP Nonrepudiation of Origin Component, 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; 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 Component Definition.

1.1 OVERVIEW

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

The scope of the Nonrepudiation of Origin Component provides the mechanisms to support Nonrepudiation of Origin, which refers to both the proof of the integrity and origin of documents in a high-assurance manner which can be verified by any party. This Component does not provide Nonrepudiation of Receipt.

According to section 7.3.1.1 of ASTM E1762-95 (2003) Standard Guide for Electronic Authentication of Health Care Information, Nonrepudiation is defined as proof that only the signer could have created a signature. Nonrepudiation cannot be ensured until the completion of the applicable dispute resolution process. This process may be influenced by agreements between the signer and verifier (for example, trading partner agreements or system rules), and such agreements would implicate the appropriate technologies that could be used to provide electronic signatures.

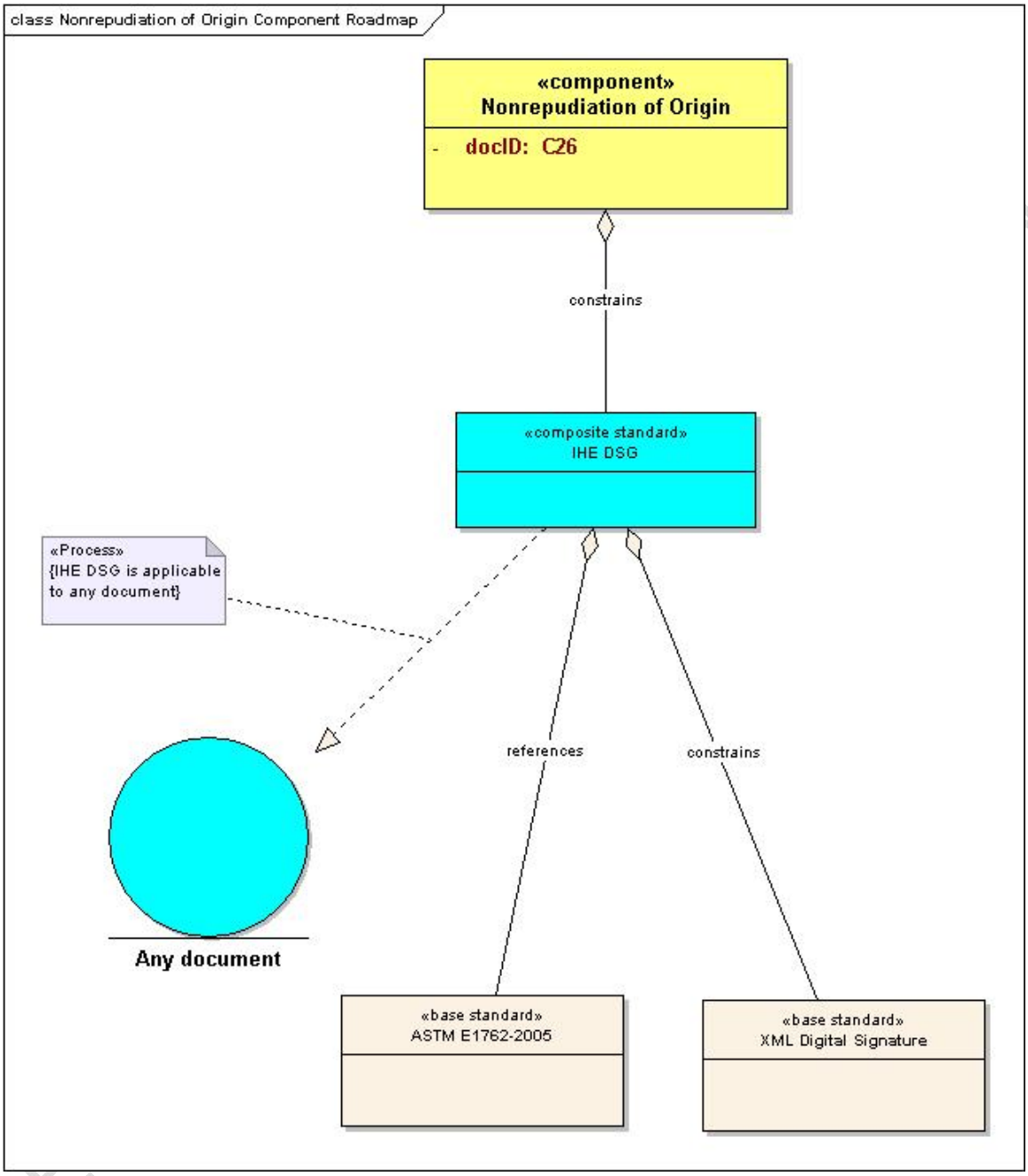
ASTM E1762-95 (2003) also defines three levels of assurance (low, medium, and high) for nonrepudiation. Low and medium levels of assurance do not require the use of digital signatures but may rely on a combination of audit log, integrity control, and access controls. Low and medium levels of assurance can be achieved by using the core set of HITSP security constructs (HITSP/T15 - Collect and Communicate Security Audit Trail, HITSP/T16 - Consistent Time, HITSP/T17 - Secured Communication Channel, and HITSP/TP20 - Access Control).

1.2 COMPONENT 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 Components and standards depicted in the diagram below. The most effective way to review the construct breakdown for any HITSP specification is to begin with the document indicated at the top of the diagram.

RELEASED FOR IMPLEMENTATION

Figure 1.2-1 Component 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.

ASTM International materials used in this document have been extracted, with permission from E2369-05 Standard Specification for Continuity of Care Record (CCR) and E1762-95 (2003) Standard Guide for Electronic Authentication of Health Care Information, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428. Copies of this standard are available through the ASTM Web Site at www.astm.org.

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 IHE 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 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 ONC 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

RELEASED FOR IMPLEMENTATION

- 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.

RELEASED FOR IMPLEMENTATION

2.0 COMPONENT DEFINITION

A Component defines atomic constructs used to support an information exchange or to meet an infrastructure requirement. This is accomplished by:

- Referencing one or more underlying standards
- Specifying constraints and other rules for using the standards

2.1 CONTEXT OVERVIEW

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

The following is the requirement derived from the AHIC Use Case for this Component:

- Authenticity of document integrity and origin is assured

According to the AHIC Use Cases, documents are persistent encapsulations of both data and context which may be authenticated to ensure nonrepudiation. In addition, Nonrepudiation of Origin is only required for some persistent documents. In some cases, only system-level document source entity identity is required, not the identity of a person. To meet the requirements of this construct, IHE XDS is the only document repository infrastructure mechanism used.

This construct enables digital signature validation. However, functions that validate the signature require a Certificate Policy to be in place to provide specific trust for the certification. We expect that future Use Cases may require signature validation functions. This construct will be updated appropriately at that time.

Only the identities of document source entities are known at the time they are created, therefore the HITSP/T17 - Secured Communication Channel construct alone cannot assure persistent data authenticity and integrity for persistent documents. When a persistent document is consumed, possibly multiple times by multiple users, a mechanism is required so each consumer can authenticate the identity and determine the authority of the document source.

This Component therefore employs standards and IHE standards-based Integration Profiles to employ digital certificates to digitally sign documents in a manner that can be subsequently validated.

RELEASED FOR IMPLEMENTATION

The following additional requirements are also derived from the Use Case for message-based transactions:

- Where it is consistent with harmonization, provide support for both messages and documents. For example, depending on specific phases of the workflow, a laboratory result might be exchanged as a message, as a document, or both
- Verify authenticity of laboratory test result file contents
- Verify integrity of test result (file) contents and that the results came from the identified source

The HITSP/T17 - Secured Communication Channel Transaction ensures message authenticity and integrity. Both the source and consumer(s) are known at the time of data transmission. Message data, once consumed, does not require persistence or re-authentication over time.

2.1.1 COMPONENT CONSTRAINTS

This section describes the constraints that limit the context in which the Component 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 Component Constraints

Constraint
Persistent document contained in (e.g. HITSP/TP13) (i.e. XDS, XDM, XDR)
Environment where policies have defined the Public Key Infrastructure (PKI) from which digital signing certificates are obtained

2.1.2 COMPONENT DEPENDENCIES

This section describes any specific mapping criteria for the standards underlying the Component. It elaborates on the relationships between different standards used by this Component, and how they map to each other. Additional required mapping criteria not currently enforced by the underlying standards, and any specific elements that are required for this mapping to succeed.

Table 2.1.2-1 Component Dependencies

Construct	Depends On (Name of construct that it depends on)	Dependency Type (Pre-Condition, Post-Condition, general)	Purpose (Reason for this dependency)
HITSP/C26 - Nonrepudiation of Origin	HITSP/TP13 - Manage Sharing of Documents	General	The signature and the document that was signed are managed in the Document Sharing

RELEASED FOR IMPLEMENTATION

2.2 RULES FOR IMPLEMENTING

The following section documents the content of the Component. It provides the basic elements and secondary standards that are supported by this Component and the constraints that are being placed on those standards. Specifically, it describes the subset or constraints that are required for this Component, and the minimum attributes of the Component as it relates to the base or composite standards on which it is based.

2.2.1 DATA MAPPING

This section describes the specific data elements used by this Component. Due to the potentially large number of data elements in a particular standard, only the fields that HITSP is constraining differently from the standard will be described here.

Table 2.2.1-1 Data Mapping

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/Pre-conditions
No applicable data mappings					

2.2.2 GUIDELINES AND EXAMPLES

This section provides additional guidelines and examples that support the underlying base or composite standards for this Component. It describes how these specifications differ from the underlying standards, and provides guidelines and examples for implementation.

See the following sections for additional information about this Component.

2.2.2.1 Pre-conditions

This section describes the necessary conditions that must be in place prior to the onset of the Component. They describe the context that must be established before the Component is executed. They are not, however, the triggers that initiate the Component. Where one or more Pre-conditions are not met, the behavior of the Component should be considered uncertain.

Table 2.2.2.1-1 Pre-conditions

Pre-conditions
Existence of policy requiring Nonrepudiation
Existence of policy to guide the creation of digital certificates as proof of identity and authority
Possession of digital certificate for signing
Existence of a PKI identity management framework
Vocabulary for the intent or authority for use of a digital signature as defined by policy
Consistent Time construct

RELEASED FOR IMPLEMENTATION

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

2.2.2.1.1 *Process Triggers*

This section describes the process triggers, including actors and/or processes, which are necessary to start the Component. They can invoke an automatic or manual process or result that in turn starts off the Component. A process 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 2.2.2.1.1-1 Process Triggers

Process Triggers
Event requiring document authentication (digital signature) occurs
Event requiring digital signature validation occurs (action currently assigned to Interoperability Specification that requires this)

These events are distinct, as the document consumer is not necessarily known at the time of document creation. One or more consumers may obtain and validate the signature over an arbitrarily long time. This is an asynchronous activity.

2.2.2.2 Post-conditions

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

Table 2.2.2.2-1 Post-conditions

Post-conditions
Existence of digital signature for the subject document
Verified identity and intent/authority of the signer (currently assigned to the construct that requires Nonrepudiation)

2.2.2.2.1 *Required Outputs*

For the Post-conditions specified above, this section further identifies the formats and usages of the required outputs that must be produced at the end of the Component in order for the Component to be deemed successfully completed.

RELEASED FOR IMPLEMENTATION

Table 2.2.2.2.1-1 Required Outputs

Required Output	Format/Usage
Digitally signed documents	Per IHE-ITI-TF3 DSG profile

2.2.2.3 Technical Actors

This section describes the Technical Actors that should be integrated in order to meet the interoperability requirements for this Component. A Technical Actor represents an entity internal to a software application, which is engaged in one or more specific Components 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 roles, and an indication of requirements for the Component.

Table 2.2.2.3-1 Technical Actors

Technical Actors	Description	Used in Component/ Composite Standard	Required = R Optional = O Conditional = C
Document Source	The Document Source Actor is the producer and publisher of documents. It is responsible for sending documents to a Document Repository Actor. It also supplies metadata to the Document Repository Actor for subsequent registration of the documents with the Document Registry Actor	IHE-ITI-TF3 DSG	R
Document Consumer	The Document Consumer Actor queries a Document Registry Actor for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors	IHE-ITI-TF3 DSG	R

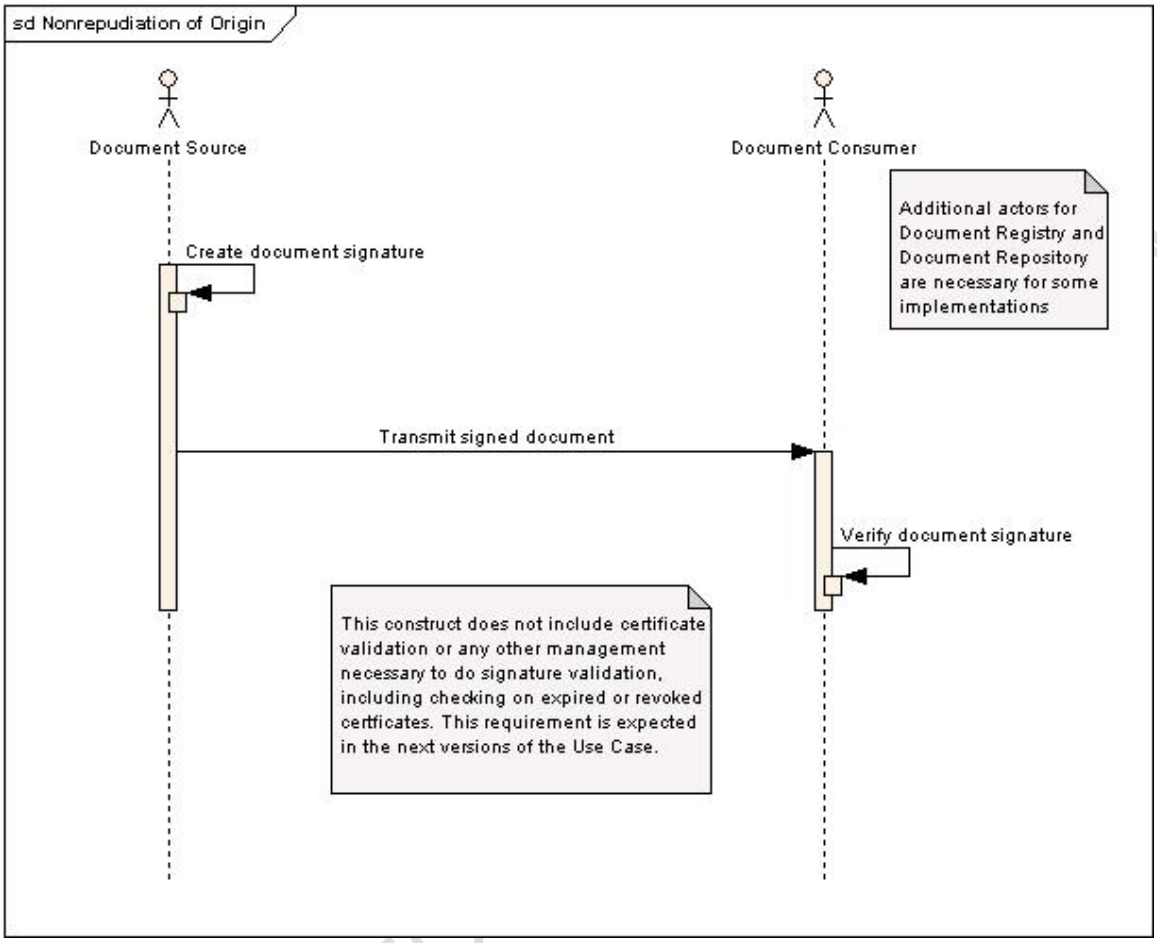
Based on implementation policies not in this Component's scope, it is possible for the document source and consumer to be human entities or automated devices.

2.2.2.4 Actor Interactions

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

RELEASED FOR IMPLEMENTATION

Figure 2.2.2.4-1 Nonrepudiation Actor Interactions



The Document Source creates a digital signature for a document according to the IHE DSG profile specification, causing a detached XML signature for the subject document to be stored in the document repository. When the Document Consumer retrieves the subject document, it also retrieves the XML signature and performs signature verification.

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 Component specification:

RELEASED FOR

Table 2.3-1 List of Standards

Standard	Description
American Society for Testing and Materials (ASTM) Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	Defines a document structure for use by electronic signature mechanisms, describes the characteristics of an electronic signature process. Defines minimum requirements for different electronic signature mechanisms. Defines signature attributes for use with electronic signature mechanisms, describes acceptable electronic signature mechanisms and technologies. Defines minimum requirements for user identification, access control, and other security requirements for electronic signatures, and outlines technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism. Visit www.astm.org for more information
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	Specifies the use of digital signatures for documents that are shared between organizations. The latest version of the IHE Technical Framework is available at www.ihe.net

RELEASED FOR IMPLEMENTATION

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, where defined, 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.

RELEASED FOR IMPLEMENTATION

4.0 APPENDIX

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):

852, 854, 855, 856, 857, 1206, 1208, 1209, 1241

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.

RELEASED FOR IMPLEMENTATION