**July 8, 2009**
**Version 1.4**

# HITSP Nonrepudiation of Origin Component

## HITSP/C26


*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

| 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 |
| 1.1.1 | Review Copy | Security, Privacy and Infrastructure Domain Technical Committee | August 20, 2008 |
| 1.2 | Released for Implementation | Security, Privacy and Infrastructure Domain Technical Committee | August 27, 2008 |
| | Template Updated to V2.4 | Project Team | July 31, 2008 |
| 1.2.1 | Review Copy | Security, Privacy and Infrastructure Domain Technical Committee | December 10, 2008 |
| 1.3 | Released for Implementation | Security, Privacy and Infrastructure Domain Technical Committee | December 18, 2008 |
| | Template V2.5 | Project Team | June 30, 2009 |
| 1.3.1 | Review Copy | Security, Privacy and Infrastructure Domain Technical Committee | June 30, 2009 |
| 1.4 | Released for Implementation | Security, Privacy and Infrastructure Domain Technical Committee | July 8, 2009 |

# TABLE OF CONTENTS

# FIGURES AND TABLES

# 1.0 INTRODUCTION

## 1.1 OVERVIEW

The scope of the HITSP/C26 Nonrepudiation of Origin 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 COPYRIGHT PERMISSIONS



## 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 1-1 Reference Documents**

| Reference Document | Document Description |
|---|---|
| HITSP Acronyms List | Lists and defines the acronyms used in this document |
| HITSP Glossary | Provides definitions for relevant terms used by HITSP documents |
| TN900 - Security and Privacy | TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs |

## 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 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.

# 2.0 COMPONENT DEFINITION

## 2.1 CONTEXT OVERVIEW

The following is the requirement derived from the American Health Information Community (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, HITSP/C26 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. This construct relates to patient identifiable documents and will be transported using the HITSP constructs for sharing of documents (HITSP/TP13 Manage Sharing of Documents, HITSP/T31 Document Reliable Interchange, or HITSP/T33 Transfer of Documents on Media).

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. The HITSP/T64 Identify Communications Recipients construct is one possibility for managing these identities.

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 selects the Integrating the Healthcare Enterprise (IHE) IT Infrastructure (ITI) Technical Framework (TF) – Document Digital Signature (DSG) Content Profile to employ digital certificates to digitally sign documents in a manner that can be subsequently validated.

The HITSP/T17 Secured Communication Channel 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

**Table 2-1 Component Constraints**

| Constraint | Constraint Section |
|---|---|
| Persistent document contained in HITSP/TP13 Manage Sharing of Documents, HITSP/T31-Document Reliable Interchange, or HITSP/T33 Transfer of Documents on Media | |
| Environment where policies have defined the Public Key Infrastructure (PKI) from which digital signing certificates are obtained | |

### 2.1.2 COMPONENT DEPENDENCIES

**Table 2-2 Component Dependencies**

| Standard/HITSP Component | Depends On (Name of standard/HITSP Component 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 |
| HITSP/C26 Nonrepudiation of Origin | HITSP/T31 Document Reliable Interchange | General | The signature and the document that was signed are managed in the Document Sharing |
| HITSP/C26 Nonrepudiation of Origin | HITSP/T33 Transfer of Documents on Media | General | The signature and the document that was signed are managed in the Document Sharing |

## 2.2 RULES FOR IMPLEMENTING

The rules for implementing this construct are wholly contained in the Integrating the Healthcare Enterprise (IHE) IT Infrastructure (ITI) Technical Framework (TF) – Document Digital Signature (DSG) Supplement.

### 2.2.1 DATA MAPPING

**Table 2-3 Data Mapping**

| Data Element | Description | Limit/Range of values | Data Source | Destination | Requirements/ Pre-conditions | Additional Specification for Component |
|---|---|---|---|---|---|---|
| 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 2-4 Pre-conditions**

| Pre-conditions |
|---|
| Existence of policy requiring Nonrepudiation of Origin |
| Existence of policy to guide the creation of digital certificates as proof of identity and authority |
| Possession of keys 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 |
| 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 |

## 2.3 STANDARDS

### 2.3.1 REGULATORY GUIDANCE

**Table 2-5 Regulatory Guidance**

| Standard | Description |
|---|---|
| No applicable regulatory guidance | |

### 2.3.2 SELECTED STANDARDS

**Table 2-6 Selected 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. For more information visit www.astm.org |
| European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES) | Extends the IETF/W3CXML-Signature Syntax and Processing specification [XMLDSIG] into the domain of nonrepudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European Directive. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature. An advanced electronic signature aligned with this document can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later. For more information visit www.etsi.org |
| Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile | Specifies the use of digital signatures for documents that are shared between organizations. For more information visit www.ihe.net |

### 2.3.3 INFORMATIVE REFERENCE STANDARDS

**Table 2-7 Informative Reference Standards**

| Standard Name | Description |
|---|---|
| No applicable informative reference standards | |

# 3.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.

# 4.0 CHANGE HISTORY

The following sections provide the history of changes made to this document.

## 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):

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

## 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 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. As such, the following specific updates were made.

Standards discussed in the narrative were added to tables:

- European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)

## 4.4 AUGUST 27, 2008

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

## 4.5 DECEMBER 10, 2008

This document is being edited to account for minor updates in underlying standard which was republished in October, 2008. Also, extraneous sections were removed that were not adding additional value, since this is defined as a Component, not a Transaction.

Minor editorial changes were made to this document.

## 4.6 DECEMBER 18, 2008

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

## 4.7 JUNE 30, 2009

Minor editorial changes were made to this document. Removed boilerplate text for simplification. The term “actor” was replaced with “interface”.

## 4.8 JULY 8, 2009

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