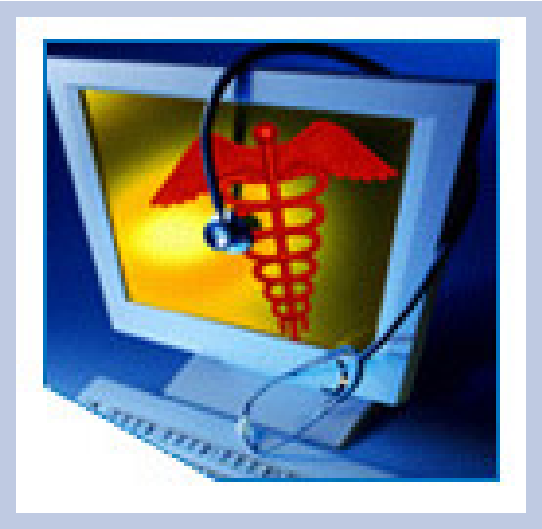
October 15, 2007
Version 1.1

HITSP Entity Identity Assertion Component

HITSP/C19



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

FIGURES AND TABLES

1.0 INTRODUCTION

As an introduction to the HITSP Entity Identity Assertion 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 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 Component Definition.

1.1 OVERVIEW

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

The Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this Component is the validation and assertion of a consumer logging on to a Personal Health Record (PHR) system.

The meaning of the Entity Identity Assertion Component will vary depending on the perspective taken by the implementer of HITSP constructs. The scope of this Component is limited by the context of AHIC Use Cases to the servicing of requests by a service provider from a service user (which can be defined as any of the business actors currently identified within HITSP Interoperability Specifications). The Component is designed to work in conjunction with the collection of an audit trail (as defined in HITSP/T15 - Collect and Communicate Security Audit Trail) and with the maintenance of consistent time (as defined in HITSP/T16 - Consistent Time).

The scope of this Component represented by all scenarios in which HITSP constructs interact across enterprise boundaries, as well as interactions that may occur within an enterprise, i.e., the assertion mechanism is the same whether the Use Case scenarios are within an enterprise or across enterprises. The scope of this Component is also limited to how to correctly assert the identity of a service user to a service provider.

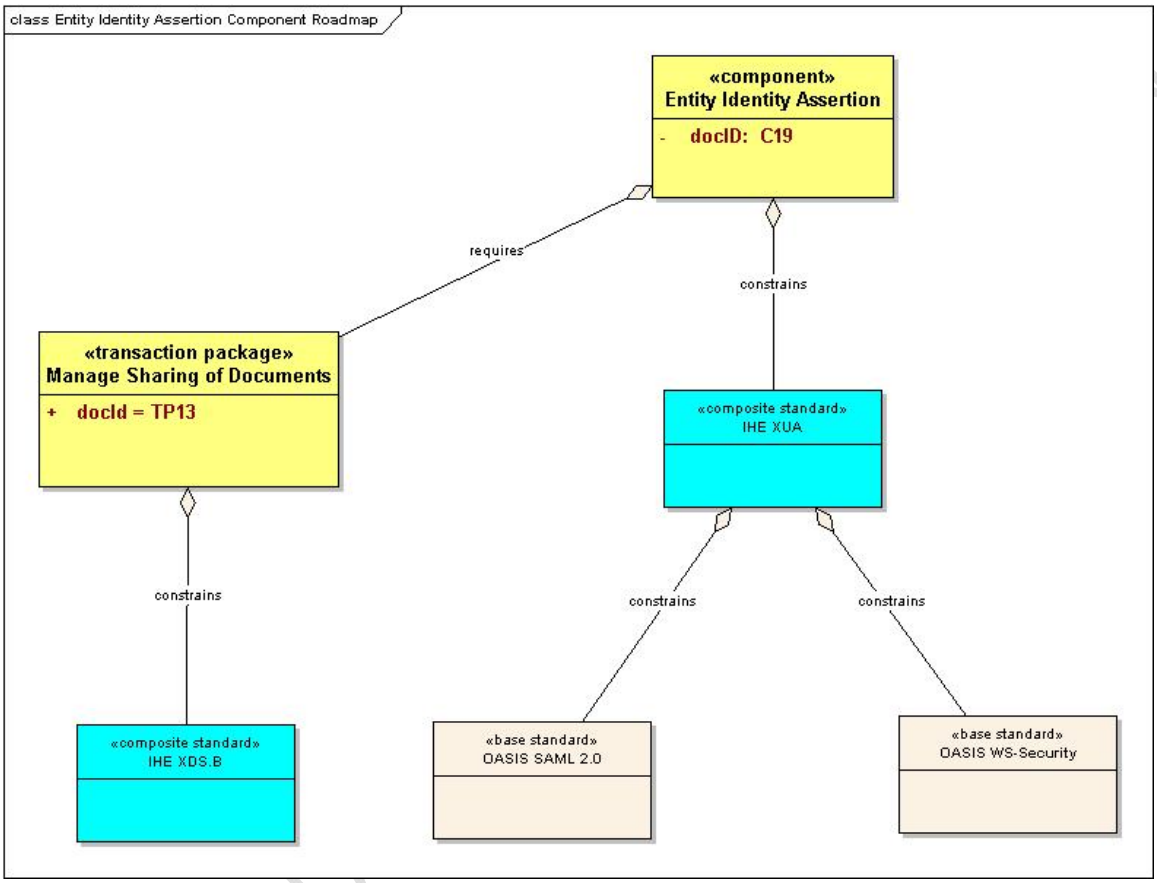
The specific perspective chosen for this Component is to leverage the IHE Cross-Enterprise User Authentication (XUA) Supplement to the IHE-ITI-TF-2. The technological mechanism that this IHE profile relies on is Security Assertion Markup Language (SAML) assertions. This Component also provides support for evolving and ongoing work to support web services through constraining the Web Service-Security standards.

1.2 COMPONENT CONSTRUCT ROADMAP

Each HITSP Interoperability 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 roadmap 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.

Figure 1.2-1 Component Construct Roadmap



1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

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.

OASIS materials used in this document have been extracted from relevant copyrighted materials with permission of the Organization for the Advancement of Structured Information Standards (OASIS). Copies of this standard are available from OASIS at www.oasis-open.org.

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 COMPONENT DEFINITION

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

(a) Referencing one or more underlying standards
(b) 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.

HITSP defines Interoperability Specifications that specify a set of transactions, the content, and the representation of the content for the exchange of information within a defined context between a service consumer and a service provider. This loose coupling is one of the concepts behind a Services Oriented Architecture (SOA). In this type of architecture there is a need for the service provider to be able to obtain a trustable identity of the user that has initiated or triggered the transaction. This method of defining a set of claims about an identity is an *assertion*. In many of the HITSP transactions there is no direct user and the action is undertaken by an automated process. For this reason, this construct identifies the roles and behaviors of an entity. The service provider may be part of a different security domain, and thus not directly under the same security controls that have defined the method used to authenticate a human user. This user authentication and all of the identity management (provisioning, role engineering, attribute management, etc) are orthogonal to the assertion, although critical to its makeup.

This Component focuses on the concept of an assertion service participating in a transaction as the Service Provider actor. This service supports a variety of authentication mechanisms, and is the means by which other actors within HITSP Interoperability Specifications obtain an identity assertion.

The following are the requirements derived from the AHIC Use Cases for the authentication and assertion of users:

1. Entities are asserted to assure that the entity is the person or application that claims the identity.

In addition, the Entity Identity Assertion Component is meant to apply to the following scenarios as defined in the HITSP Interoperability Specifications:

2. User using a Document Registry or Document Repository where the Service Provider wants a user identity for additional detail in their audit log.

3. User using a Document Registry or Document Repository where the Service Provider wants to be assured that the user has been authenticated to a specific assurance level.

4. User using a Document Registry or Document Repository where the Service Provider wants to impose additional access controls.

5. User using a Document Registry or Document Repository is the consumer. The consumer is using an authorized PHR service which is handling the Document Consumer responsibilities. The Service Provider wants to restrict the information returned to those that have been released for consumer consumption (for example a lab result that regulations require the provider to discuss in person before releasing the information).

2.1.1 COMPONENT CONSTRAINTS

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

Component Constraint
Construct is constrained to HITSP interactions that require that a user identity is conveyed

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, are also provided.

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/C19 - Entity Identity Assertion	HITSP/TP13 - Manage Sharing of Documents (provisional on its update to use XDS.b)	General	This construct utilizes IHE XUA and specifies the use of SAML 2.0 assertions, both which require the adoption of IHE XDS.b.

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.

For the purposes of this Component, pre- and post- conditions, as well as triggers and outputs, are also identified. A UML sequence diagram is provided to show the high-level outline of how the Component works.

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 pre-conditions that must be in place prior to the onset of the workings of the Component. The pre-conditions are used to convey any conditions that must be true at the outset of a 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-condition
Entities must have been identified and provisioned (credentials issued, privileges assigned)
Audit services are initialized as outlined in the HITSP/T15 - Collect and Communicate Security Audit Trail Transaction

Pre-condition
Secure channels are initialized in accordance with HITSP/T17 - Secured Communication Channel Transaction
All actors are synchronized to a consistent time base by the HITSP/T16 - Consistent Time Transaction

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 Trigger
Entity successfully connects to a local authentication mechanism and provides identity credentials and authentication information

2.2.2.2 Post-conditions

This section provides an overview of the post-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-condition
Entity has authenticated
An error condition occurs. This can include errors in the verification step – malformed assertion; assertion from a distrusted identity provider; assertion from individual without enough information to perform verification; or identity provider is unknown.
Entity identity assertion is verified

The following post-conditions are noted:

1. There may be an additional post-condition of the assertion being reformulated for application-specific usage. This is outside the scope of this Component as it is an implementation-specific detail.

2. There may be an additional post-condition of conveying authentication and/or assertion information. This is outside the scope of this Component as it is an implementation-specific detail.

2.2.2.2.1 Required Outputs

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

Table 2.2.2.2.1-1 Required Outputs

Required Output	Format/Usage
The results of the assertion are made available to the assertion provider	SAML assertion
A security audit event is generated	a specific audit event will be generated specific to the vocabulary required to generate that event
Authentication information that was verified is available	Standards for minimum core set of required data are specific to a domain or organization

In subsequent iterations of this Component, the HITSP Security and Privacy Technical Committee will define in more detail what specific data are available from this Component. This will include the definition of a minimum data set which needs to be recognized as the minimum data set for assertions.

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 interactions 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 Component.

Table 2.2.2.3-1 Technical Actors

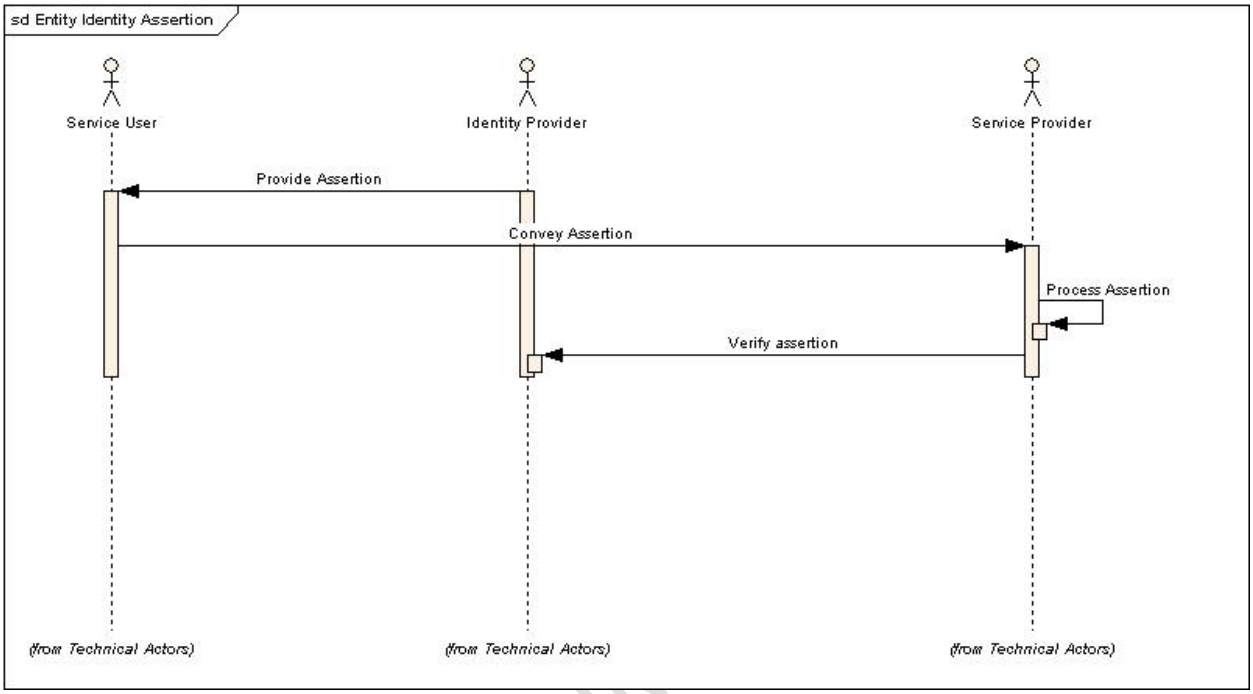
Technical Actor	Description	Used in Component/ Composite Standard	Required = R Optional = O Conditional = C
Service User	The entity represents any individual entity (such as a clinician or a EHR/PHR system) that needs to make a service request of a Service Provider. The Entity may also be known as a principal and/or entity, which represents an end user, an application, a machine, or any other type of entity that may act as a requester in a transaction. A principal is typically represented in a transaction with a digital identity and the principal may have multiple valid digital identities to use with different transaction.	IHE-ITI-TF-2 XUA	R
Identity Provider	The identity provider receives the credentials and identifier from the Entity (principal). It may perform authentication at that point or may require additional authentication from another source (the Service Provider).	IHE-ITI-TF-2 XUA	R
Service Provider	The service provider represents the system providing a service to all entities that need an assertion or authentication. The service (or assertion) provider is the trusted third party issuer of the trustable identity assertion.	IHE-ITI-TF-2 XUA	R

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. It describes 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.

Figure 2.2.2.4-1 Entity Identity Assertion Sequence Diagram



This process flow focuses on the provision of a SAML Identity Assertion, which represents a set of claims about an authenticated principal (entity, application, system...) that is issued either by an Assertion Provider (represented in the above diagram as the Identity Provider technical actor) or by a service provider (defined in this diagram as the Service Provider Technical Actor).

Within the Entity Identity Assertion process flow, the Service User (defined as an entity or principal) is asserted by an Identity Provider, which provides an assertion as outlined in the “Provide Assertion” interaction. The “Provide Assertion” interaction outlines how this Component provides a trustable user assertion from the Identity Provider to the Service User.

The Service User (representative of an entity or principal) then communicates with a Service Provider (defined in this diagram as the Service Provider Technical Actor), conveying their identifier and authenticating assertions (represented in a SAML assertion). This is represented in the “Convey Assertion” interaction.

A Service User may invoke this Component by making a request to another entity within a HITSP Interoperability Specification, such as a laboratory or public health agency, which represents the trigger for the presentation of credentials for SAML assertion. Receipt of this assertion is the trigger for a

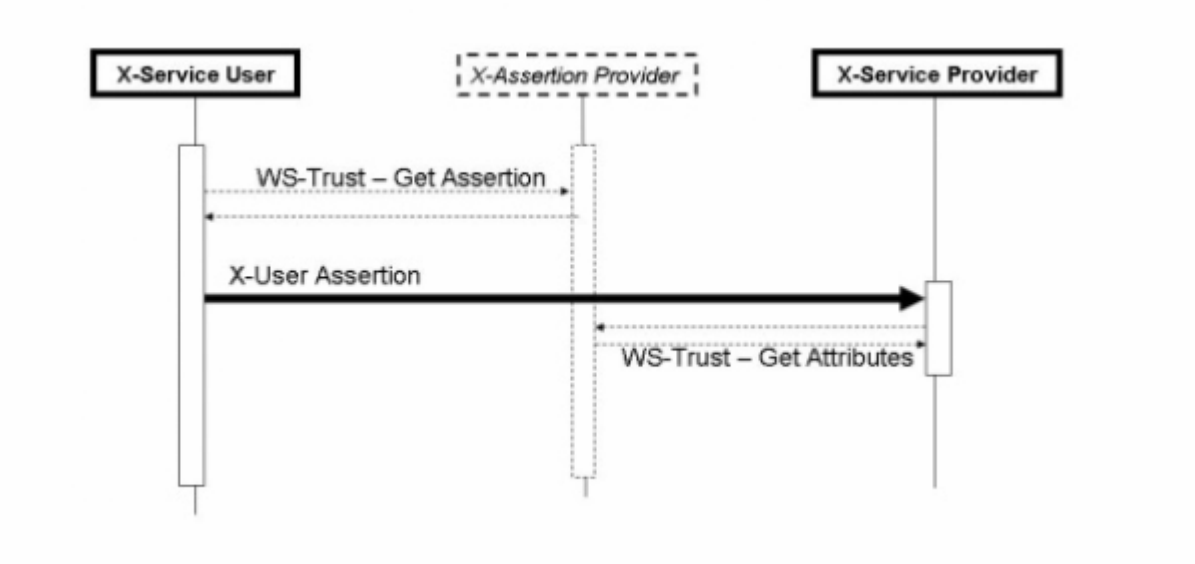
possible additional scenario; the processing and verification of the assertion (captured in the Process Assertion and Verify Assertion interactions).

This Component, when completed, will constitute an auditable event. This Component does not specify how to reference the Identity Assertion in an audit message. This Component is designed to be agnostic to the mechanisms that provide the specific auditing event.

2.2.2.5 Web Services Flows

For authentications made through user assertion using Web Services, the following data flow applies (from the IHE Cross-Enterprise User Authentication (XUA) Supplement to the IHE-ITI-TF-2):

Figure 2.2.2.5-1 WS-Security Assertion Sequence Diagram



This is added as reference material for those implementations that are specific to Web Services. The same interactions related to assertion in section 2.2.2.2 will apply.

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:

Table 2.3-1 List of Standards

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 3.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev.3.0 for Final Text, specifies the IHE transactions defined and implemented as of December 9, 2006. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross Enterprise User Assertion (XUA)	The Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate claims about the user identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries. To provide accountability in these cross enterprise transactions there is a need to identify the requesting user in a way that the receiver can make access decisions and proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the entities, and others that may have chosen to use a third party to perform the authentication. The latest version of the IHE framework is available at www.ihe.net
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 OASIS Standard; ITU-T X.1141	SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. Visit www.oasis-open.org for more information
Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security SOAP Message Security Version 1.0	Describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e.. support multiple security token formats. Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message. Visit www.oasis-open.org for more information.
Organization for the Advancement of Structured Information Standards (OASIS) Simple Object Access Protocol (SOAP) Version 1.1	SOAP is a protocol specification for invoking methods on servers, services, components and objects. SOAP codifies the existing practice of using XML and HTTP as a method invocation mechanism. The SOAP specification mandates a small number of HTTP headers that facilitate firewall/proxy filtering plus an XML vocabulary that is used for representing method parameters, return values, and exceptions. {DevelopMentor} SOAP consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. Visit www.oasis-open.org for more information

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.

4.0 APPENDIX

No additional information at this time.

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):

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.