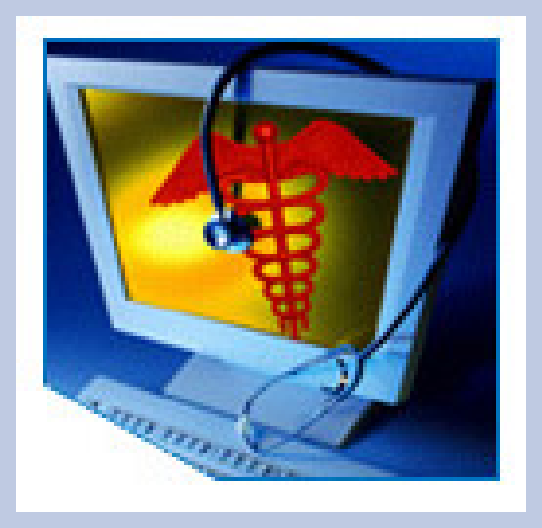
May 16, 2008
Version 2.1

HITSP Secure Web Connection Component

HITSP/C44



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Provider Perspective Technical Committee
(Formerly Care Delivery Technical Committee)

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Final Draft	Electronic Health Record Technical Committee	August 18, 2006
1.1	Ready for Public Comment	Electronic Health Record Technical Committee	September 12, 2006
1.2	Ready for Implementation Testing	Electronic Health Record Technical Committee	October 20, 2006
1.3	Review Copy	Care Delivery Technical Committee	April 27, 2007
2.0	Released for Implementation	Care Delivery Technical Committee	May 11, 2007
2.0.1	Review Copy	Provider Perspective Technical Committee	May 8, 2008
2.1	Released for Implementation	Provider Perspective Technical Committee	May 16, 2008

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

As an introduction to the HITSP Secure Web Connection 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 a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Component Definition.

1.1 OVERVIEW

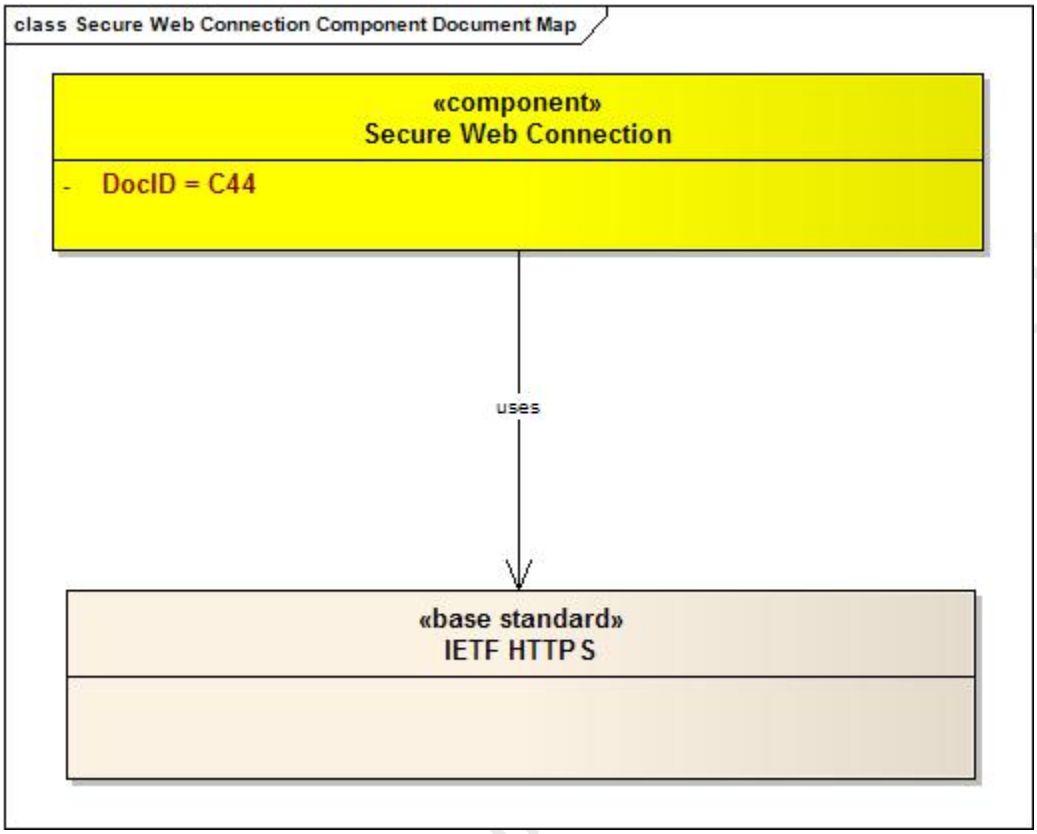
This section describes the contents of this specification and provides a high level definition of this Component and background information about the underlying standards that the Component is based on.

This Component provides the capability to access documents through a secure web browser. Hypertext Transfer Protocol Secure (HTTPS) is a Uniform Resource Identifier (URI) scheme which is syntactically identical to the http: scheme normally used for accessing resources using Hypertext Transfer Protocol (HTTP). Using an https: Uniform Resource Locator (URL) indicates that HTTP is to be used, but with a different default port and an additional encryption/authentication layer between HTTP and Transmission Control Protocol (TCP). This system was developed by Netscape Communications Corporation to provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication, such as payment transactions.

1.2 COMPONENT DOCUMENT MAP

Each HITSP Interoperability Specification (IS) is comprised of a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications that will satisfy the requirements imposed by a given Use Case. The IS groups specific actions and actors to describe the relevant contexts using HITSP constructs that further identify and constrain standards where necessary. There are four types of HITSP constructs called Interoperability Specifications (IS), Transaction Packages (TP), Transactions (T), and Components (C). The current Secure Web Connection Component specification is used with other constructs to meet the requirements of one or more ISs. Review Section 1.2 (Interoperability Specification Document Map) from the relevant IS to better understand the context, dependencies, and relationships between the constructs that are used to meet the IS requirements. The document map in Figure 1.2-1 depicts primary standards that are selected, constrained, or referenced to define the atomic constructs used in an information exchange, or to meet an infrastructure requirement. Implementers should read the documents that describe the standards represented in the diagram for their details and specific uses.

Figure 1.2-1 Component Document Map



1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

1.4 REFERENCE DOCUMENTS

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

Table 1.4-1 Reference Documents

Reference Document	Document Description
HITSP Interoperability Specification Overview	Provides 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.

Reference Document	Document Description
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications.
HITSP Acronyms List	Lists and defines the acronyms used in this document.
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents.
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built.
TN900 - Security and Privacy Technical Note	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 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.

This HITSP Component provides the capability to access documents through a Secure Web Browser. Hypertext Transfer Protocol Secure (HTTPS) is a Uniform Resource Identifier (URI) scheme which is syntactically identical to the http: scheme normally used for accessing resources with Hypertext Transfer Protocol (HTTP). Using an https: Uniform Resource Locator (URL) indicates that HTTP is to be used, but with a different default port and an additional encryption/authentication layer between HTTP and the Transmission Control Protocol (TCP). This system was developed by Netscape Communications Corporation to provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication, such as payment transactions.

The context for the Secure Web Connection has the premise that a system needs to establish a secure communication session with another system across a potentially insecure network. Before exchanging any messages, the sending system must verify the identity of the other system, and the two systems must agree on cryptographic protocols to both initiate the session and to encrypt data during the session to prevent eavesdropping, and to exchange information in a manner that prevents tampering and message forgery.

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	Constraint Section
The level of https protection depends on the correctness of the implementation by the web browser and the server software and the actual cryptographic algorithms supported	N/A
Because SSL operates below http and has no knowledge of the higher level protocol, SSL servers can only present one certificate for a particular Internet Protocol (IP) port combination	N/A

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

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)
No applicable dependencies			

2.2 RULES FOR IMPLEMENTING

The following section documents the content of the Component. It provides the basics 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	Additional Specification for Component
No applicable data mappings						

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

Standards	Description
Internet Engineering Task Force (IETF) Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) (RFC) #2818, May 2000	Describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port. For more information visit www.ietf.org.

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

The following sections include relevant materials referenced throughout this document.

No additional information at this time.

5.0 CHANGE HISTORY

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

5.1 MAY 11, 2007

This document is now Released for Implementation.

5.2 May 8, 2008

This document has been updated to include the HITSP Security and Privacy constructs and has been updated to reflect the new template.

- Replaced standard reference to Hypertext Transfer Protocol Secure (HTTPS) 443/tcp with the more accurate reference to standard IETF RFC 2818 for HTTP over TLS in Table 2.3-1
- Deleted Table 3.1-2 Reserved Port Numbers. This port information is now available online at: http://www.iana.org/assignments/port-numbers

5.3 MAY 16, 2008

Upon approval by the HITSP Panel on May 16, 2008, this document is now Released for Implementation.