## Document Change History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Description of Change</th>
<th>Name of Author</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Final Draft</td>
<td>Electronic Health Record Technical Committee</td>
<td>August 18, 2006</td>
</tr>
<tr>
<td>1.1</td>
<td>Ready for Public Comment</td>
<td>Electronic Health Record Technical Committee</td>
<td>September 12, 2006</td>
</tr>
<tr>
<td>1.2</td>
<td>Ready for Implementation Testing</td>
<td>Electronic Health Record Technical Committee</td>
<td>October 20, 2006</td>
</tr>
<tr>
<td>1.3</td>
<td>Review Copy</td>
<td>Care Delivery Technical Committee</td>
<td>April 27, 2007</td>
</tr>
<tr>
<td>2.0</td>
<td>Released for Implementation</td>
<td>Care Delivery Technical Committee</td>
<td>May 11, 2007</td>
</tr>
<tr>
<td>2.0.1</td>
<td>Review Copy</td>
<td>Provider Perspective Technical Committee</td>
<td>May 8, 2008</td>
</tr>
<tr>
<td>2.1</td>
<td>Released for Implementation</td>
<td>Provider Perspective Technical Committee</td>
<td>May 16, 2008</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Domain Committee</td>
<td>August 20, 2008</td>
</tr>
<tr>
<td>2.2</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Domain Committee</td>
<td>August 27, 2008</td>
</tr>
<tr>
<td></td>
<td>Template V2.5</td>
<td>Project Team</td>
<td>June 30, 2009</td>
</tr>
<tr>
<td>2.2.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Domain Committee</td>
<td>June 30, 2009</td>
</tr>
<tr>
<td>2.3</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Domain Committee</td>
<td>July 8, 2009</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1.0 INTRODUCTION ................................................................................................................................. 5  
1.1 Overview........................................................................................................................................ 5  
1.2 Copyright Permissions...................................................................................................................... 5  
1.3 Reference Documents....................................................................................................................... 5  
1.4 Conformance .................................................................................................................................... 5  
  1.4.1 Conformance Criteria ............................................................................................................... 5  
  1.4.2 Conformance Scoping, Subsetting and Options ....................................................................... 6  

2.0 COMPONENT DEFINITION ................................................................................................................ 7  
  2.1 Context Overview .......................................................................................................................... 7  
    2.1.1 Component Constraints ........................................................................................................ 7  
    2.1.2 Component Dependencies ..................................................................................................... 7  
  2.2 Rules For Implementing ............................................................................................................... 7  
    2.2.1 Data Mapping ....................................................................................................................... 7  
  2.3 Standards ....................................................................................................................................... 7  
    2.3.1 Regulatory Guidance ............................................................................................................. 7  
    2.3.2 Selected Standards ............................................................................................................... 8  
    2.3.3 Informative Reference Standards ......................................................................................... 8  

3.0 APPENDIX ........................................................................................................................................ 9  

4.0 CHANGE HISTORY ............................................................................................................................ 10  
  4.1 May 11, 2007 ................................................................................................................................. 10  
  4.2 May 8, 2008 ................................................................................................................................. 10  
  4.3 May 16, 2008 ............................................................................................................................... 10  
  4.4 August 20, 2008 ........................................................................................................................... 10  
  4.5 August 27, 2008 ........................................................................................................................... 10  
  4.6 June 30, 2009 ............................................................................................................................... 10  
  4.7 July 8, 2009 ................................................................................................................................ 10
FIGURES AND TABLES

Table 1-1 Reference Documents ................................................................. 5
Table 2-1 Component Constraints ............................................................. 7
Table 2-2 Component Dependencies ......................................................... 7
Table 2-3 Data Mapping ............................................................................ 7
Table 2-4 Regulatory Guidance ................................................................. 7
Table 2-5 Selected Standards ................................................................. 8
Table 2-6 Informative Reference Standards ........................................... 8
1.0 INTRODUCTION

1.1 OVERVIEW

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 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 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.

1.2 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2009 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.

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>
<thead>
<tr>
<th>Reference Document</th>
<th>Document Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HITSP Acronyms List</td>
<td>Lists and defines the acronyms used in this document</td>
</tr>
<tr>
<td>HITSP Glossary</td>
<td>Provides definitions for relevant terms used by HITSP documents</td>
</tr>
<tr>
<td>TN900 - Security and Privacy</td>
<td>TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs</td>
</tr>
</tbody>
</table>

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 interface 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 context for the HITSP Secure Web Connection Component is 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

Table 2-1 Component Constraints

<table>
<thead>
<tr>
<th>Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>The level of https protection depends on the correctness of the implementation by the web browser, the server software and the actual cryptographic algorithms supported</td>
</tr>
<tr>
<td>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</td>
</tr>
</tbody>
</table>

2.1.2 COMPONENT DEPENDENCIES

Table 2-2 Component Dependencies

<table>
<thead>
<tr>
<th>Standard/HITSP Component</th>
<th>Depends On (Name of standard/HITSP Component that it depends on)</th>
<th>Dependency Type (Pre-condition, Post-condition, General)</th>
<th>Purpose (Reason for this dependency)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable dependencies</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2 RULES FOR IMPLEMENTING

2.2.1 DATA MAPPING

Table 2-3 Data Mapping

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Description</th>
<th>Limit/Range of values</th>
<th>Data Source</th>
<th>Destination</th>
<th>Requirements/Pre-conditions</th>
<th>Additional Specification for Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable data mappings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3 STANDARDS

2.3.1 REGULATORY GUIDANCE

Table 2-4 Regulatory Guidance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable regulatory guidance</td>
<td></td>
</tr>
</tbody>
</table>
2.3.2 SELECTED STANDARDS

Table 2-5 Selected Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Engineering Task Force (IETF) Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) (RFC) #2818, May 2000</td>
<td>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 <a href="http://www.ietf.org">www.ietf.org</a></td>
</tr>
</tbody>
</table>

2.3.3 INFORMATIVE REFERENCE STANDARDS

Table 2-6 Informative Reference Standards

<table>
<thead>
<tr>
<th>Standard Name</th>
<th>Description/Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable informative reference standards</td>
<td></td>
</tr>
</tbody>
</table>
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 MAY 11, 2007

This document is now Released for Implementation.

4.2 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 Section 2.3
- Deleted Table: Reserved Port Numbers. This port information is now available online at: http://www.iana.org/assignments/port-numbers

4.3 MAY 16, 2008

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

4.4 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.

4.5 AUGUST 27, 2008

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

4.6 JUNE 30, 2009

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

4.7 JULY 8, 2009

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