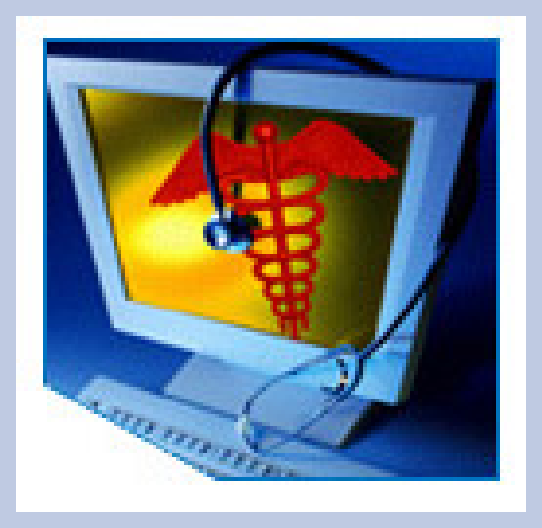
May 11, 2007
Version 2.0

HITSP Secure Web Connection Component

HITSP/C44



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

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
1.2.1	Review Draft – Released to TC for internal review	Care Delivery Technical Committee	March 28, 2007
1.3	Review Copy	Care Delivery Technical Committee	April 27, 2007
2.0	Released for Implementation	Care Delivery Technical Committee	May 11, 2007

TABLE OF CONTENTS

FIGURES AND TABLES

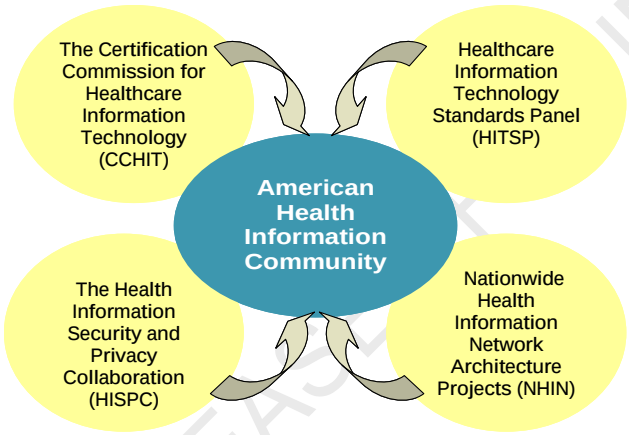
1.0 FOREWORD

This document is referred to as a Component and is an artifact of the Healthcare Information Technology Standards Panel (HITSP).

The following paragraphs provide background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. It also describes the HITSP process for healthcare standards harmonization and explains how to use this document and other related documents to inform your health Information Technology (IT) product development or product refinement. If you are familiar with HITSP and HITSP artifacts, please proceed to Section 2.0.

U.S. Nationwide Health Information Interoperability

Studies published by the Institute of Medicine and others have raised awareness of the extent to which the fragmented nature of clinical information adversely impacts the quality of care across the U.S. Health Information Technology (IT) can be used to enable better integration of clinical information. However, as of 2007, only a small number of U.S. healthcare providers have fully adopted health IT due, in part, to technical barriers associated with a lack of unambiguous and nationally recognized Interoperability Standards.



The American Health Information Community[1] (AHIC), a 2005 federally-chartered commission made up of leaders from public and private health sectors, was formed to provide recommendations on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way. At the same time, the Department of Health and Human Services, through the Office of the National Coordinator for Health IT (ONC) awarded contracts to 1) identify Interoperability Standards to facilitate the exchange of patient data (HITSP), 2) define a process for certifying that health IT products comply with appropriate standards through the Certification Commission for Healthcare Information Technology (CCHIT), and 3) develop a series of prototypes to establish the requirements of a Nationwide Health Information Network (NHIN). Under a renewed second year contract, HITSP scheduled activities will include identifying and constraining the standards needed for a standards-based security framework that provides the mechanisms needed to protect patient privacy and maintain confidentiality of information about the patient, as well as further work in additional Use Case priority areas recommended by AHIC. This year, CCHIT is expanding its certification efforts to inpatient, or hospital, electronic health record products. In

[1] http://www.hhs.gov/healthit/ahic.html

January 2007, four NHIN prototypes were delivered based on the requirements for health information exchange. The next phase will be to connect the prototypes and state and regional health information exchange efforts in trial implementations. These activities share the goal of widespread adoption of Interoperable electronic health records within 10 years through public-private collaboration.

HITSP's Role within Nationwide Interoperability Efforts

The HITSP[2] is a multi-stakeholder coordinating body designed to provide the process within which affected parties can identify, select, and harmonize standards for communicating healthcare information throughout the healthcare spectrum. As used by HITSP, the term "standard" refers, but is not limited to Specifications, Implementation Guides, Code Sets, Terminologies, and Integration Profiles. A standard should be produced through a well defined approach that supports a business process and

1. has been agreed upon by a group of experts
2. has been publicly vetted
3. provides rules, guidelines, or characteristics
4. helps to ensure that materials, products, processes, and services are fit for their intended purpose
5. is available in an accessible format
6. is subject to an ongoing review and revision process

HITSP functions as a partnership of the public and private sectors and operates with a neutral and inclusive governance model administered by the American National Standards Institute. The goal of the Panel is to:

- Facilitate the development of harmonized Interoperability Specifications and information policies, including Standards Development Organization (SDO) work products (e.g. standards, technical reports). These policies, profiles and work products are essential for establishing privacy, security and Interoperability among healthcare software applications
- Coordinate, as appropriate, with other national, regional and international groups addressing healthcare information to ensure that the resulting standards are globally relevant
- Be Use Case driven, using information from stakeholders and basing decisions on industry needs

The work of the HITSP is conducted through formally chartered Technical Committees and Work Groups. The artifact of the Technical Committee and Work Group activities is an Interoperability Specification (IS) and related constructs referred to as Transaction Packages, Transactions, or Components. For additional information on these constructs, please refer to the HITSP Harmonization Framework.

This HITSP document pertains to the Interoperability Specification for the following:

[2] www.hitsp.org

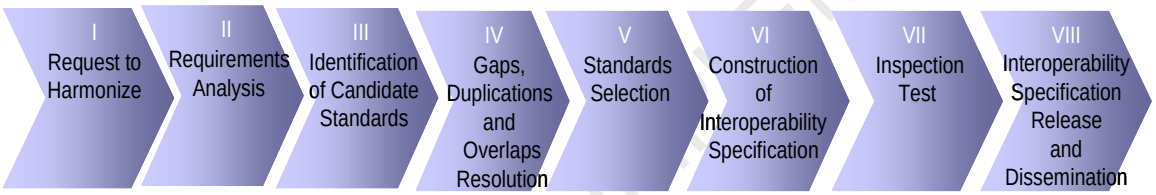
Use Case	Specific Scope of this Use Case
Electronic Health Record	Allow ordering clinicians to electronically access laboratory results, and allow non-ordering authorized clinicians to electronically access historical and other laboratory results for clinical care.

In its final state, this Interoperability Specification provides unambiguous instructions for how two or more systems should exchange information within this specific context of the Use Case.

How Use Cases and HITSP Interoperability Specifications are Developed

The American Health Information Community, as the representative of public and private health sector stakeholders, identified the three Use Cases (available at hitsp.org) that drove the initial efforts of the HITSP. Nationwide public and private health sector priorities continue to focus the efforts of the HITSP. The Use Case driven HITSP harmonization process is implemented by formally chartered Technical Committees. The volunteers that comprise a Technical Committee followed an 8 step process, depicted below in Figure 1.0-1.

Figure 1.0-1 HITSP Harmonization Process Steps



How to Read this Interoperability Specification

Each Interoperability Specification (IS) is actually a suite of documents that, taken as a whole, provide a detailed map to existing standards and specifications that will satisfy the requirements imposed by a given Use Case. It identifies and constrains standards where necessary, and creates groupings of specific actions and actors to further describe the relevant contexts. Where gaps and overlaps are identified, the Interoperability Specification provides recommendations and a roadmap for corrections to be made. This Interoperability Specification includes the Transaction Packages, Transactions, and Components.

2.0 INTRODUCTION

As an introduction to the Secure Web Connection Component, this section provides a high level overview of an information sharing scenario enabled by following this specification, outlines the technical scope of the specification, describes the intended audience for the technical content of the document, acknowledges the copyright protections that pertain, provides Internet links to the HITSP Acronyms List and an explanation of the conventions used to convey the full descriptions and usage of standards. If you are already familiar with this information, proceed to Section 3.0 Referenced Standards.

2.1 OVERVIEW

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.

2.2 TECHNICAL ASSUMPTIONS AND SCOPE

This Interoperability Specification focuses on a set of constrained standards for information interchange that address the core requirements of the Use Case described above. It may not define all functions, constructs and standards necessary to implement a conforming system in a real world environment. The following paragraphs provide the HITSP principles with regard to several critical topics to ensure consistent interpretation of the Interoperability Specifications.

2.2.1 INTEROPERABILITY SPECIFICATIONS NOT FUNCTIONAL SPECIFICATIONS

The HITSP Interoperability Specification defines how two or more systems exchange standard data content in a standardized manner. Interoperability Specifications define the necessary business and technical actors, the transactions between them including the message, content and terminology standards for the actual information exchange. Interoperability Specifications do not specify the functional requirements or behaviors of the systems or applications.

2.2.2 ARCHITECTURAL NEUTRALITY

HITSP Interoperability Specifications, unless otherwise noted, are not intended to define or prescribe any system architecture or implementation. At the most basic level, the Interoperability Specifications define specific information exchange standards that are to be used by any two systems. Information exchange must be placed within the context of a transaction between defined technical actors which fulfill higher level business requirements derived from the Use Case. In some cases the necessary technical actors

may require some architectural structure or make some assumptions involving synchronous or asynchronous data exchanges, or require specific type of exchange, such as a message or document. These requirements may constrain to some degree the total range of choices regarding system architectures. When constraints are necessary to meet the Use Case requirements, the Interoperability Specification will note this and will retain as much architectural neutrality as possible. When appropriate, the Interoperability Specifications may provide architectural examples and discuss considerations of such examples.

2.2.3 THE USE OF MESSAGES AND DOCUMENTS AS APPROPRIATE

Within healthcare information there is an ongoing debate concerning the proper role of messages and documents as methods of exchanging data. Messages are typically non-persistent encapsulations of highly structured data that require external context. Documents are persistent encapsulations of both data and context which may be authenticated to insure non-repudiation. Persistence as defined by Health Level Seven (HL7), means that a clinical document continues to exist in an unaltered state for a time period defined by local and regulatory requirements. Non-repudiation, as defined by ISO adapted from ASTM E31, means a service that provides proof of the integrity and origin of data, which can be verified by any party. HITSP recognizes that requirements for both messages and documents exist and where consistent with harmonization will support both. For example, depending on specific phases of the workflow, a laboratory result might be exchanged as a message, as a document, or both. Business requirements may define which format is more effective.

2.2.4 IMPLEMENTATION TESTING

The 2006 set of Interoperability Specifications were evaluated by inspection testers (desktop review) and reviewed by HITSP members prior to HITSP approval. Although the Interoperability Specifications are based on approved standards, when published, they represent combinations and constraints that have not been tested in actual implementations. HITSP enlisted partners to develop test plans, data and suites to test the implementation and then to support a program for progressive testing, feedback and deployment of implementations. Feedback from test implementers has been used in the revisions in Version 2.0.

2.2.5 SECURITY AND PRIVACY

The Health Insurance Portability and Accountability Act (HIPAA) and its Administrative Simplification sections establish the minimum federal requirements for security and privacy of individually identifiable health information (IIHI). HIPAA requires that “covered entities” establish and maintain secure systems that protect IIHI from unauthorized disclosures while ensuring its availability for authorized uses. Most providers, health plans and intermediaries, and by contract their business associates, are covered by HIPAA regulation. However, HIPAA does not cover personal health records unless they are held by a covered entity, nor an individual’s use of their own health information.

Currently, HITSP is charged by ONC to harmonize standards based on Use Cases derived from AHIC requirements and priorities. Implicitly and in some cases explicitly, the Use Cases require a secure infrastructure and certain security or privacy functions. Because of time and resource constraints and the need for further information as described below, HITSP has decided to defer specifying most security requirements, instead treating these as a pre-condition for implementing the core information exchanges. The underlying premise is that HITSP**,** based upon prioritization by AHIC and ONC, will in the future identify and constrain the standards needed for a standards-based security framework that provides the mechanisms needed to protect patient privacy and maintain confidentiality of information about the patient. This standards-based security framework will need to accommodate federal, state, local, and healthcare enterprise security and privacy policies and processes. Exceptions to the deferred requirements that are addressed in this first release are secure web-based messaging, pseudonymization and anonymization.

There is a special case for the Consumer Empowerment (CE) Use Case. In the first year of HITSP's work, the Consumer Empowerment TC is to provide an Interoperability Specification for sharing of demographic data, medication lists, and allergies *based on patient consent*. Patient consent is clearly within the scope of the CE Use Case. However, HITSP requires further guidance on patient consent, particularly since patient consent is not addressed by HIPAA in the case of a personal health record (PHR) nor is it established within widely accepted PHR standards. Therefore HITSP identifies patient consent as a necessary pre-condition for successful implementation of a PHR that contains personal demographic data and medication histories. Patient consent will be documented as a pre-condition in the CE Interoperability Specification. Work on patient consent has been deferred until the second year of HITSP work.

2.3 AUDIENCE

The Interoperability Specification is designed to be used by analysts who need to understand the Interoperability requirements for the described Use Case, and by implementers working to develop interoperable applications. Understanding and using the relevant set of specifications is a key requirement for establishing interoperability compliance.

2.4 COPYRIGHT PERMISSIONS

2.5 ACRONYMS

The acronyms used in this document are contained in the HITSP Acronyms List.

2.6 CONVENTIONS

The conventions are used to convey the full descriptions and usage of standards in the Interoperability Specification and are contained the HITSP Conventions List.

3.0 REFERENCED STANDARDS

It is HITSP's policy to incorporate only standards that have been approved according to the formal policy of standards organization, as defined by HITSP, which publishes the standard. HITSP interprets approval to include Draft Standards for Trial Use. The objective is to incorporate only standards that are managed within a formal life cycle process as defined by the standards organization. In some cases, where we believe a standard that is not yet approved may best meet the requirements of an Interoperability Specification, HITSP may provide a roadmap of its future intent conditional on future actions by either or both the standards organizations and the HITSP Technical Committee. Thus there are four classes of HITSP-committed standards.

- Approved for Use – standards included for unconditional use within a HITSP construct
- Interim – standards included for use now within a HITSP construct but for a defined time period or conditional on future actions, e.g., "Intended for Use" standard is available
- Provisional - standards that are not yet but are expected to be approved by the Standards Organization by the time the Interoperability Specification is released by HITSP. A "Provisional" standard becomes an "Approved for Use" standard only if:
  - It is approved by the Standards Organization by the time that the Interoperability Specification is released by HITSP and
  - It is substantially the same as it was when it was provisionally used and
  - It requires no further action by the Technical Committee
- Intended for Use – proposed standards that are roadmapped for future use pending actions by the TC and/or the standards organization. Therefore a standard is defined as "Intended for Use" because it will not be approved by the time that the HITSP construct is released but is sufficiently defined to enable detailed evaluation of how well it will meet technical and business requirements

HITSP may continue to use "Provisional" or "Interim" standards as they existed when incorporated into the HITSP construct if the expected conditions are not satisfied until such time as HITSP can replace it with a more suitable standard. In this circumstance, the Standards Organization would have no responsibility to maintain or correct this artifact. If a standard "Intended for Use" is not developed and approved in terms of time frame or content as expected by the TC at the time of its initial selection, it may be replaced. All standards used by HITSP must meet the HITSP selection criteria. The use of "Interim" and "Intended for Use" standards will be weighed against the alternative of simply declaring a gap for HITSP and the Standards Organizations to resolve.

3.1 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 Interoperability Specification:

Table 3.1-1 List of Standards

Standards	Description
Hypertext Transfer Protocol Secure (HTTPS) 443/tcp	http protocol over TLS/SSL

As of October 1998, SSL has the following port numbers reserved with the Internet Assigned Numbers Authority (IANA), a part of the Internet Engineering Task Force (IETF):

Table 3.1-2 Reserved Port Numbers (SSL)

Keyword	Decimal	Description
Nsiiops	261/tcp	IIOP Name Service over TLS/SSL
https	443/tcp	http protocol over TLS/SSL
ddm-ssl	448/tcp	DDM-SSL
Smtps	465/tcp	smtp protocol over TLS/SSL
Nntps	563/tcp	nntp protocol over TLS/SSL
sshell	614/tcp	SSLshell
ldaps	636/tcp	ldap protocol over TLS/SSL
ftps-data	989/tcp	ftp protocol, data, over TLS/SSL
ftps	990/tcp	ftp, control, over TLS/SSL
telnets	992/tcp	telnet protocol over TLS/SSL
imaps	993/tcp	imap4 protocol over TLS/SSL
ircs	994/tcp	irc protocol over TLS/SSL
pop3s	995/tcp	pop3 protocol over TLS/SSL

4.0 COMPONENT

4.1 CONTEXT OVERVIEW

4.1.1 CONTEXTUAL CONSTRAINTS

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. 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.

4.1.2 TECHNICAL ACTORS

Table 4.1.2-1 Technical Actors

Actor	Description
Web browser	This is the software that allows a user to access and view HTML documents. (e.g., Internet Explorer)
Server	A computer that delivers information and software to other computers linked by a network.

4.1.3 SSL OVERVIEW FROM THE CUSTOMER'S BROWSER VIEWPOINT

1) Browser checks the certificate to make sure that the site you are connecting to is the real site and not someone intercepting
2) Determine encryption types that the browser and web site server can both use to understand each other
3) The site server and client browser authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data
4) The browser and Server communicate using the encryption, the web browser indicates (usually with an icon) that the web pages are processed using SSL

4.2 INFORMATION INTERCHANGE COMPONENTS: RULES FOR IMPLEMENTING

4.2.1 PROCESS PRE-CONDITIONS

Browser checks the certificate to make sure that the intended destination site is the real site.

4.2.1.1 PROCESS TRIGGERS

1) Browser checks the certificate to make sure that the site you are connecting to is the intended destination site
2) Determine encryption types that the browser and web site server can both use to communicate with each other
3) The site server and client browser authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data

4) The browser and Server communicate using the encryption, the web browser indicates (usually with an icon) that the web pages are processed using SSL

4.2.2 PROCESS POST-CONDITIONS

Not Applicable.

4.2.2.1 PROCESS OUTPUTS

Not Applicable.

4.2.3 DATA STRUCTURE

Not Applicable.

4.2.3.1 DATA MAPPING

Not Applicable.

4.2.3.2 MINIMUM DATA-SET

Not Applicable.

4.2.4 ADDITIONAL SPECIFICATIONS

The primary goal of Secure Sockets Layer (SSL) is to provide privacy and reliability between two communicating applications. SSL is composed of two layers. At the lower level, layered on top of some reliable transport Protocol, for example Transmission Control Protocol (TCP), is the SSL Record Protocol, which is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application Protocol independent. A higher level Protocol can layer on top of SSL transparently. For Internet applications, a generalized variant of SSL called Transport Layer Security (TLS) has been developed. TLS was developed as the successor to SSL, and is nearly identical to SSL, except that it implements an open and standards-based solution, more non-proprietary ciphers, better error reporting, and Keyed-Hash Message Authentication Code (HMAC) digests instead of simple Message-Digest Algorithm 5 (MD5). The structure of the start of a TLS session allows negotiation of the level of the protocol to be used. This way, a Client or Server can simultaneously support TLS and SSL and negotiate the most appropriate protocol for the connection.

4.3 SECURITY COMPONENTS: RULES FOR IMPLEMENTING

4.3.1 SECURITY CONSTRAINTS

HTTPS is HTTP riding on top of SSL. The primary goal of SSL is to provide privacy and reliability between two communicating applications. SSL is composed of two layers. At the lower level, layered on top of some reliable transport Protocol, for example TCP, is the SSL Record Protocol, which is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application Protocol independent. A higher level Protocol can layer on top of SSL transparently. For Internet applications, a generalized variant of SSL called TLS has been developed.

4.3.2 CODING SPECIFICATION

Not Applicable.

4.3.3 MAPPINGS AND ELEMENTS

Not Applicable.

4.3.4 ADDITIONAL SPECIFICATIONS

Not Applicable.

5.0 CONSTRAINTS FOR REUSE

None.

6.0 CHANGE HISTORY

6.1 MAY 11, 2007

This document is now Released for Implementation.