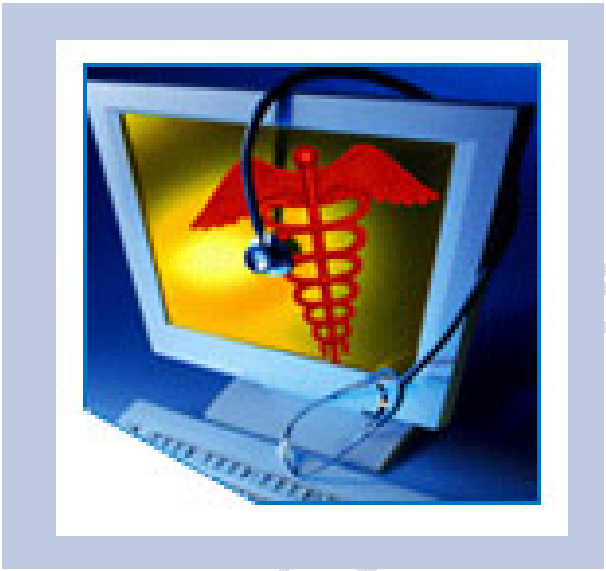
August 18, 2006
Version 1.0

HITSP Interoperability Specification: Secure Web Connection Component

HITSP/ISC-44



Submitted to:
Healthcare Information Technology Standards Panel

Submitted by:

Electronic Health Record Technical Committee

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Final Draft	Electronic Health Record Technical Committee	18 August 2006

1.0 FOREWORD

Healthcare Information Technology Standards Panel (HITSP) 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. 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 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 informatics to ensure that the resulting standards are globally relevant.
- Be use-case driven, utilize information from stakeholders and base its decisions on industry needs.

The HITSP shall serve the public good by working to ensure that the combined work of various healthcare information standards organizations supports interoperability, accurate use, access, privacy and security of shared health information.

In order to advance the goal of expanding harmonized interoperability specifications and information policies, HITSP was tasked with developing interoperability specifications for three main use case "breakthroughs areas" in which specific, near term value to the health care consumer could be realized. The harmonized use case areas are:

1.	Biosurveillance	Transmit essential ambulatory care and emergency department visit, utilization, and lab result data from electronically enabled health care delivery and public health systems in standardized and anonymized format to authorized Public Health Agencies with less than one day lag time.
2.	Consumer Empowerment	Allow consumers to establish and manage permissions access rights and informed consent for authorized and secure exchange, viewing, and querying of their linked patient registration summaries and medication histories between designated caregivers and other health professionals.
3.	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.

The interoperability specification provides a detailed mapping of existing standards and specifications such as implementation guides, integration profiles to actions and actors that satisfy the requirements

imposed by the relevant use cases. 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.

2.0 INTRODUCTION

A protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). S-HTTP is designed to transmit individual messages securely. This protocol was approved by the Internet Engineering Task Force (IETF) as a standard. IETF is the main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

2.1 OVERVIEW

https is a URI scheme which is syntactically identical to the http: scheme normally used for accessing resources using HTTP. Using an https: URL indicates that HTTP is to be used, but with a different default port and an additional encryption/authentication layer between HTTP and 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 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 interoperability set of specifications is a key requirement for establishing interoperability compliance.

2.3 TERMS AND DEFINITIONS

The definitions used for the purposes of this document can be found in the glossary. Refer to the appendix for the glossary.

2.4 CONVENTIONS

This specification uses the following to convey the full descriptions and usage of standards:

UML sequence and activity diagrams

In these diagrams, the actors and transactions are highlighted within the framework of the specific scenario or context. The actors involved in the specified use-scenario or context are mapped out, and the interactions between each action and actor for a particular context, and the flow of data are provided through the use of arrows. Diagrams are named according to the section in which they reside, and will use the following naming convention:

Figure <section number>-<consecutive number for the diagram, e.g. 1, 2, 3, etc.>. <Short name/description of diagram>. For example, a diagram residing in section 3.1.3 showing the Actor Interactions for the Send Lab Results transaction package is named:

Figure 3.1.3-1. Send Lab Results Transaction Package

Tables

Tables are used to indicate standards categorizations, as well as dependencies and constraints between constructs. Tables are named according to the section in which they reside, and will use the following naming convention:

Table <section number>-<consecutive number for the table, e.g. 1, 2, 3, etc.>. <Short name/description of table>. For example, a table residing in section 2.7.1 showing the Dependencies between the transactions for the Send Lab Results transaction package is named:

Table 2.7.1-1. Send Lab Results Transaction Package dependencies

References

When references are made to another section within an Interoperability Specification a section number is used by itself. When references are made to other constructs that are related to the Interoperability Specification, such as Transaction Packages, Components or Composite Standards, the HITSP document short name and section number are displayed as follows:

<HITSP Document short name or Composite Standard Short Name>-<Volume Number>: <section number>

where:

<HITSP document short name> is a short designator for the construct (e.g. HITSP/ISTP-013)

<Composite Standard Short Name> is a short designator for the composite standard (e.g. IHE-ITI TF)

<Volume Number> is the applicable volume within the given composite standard (e.g. 1)

<section number> is the applicable section number (e.g. 3.1)

For example: HITSP/ISTP-013: 3.1 refers to Section 3.1 in the Interoperability Specification for a Transaction Package, IHE-ITI TF-2: 4.33 refers to Section 4.33 in volume 2 of the IHE IT Infrastructure Technical Framework.

Reproductions

Where large sections of composite standards or base standards are reproduced within a HITSP specification, the reproduced sections are cited with introductory text containing the reference information for the composite or base standard. In addition, the beginning and ending of the reproduced text are respectively shown using a beginning statement:

The text for the <composite or base standard name> specification begins here:

And an ending statement:

The text for the <composite or base standard name> ends here.

2.5 COMMENTS

To submit comments for this interoperability specification, please download the Comment Submission sheet from the HITSP site at www.hitsp.org and provide all relevant information, and then email the completed document to hitspcomments@ansi.org. Comments are consolidated periodically and sent to the Technical Committees for review.

2.6 COPYRIGHT PERMISSIONS

3.0 STANDARDS REFERENCES

3.1 LIST OF BASE STANDARDS

Theoretically SSL can transparently secure any TCP-based protocol running on any port if both sides know the other side is using SSL. However, in practice, separate port numbers have been reserved for each protocol commonly secured by SSL – this allows packet filtering firewalls to allow such secure traffic through.

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):

Keyword	Decimal	Description
https	443/tcp	http protocol over TLS/SSL

Table 3.1-1. Reserved Port Numbers (SSL)

TLS is the Transport Layer Security Working Group of the IETF (Internet Engineering Task Force). It is the working group responsible for moving transport layer protocols such as SSL through the standards tracks.

3.2 LIST OF COMPOSITE STANDARDS

Theoretically SSL can transparently secure any TCP-based protocol running on any port if both sides know the other side is using SSL. However, in practice, separate port numbers have been reserved for

each protocol commonly secured by SSL -- this allows packet filtering firewalls to allow such secure traffic through.

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):

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

Table 3.2-1. Reserved Port Numbers (SSL)

TLS is the Transport Layer Security Working Group of the IETF (Internet Engineering Task Force). It is the working group responsible for moving transport layer protocols such as SSL through the standards tracks.

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 IP/port combination.

4.1.2 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.

Table 4.1.2-1 Technical Actors

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. Browser and Server send each other unique codes to use when scrambling (or encrypting) the information that will be sent.
4. The browser and Server start talking using the encryption, the web browser shows the encrypting icon, and web pages are processed secured.

4.2 INFORMATION INTERCHANGE COMPONENTS: RULES FOR IMPLEMENTING

4.2.1 PROCESS PRE-CONDITIONS

Browser checks the certificate to make sure that the site you are connecting to is the real site and not someone intercepting.

4.2.1.1 PROCESS TRIGGERS

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. Browser and Server send each other unique codes to use when scrambling (or encrypting) the information that will be sent.
4. The browser and Server start talking using the encryption, the web browser shows the encrypting icon, and web pages are processed secured.

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 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. 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 HMAC digests instead of simple 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. 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 HMAC digests instead of simple 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.

4.3.2 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 APPENDIX

6.1 GLOSSARY

Included is the common interoperability glossary that is used for all the Use Cases. This is the HITSP glossary that spans all the interoperability specifications, which can be found in the following folder on the HITSP site:
http://publicaa.ansi.org/sites/apdl/Documents/Forms/AllItems.aspx?RootFolder=http%3a%2f%2fpublicaa%2eansi%2eorg%2fsites%2fapdl%2fDocuments%2fStandards%20Activities%2fHealthcare%20Informatics%20Technology%20Standards%20Panel