Transport of Immunization HL7 transactions over the Internet Using Secure HTTP

Version 1.0
September 17, 2002

By The HL7 Immunization Registry Task Force sub group on HTTP message transport.

Joseph Rockmore – IBM Corporation
Andrey Yeatts – Scientific Technologies Corporation
Kevin Davidson – QS Technologies, Inc.

Introduction

This document discusses conventions that may be used to transport Health Level Seven (HL7) messages over the Internet using Secure HTTP (HTTPS). It is the intent of sub group to use existing standards wherever possible.

Privacy

When transporting identifiable health information, the privacy of the information must be insured. Privacy may be insured by encrypting the message or transmitting the message over a secure channel. The HTTPS protocol, widely used for secure transactions in eCommerce, provides encryption and is recommended by this standard. The HTTPS protocol is defined in RFC 2660 (http://www.ietf.org/rfc/rfc2660.txt); however, we anticipate that commercial and public domain web servers and browsers will implement the protocol for these transactions and that immunization registry implementers will not be concerned with the details of the HTTPS protocol. If a secure channel (e.g. VPN or leased communications line) is available, the HTTP protocol may be used in lieu of HTTPS subject to local law and registry policy.

Authentication

Health information messages state important facts about personal information. Because of this, it is necessary to provide assurance of the identity of party asserting the facts in these messages. Authentication provides such assurance.

Two authentication methods are proposed.

1. User ID/Password. An immunization registry will provide each of its clients (other immunization registries and data providers) a User ID and a strong password. The client will present this User ID and password whenever sending transactions. Standards for User IDs and Passwords may be set by individual registries.
2. The HL7 message will be digitally signed using X.509 certificates and formatted according to the S/MIME standard. X.509 is a standard of the International Telecommunications Union.

Method 1 is considered primarily as a means whereby immunization data providers may authenticate with their state or regional registry. Method 2 is the preferred means for authentication between registries. However, either method is allowed in either situation subject to law and registry policy.

The sub group also recognizes that the complexity of implementing the digital signature may result in the User ID/Password method being the first deployed.

The S/MIME standard provides a structure to format messages that are digitally signed using an X.509 certificate. Encryption is an optional component of S/MIME. This

standard assumes that encryption through HTTPS or other secure channel will be used, and therefore use of the encryption facility of S/MIME is not required.

In order to use S/MIME, both the sender and the receiver must obtain X.509 digital certificates from agreed-upon Certificate Authority(s). The presentation of a message from a recognized Certificate Authority insures the identity of the sender and the integrity and non-deniability of the message. It does not, in and of itself, determine whether the sender is someone the registry should talk to; each registry implementation must develop a means of determining which presenters of valid certificates have permission to exchange messages with the registry.

This document does not address the issue of obtaining or distributing digital certificates, but we note that this is a significant issue.

Transport Protocol for HL7 Messages over HTTPS when using User ID/Password Authentication

When using User ID/Password Authentication, application programs will contact the registry server by issuing an HTTP POST transaction with the following data fields:

- USERID – This is the registry-assigned User ID. Implementations must support User ID's of at least 8 characters, including upper and lower case letters and digits. Case sensitivity of User ID is at the option of the implementing registry.
- PASSWORD – This is the registry-assigned Password for the User. Implementations must support Passwords of at least 8 characters, including upper and lower case letters and digits. Case sensitivity of the Password is at the option of the implementing registry.
- FACILITYID - The Facility ID is as defined in *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol*, section 2.24.1.4 for the MSH Sending facility.
- MESSAGEDATA – The HL7 message as ASCII text. The message must begin with the character string "MSH".

The response content to the HTTP POST will be the appropriate HL7 message as required by *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol.* The HL7 message will not be encapsulated in any way.

Transport Protocol for HL7 Messages over HTTPS when using Digital Signatures

When using Digital Signatures for Authentication, application programs will contact the registry server by issuing an HTTP POST transaction with the following data fields:

- FACILITYID - The Facility ID is as defined in *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol*, section 2.24.1.4 for the MSH Sending facility.
- MESSAGEDATA – The Message content will be the digitally signed HL7 message formatted in accordance S/MIME Version 2 specification available at http://www.ietf.org/rfc/rfc2311.txt.

The response content to the HTTP POST will be the appropriate HL7 message as required by *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard*. Message content will be the digitally signed HL7 message formatted in accordance S/MIME Version 2.

HTTP Version and Recommended Headers

Where possible, HTTP version 1.1 (http://www.ietf.org/rfc/rfc2616.txt) should be used for all client messages.

When HTTP messages are sent, intervening servers may cache responses to improve overall network response. Because the messages discussed here are dynamic queries and updates, cached results are likely to be incorrect or out of date. HL7 query ids should be unique and so should not be cached, but to avoid any possible interaction with caching servers, the `no-cache` directives should be used in all HTTP headers. In HTTP version 1.1, these take the form:

```
Cache-control: no-cache
```

In version 1.0, the equivalent is:

```
Pragma: no-cache
```

Registry Server Lookup service

Both public key infrastructure and registry-to-registry communication require a lookup service to link registries with their public keys and http addresses.

Such a lookup (or directory) service should provide sufficient information to a client that the client could adequately determine the likely authoritative registry given address information in an HL7 query message or “other previous residence” address hints.

The information returned should include addresses for the HL7 HTTP server and human technical contact, and the public key used to communicate authentication messages to the registry.

The search information schema should include for each registry:

A printable name for the registry (ex: Arizona State Immunization Registry)

The country the covered by the registry's domain of service (ex: USA)
The state the registry's domain of service covers (ex: AZ)
If the registry is not authoritative for the entire state:
The list of counties the registry is authoritative for (ex: Maricopa)
If the registry is not authoritative for the entire county, or if there are cities outside the jurisdiction of any county for which the registry is authoritative:
The list of cities the registry is authoritative for (ex: Chandler, Mesa)

The returned data for a matching registry should include:

The HTTP/HTTPS URL for the HL7 service
The X509 public key for the service
A human technical contact email address
A human technical contact telephone

We recommend that an authority within the Immunization Registry community maintain a web site containing a directory of immunization registry HTTP servers by state, containing the URL, contact person, and phone number. The web page will be designed to be friendly to automated HTML parsers.

or

We recommend that an authority within the Immunization Registry set up an LDAP server to provide the URL, contact person, phone number and public key of each immunization registry HTTP server.

Batch Uploads via HTTPS

When batches of HL7 messages are sent via HTTP, they should be combined according to the HL7 Batch Protocol as described in by *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol* . Batch uploads use the same specifications above, except that instead of the messages starting with "MSH", batches start with "FHS".

Reference Implementations

The working group proposed the creation of reference implementations demonstrating the protocols described herein. The purpose of the reference implementation is to provide examples that may be used as starting points by registry developers in implementing the protocols in this standard. The following are general principles for the reference implementations:

1. The reference implementations shall be open source.
2. The reference implementations should avoid, to the extent possible, registry-specific business logic, and should concentrate on the protocols.

3. The reference implementations should provide simple interfaces for authentication and message logging by external routines to be provided by the specific registry implementers.