January 25, 2010
Version 1.1

HITSP HL7 Messaging Service Collaboration

HITSP/SC115

Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security, Privacy and Infrastructure Domain Technical Committee
(Formerly Security and Privacy Technical Committee)

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
0.0.1	Review Copy	Security, Privacy and Infrastructure Tiger Team	June 30, 2009
1.0	Released for Implementation	Security, Privacy and Infrastructure Tiger Team	July 8, 2009
1.0.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	January 18, 2010
1.1	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	January 25, 2010

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

1.1 SERVICE COLLABORATION OVERVIEW AND SCOPE

The HL7 Messaging Service Collaboration provides the ability to send and receive HL7 messages to a raw HL7 MLLP message transaction. The Service Collaboration applies the necessary Security and Privacy Constructs. The Service Collaboration supports all the HL7 messaging needs of the HITSP Constructs including:

- HITSP/T14 Send Laboratory Result Message
- HITSP/T17 Secured Communication Channel
- HITSP/C34 Patient Level Quality Data Message
- HITSP/C36 Lab Result Message
- HITSP/C39 Encounter Message
- HITSP/C41 Radiology Result Message
- HITSP/TP43 Medication Orders
- HITSP/T67 Clinical Referral Request Transport
- HITSP/C70 Immunization Query and Response
- HITSP/C72 Immunization Message

For more information about the underlying Capabilities, pre-conditions, post-conditions, data flows and other detailed information, please refer to the constructs that are used by this Service Collaboration.

This Service Collaboration creates two 'virtual' interfaces that are not otherwise specified in HITSP but are implied once the Message is separated from the HL7 v2 MLLP transport. The "Generic HL7 Message Sender" and "Generic Message Receiver" virtual interfaces leverage the common HL7 transport profiled in IHE ITI Technical Framework Version 4.0 (or later), Appendix C.2.1. Details of the required or optional acknowledgment(s) depend on the message and the implementation, and are explained in the underlying standards.

The Service Collaboration document illustrates one internal view diagram and sequence table for each service interface. The diagrams are descriptive and the sequences are not mandatory. They may be affected by policy, chosen architecture, and implementation details. Conformance is measured against the underlying constructs.

1.2 SERVICE COLLABORATION INVOCATION

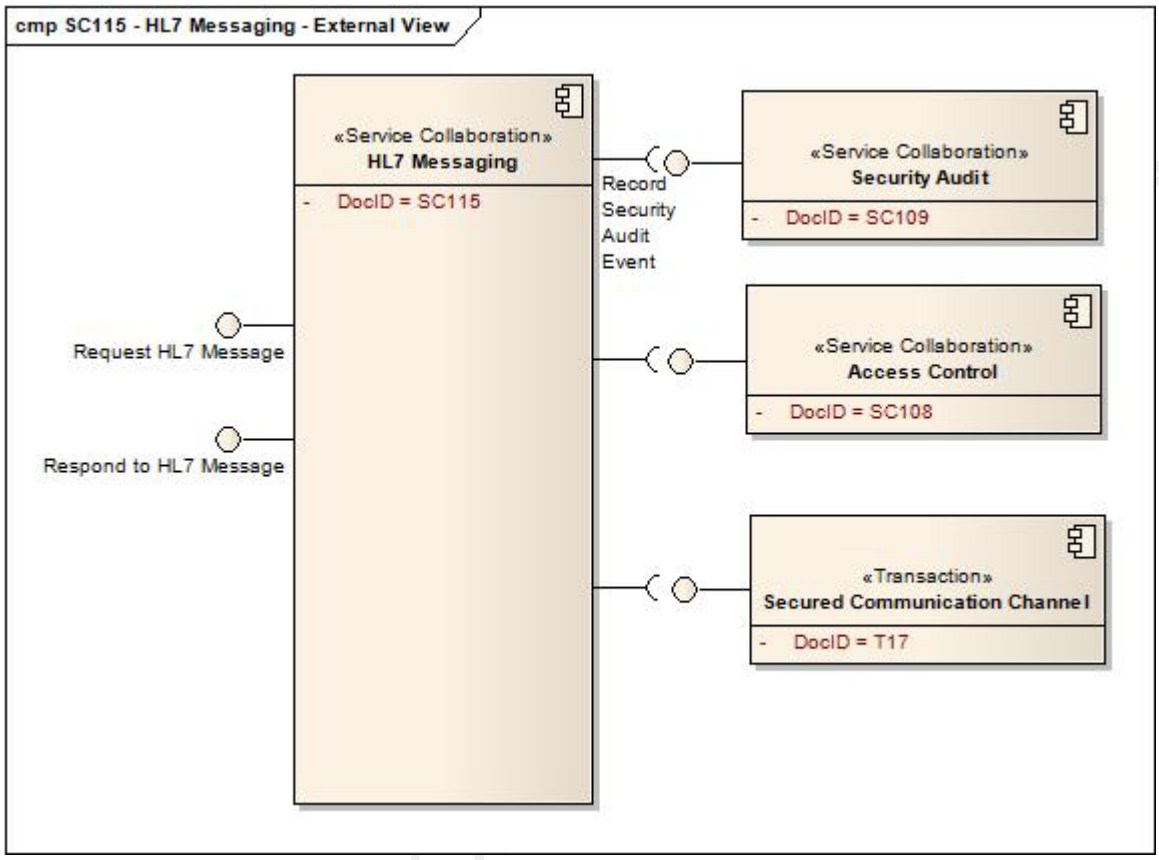
Table 1-1 Service Collaboration Transactions and Data

Service Collaboration	Service Collaboration Description	Interface	Optionality
HITSP/SC115	Provides the collaboration details on the requests side of an HL7 messaging interaction	Request HL7 Message	R
HITSP/SC115	Provides the collaboration details on response side of an HL7 messaging interaction	Respond to HL7 Message	R

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

1.3 EXTERNAL VIEW (i.e.,“Black Box” Diagram)

Figure 1-1 HL7 Messaging External View



1.3.1 SERVICE COLLABORATION SOURCE CONSTRUCTS

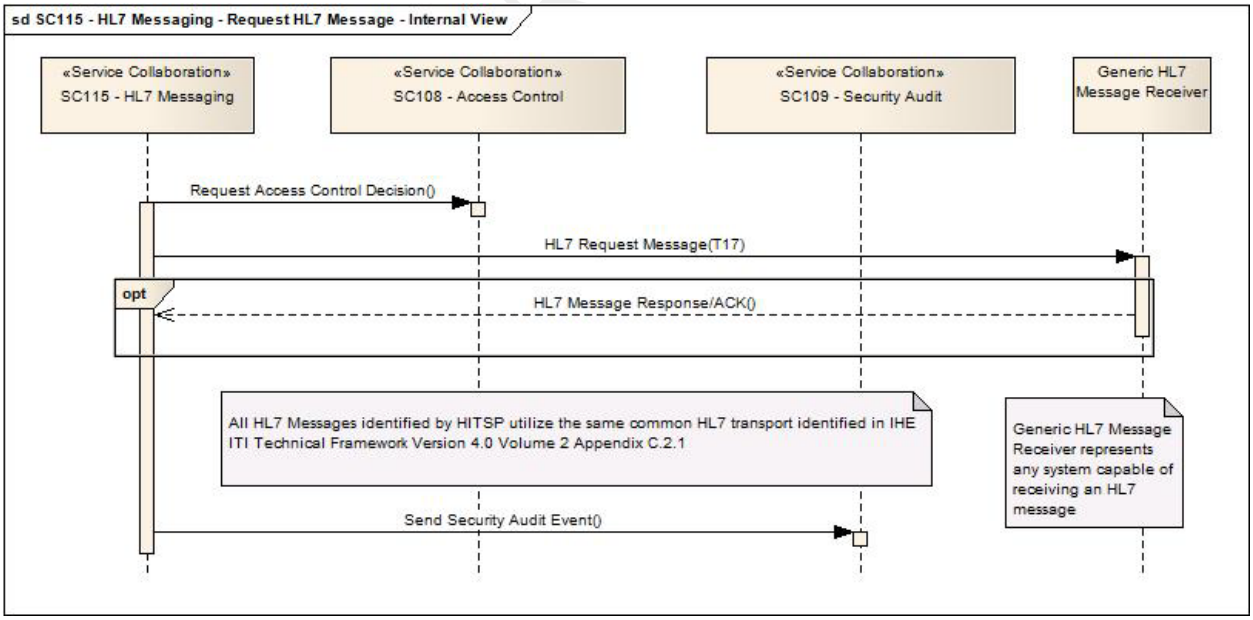
Table 1-2 List of Source Constructs

Construct	Description
HITSP/SC108 - Access Control	The HITSP Access Control Service Collaboration provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control, entity based access control, context based access control, and the execution of consent directives
HITSP/SC109 - Security Audit	The HITSP Security Audit Service Collaboration describes the mechanism to record security relevant events in support of policy, regulation, or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed
HITSP/T17 - Secured Communication Channel	The HITSP Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transmissions, and the mutual trust between communicating parties. Its objectives include providing: mutual node authentication to assure each node of the others' identity; transmission integrity to guard against improper information modification or destruction while in transit; and transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes
HL7 Messaging as identified in multiple HITSP constructs	

1.4 INTERNAL VIEW DIAGRAM WITH SEQUENCING (i.e., "White Box" Diagram)

1.4.1 INTERFACE: REQUEST HL7 MESSAGE

Figure 1-2 Request HL7 Message Internal View



1.4.1.1 SEQUENCE DETAILS

Table 1-3 Request HL7 Message – Pre-conditions

Pre-condition	Uses SC, T, TP or C	Interface	Purpose
None			

Table 1-4 Request HL7 Message – Sequence of Constructs

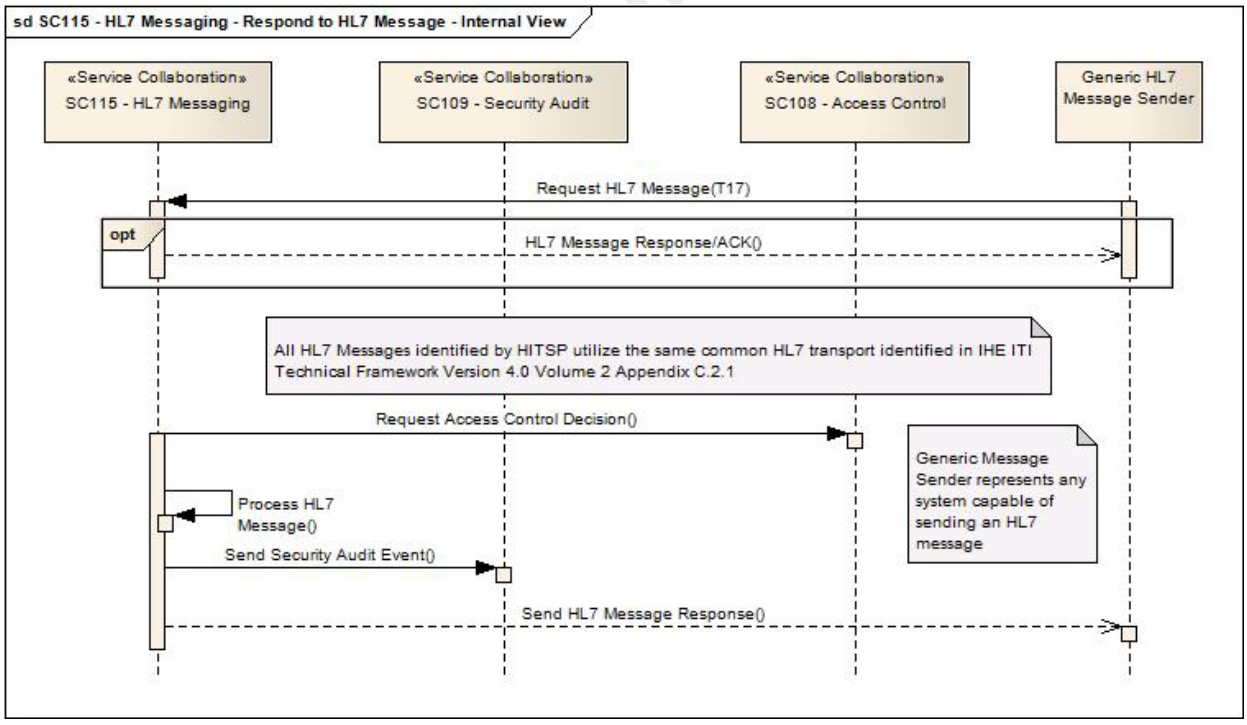
Step Number	Uses SC, T, TP or C	Interface	Purpose
1	HITSP/SC108 - Access Control	Request Access Control Decision	To ensure that the user of this Service Collaboration has the authorization to send the identified HL7 Message to the identified endpoint
2	HITSP/T17 - Secured Communication Channel	Secure Node	To open a secured communication channel to the identified endpoint to transmit clinical data
3	HL7 Message[1]		To deliver the message and receive back any response
4	HITSP/SC109 - Security Audit	Send Security Audit Event	To record the success or failure of the interface

Table 1-5 Request HL7 Message – Post-conditions

Post-condition	Uses SC, T, TP or C	Interface	Purpose
None			

1.4.2 INTERFACE: RESPOND TO HL7 MESSAGE CAPABILITY

Figure 1-3 Respond to HL7 Message Internal View



[1] All HL7 Messages identified by HITSP utilize the same common HL7 transport identified in IHE ITI Technical Framework Version 4.0 or later, Appendix C.2.1

1.4.2.1 SEQUENCE DETAILS

Table 1-6 Respond to HL7 Message – Pre-conditions

Pre-condition	Uses SC, T, TP or C	Interface	Purpose
None			

Table 1-7 Respond to HL7 Message – Sequence of Constructs

Step Number	Uses SC, T, TP or C	Interface	Purpose
1	HITSP/T17 - Secured Communication Channel	Secure Node	To receive a secured communication channel for the HL7 message
2	HL7 Messaging[2]	Depends on payload.	Receive the HL7 Message
3	HITSP/SC108 - Access Control	Request Access Control Decision	To ensure that the system that has connected has the authorization for the purpose of the message
4	n/a (loopback)	Internal Processing	If authorized process the message as defined by the message type
5	HITSP/SC109 - Security Audit	Send Security Audit Event	To record the success or failure of the HL7 message
6	HL7 Messaging[3]	Depends on payload	Return the appropriate response according to authorization and the HL7 message request

Table 1-8 Respond to HL7 Message – Post-conditions

Post-condition	Uses SC, T, TP or C	Interface	Purpose
None			

[2] All HL7 Messages identified by HITSP utilize the same common HL7 transport identified in IHE ITI Technical Framework Version 4.0 or later, Appendix C.2.1

[3] All HL7 Messages identified by HITSP utilize the same common HL7 transport identified in IHE ITI Technical Framework Version 4.0 or later, Appendix C.2.1

2.0 DOCUMENT UPDATES

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

2.1 JUNE 30, 2009

No changes. This is the first published version of the document.

2.2 JULY 8, 2009

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

2.3 JANUARY 18, 2010

Editorial updates to text and diagrams to:

- Explain the Generic HL7 Message Sender and Generic HL7 Message Receiver as being virtual interfaces built off of the common HL7 MLLP transport profile found in IHE ITI TF Appendix C.2.1
- Correct footnotes to include the Appendix C.2.1
- Change the diagrams to use “HL7 Message Request” and “HL7 Message Response/ACK” to more completely support “No-ack”, “Ack”, and “Response”
- Updated document to HITSP Service Collaboration Template Version 1.0

2.4 JANUARY 25, 2010

Upon approval by the HITSP Panel on January 25, 2010, this document is now Released for Implementation.