January 25, 2010
Version 1.1

HITSP Access Control Service Collaboration

HITSP/SC108

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

COPYRIGHT NOTICE

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

1.1 SERVICE COLLABORATION OVERVIEW AND SCOPE

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. An example of this is a functional role that has the permission to perform an act (e.g., consumer updating a Personal Health Record (PHR)). In an emergency, this construct must support the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents. This Service Collaboration utilizes the following constructs:

- HITSP/T17 Secured Communication Channel and HITSP/C19 Entity Identity Assertion as pre-conditions
- HITSP/TP20 Access Control
- HITSP/TP30 Manage Consent Directives

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.

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

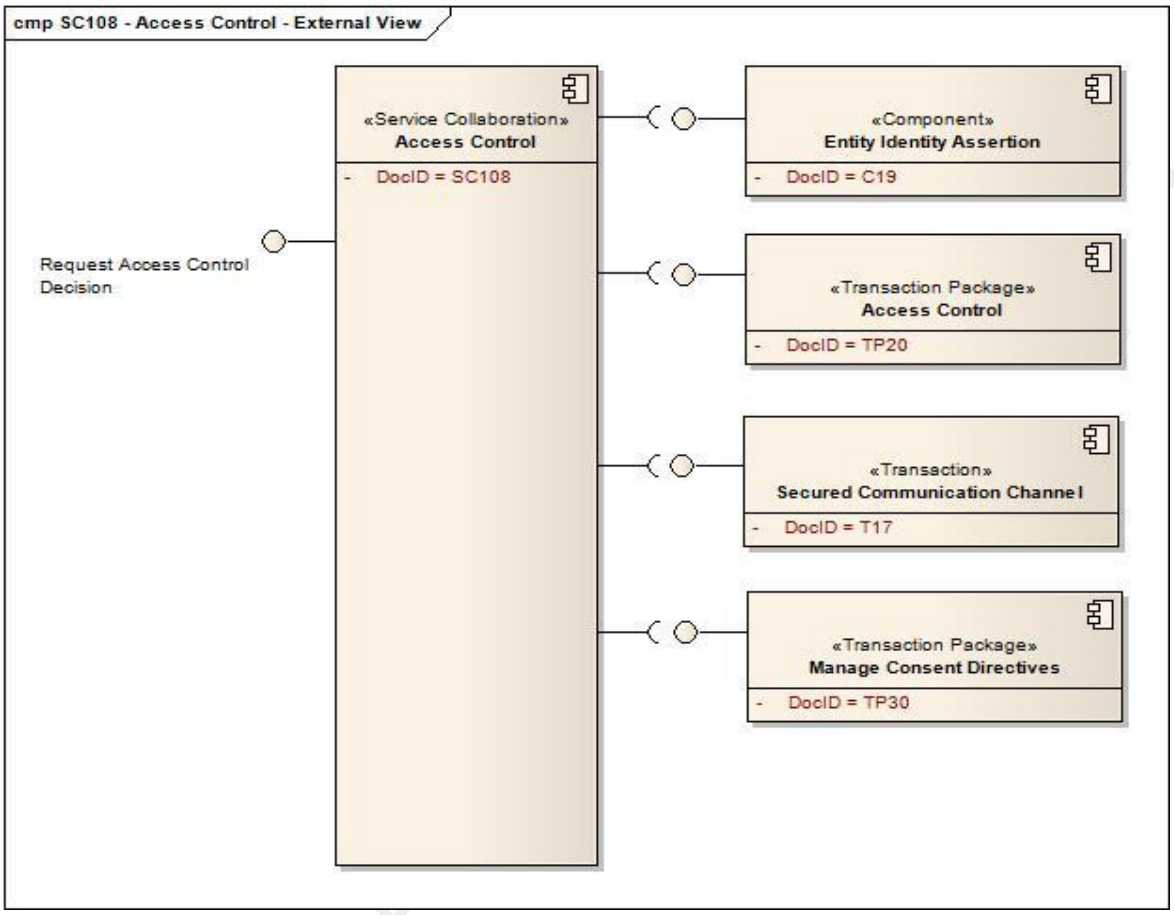
Table 1-1 Service Collaboration Transactions and Data

Service Collaboration	Service Collaboration Description	Interface	Interface Optionality
HITSP/SC108	Provides mechanism for an access control decision to be made	Request access control decision	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 Access Control External View Diagram



1.3.1 SERVICE COLLABORATION SOURCE CONSTRUCTS

Table 1-2 List of Access Control Constructs

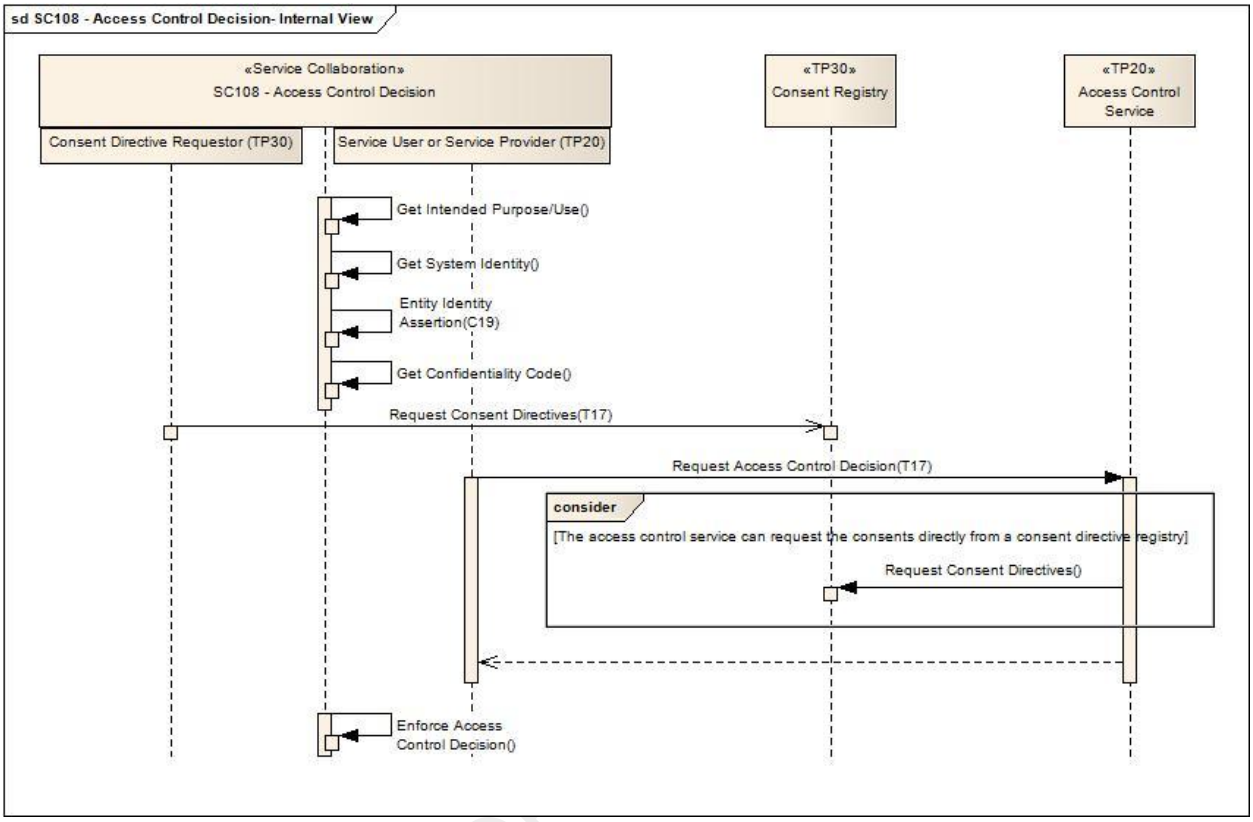
Construct	Description
HITSP/C19 - Entity Identity Assertion	The HITSP Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this Component is the validation and assertion of a consumer logging on to a Personal Health Record (PHR) system
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
HITSP/TP20 - Access Control	The HITSP Access Control Transaction Package 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. An example of this is a functional role that has the permission to perform an act (e.g., consumer updating a Personal Health Record (PHR). In an emergency, this construct must support the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents
HITSP/TP30 - Manage Consent Directives	The HITSP Manage Consent Directives Transaction Package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use or disclose individually identifiable health information (IIHI), and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13 - Manage Sharing of Documents

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

There is one example diagram included 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.

1.4.1 INTERFACE: REQUEST ACCESS CONTROL DECISION

Figure 1-2 Request Access Control Decision Internal View Diagram



1.4.1.1 SEQUENCE DETAILS

Table 1-3 Request Access Control Decision – Pre-conditions

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

Table 1-4 Request Access Control Decision – Sequence of Constructs[1]

Step Number	Uses SC, T, TP or C	Interface2	Purpose
1	None	None	Get the intended purpose of the request
2	None	None	Get the identity of the system requesting the access control decision
3	HITSP/C19 - Entity Identity Assertion	Content Consumer	Retrieve the identity attributes about the entity requesting the access control decision
4	HITSP/TP30 - Manage Consent Directives	Consent Directive Requestor	Retrieve appropriate consent attributes
5	None	None	Get the confidentiality code of the object for which access is being requested

[1] Note the access control service can request the consents directly from a consent directive registry.

[2] Steps that do not list specific constructs or interfaces are internal to the HITSP/SC108 Access Control and do not reference an interface within an underlying construct. This is considered a loopback.

Step Number	Uses SC, T, TP or C	Interface2	Purpose
6	HITSP/T17 - Secured Communication Channel	Secure Node	A secure communications channel must be open in order to protect the authenticity, confidentiality and integrity of the information being transmitted
7	HITSP/TP20 - Access Control	Service User or Service Provider	Request an access control decision from the Access Control Service, providing it with all of the attributes collected in steps 1-5
8	None	None	Enforce the access control decision. (e.g.: Grant or deny access.)

Table 1-5 Request Access Control Decision – Post-conditions

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

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 cleanup: The interface name “Request Access Control Decision” was not used consistently, and represented HITSP/C19 and HITSP/T17 in the same way done in other SC.

Sequence Tables and Sequence Diagrams updated for consistency and accuracy

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.