July 8, 2009
Version 1.0

HITSP Security Audit Service Collaboration

HITSP/SC109

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security, Privacy and Infrastructure Tiger Team

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

COPYRIGHT NOTICE

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

1.1 SERVICE COLLABORATION CONTEXT OVERVIEW AND SCOPE

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. This Service Collaboration utilizes the following constructs:

- HITSP/T15 Collect and Communicate Security Audit Trail
- HITSP/T16 Consistent Time

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 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

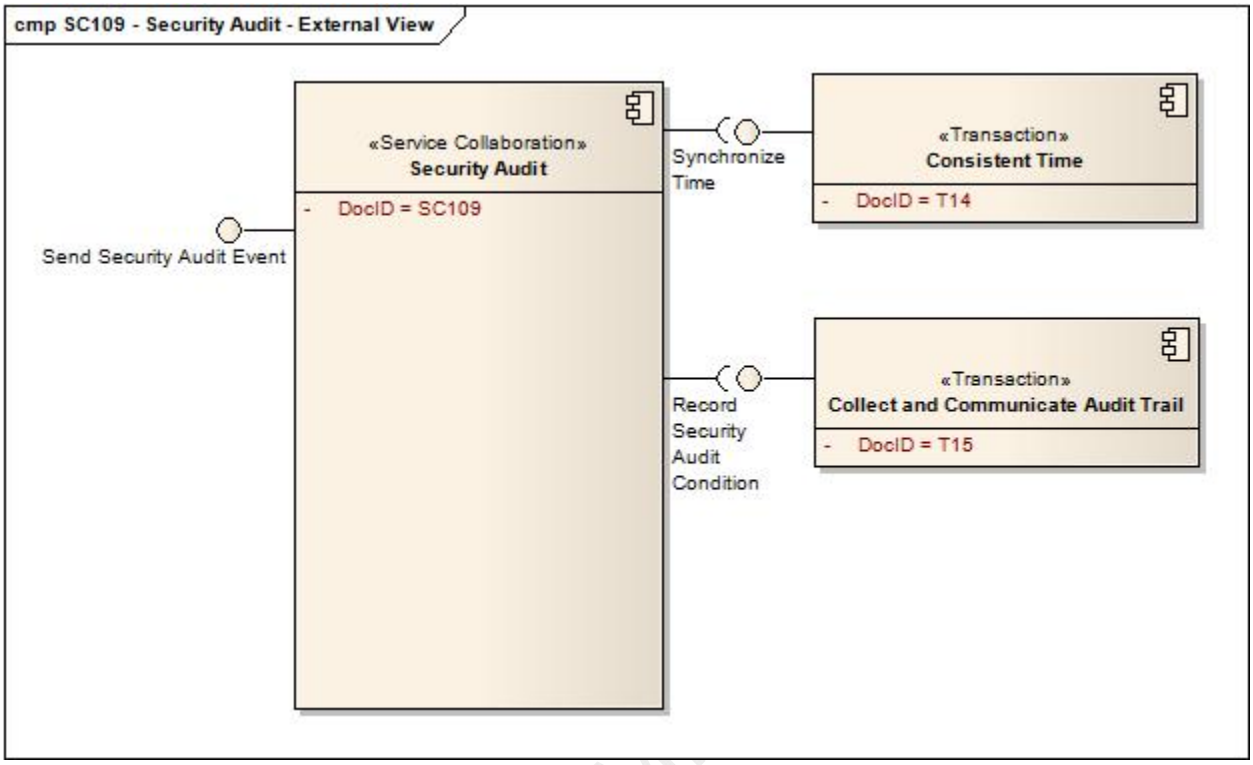
Service Collaboration	Service Collaboration Description	Interface	Interface Optionality[1]
HITSP/SC109	Provides the mechanism to record security audit events	Send Security Audit Event	R

1.3 EXTERNAL VIEW (i.e.,"black 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] Optionality = "R" for Required, "R2" for Required if Known or "O" for Optional, or "C" for Conditional

Figure 1-1 Security Audit External View Diagram



1.3.1 SERVICE COLLABORATION SOURCE CONSTRUCTS

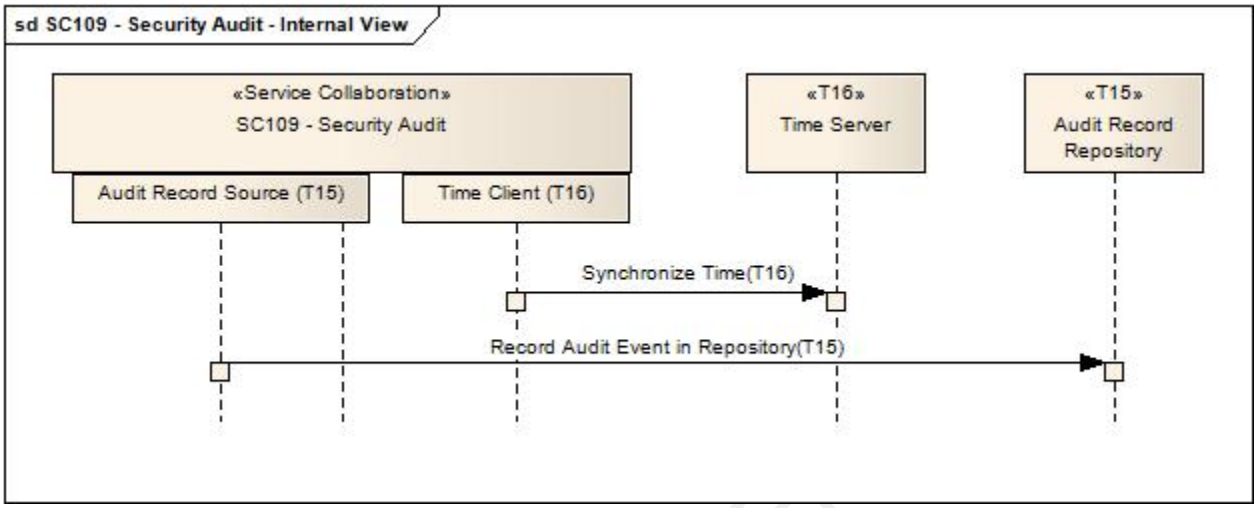
Table 1-2 List of Constructs

Construct	Description
HITSP/T15 - Collect and Communicate Security Audit Trail	The Collect and Communicate Security Audit Trail Transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. This document describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed
HITSP/T16 - Consistent Time	The Consistent Time Transaction provides a mechanism to ensure that all of the entities that are communicating within the network have synchronized system clocks

1.4 INTERNAL VIEW DIAGRAM WITH SEQUENCING (i.e., “white box” diagram)

1.4.1 INTERFACE: SEND SECURITY AUDIT EVENT

Figure 1-2 Send Security Audit Internal View



1.4.1.1 SEQUENCE DETAILS

Table 1-3 Send Security Audit Event – Pre-conditions

Pre-conditions	Uses SC, T, TP or C	Interface	Purpose
Time has been synchronized	HITSP/T16 - Consistent Time	Time Client	To synchronize time with well known time source

Table 1-4 Send Security Audit Event – Sequence of Constructs

Step Number	Uses SC, T, TP or C	Interface[2]	Purpose
1	HITSP/T15 - Collect and Communicate Security Audit Trail	Audit Record Source	Record audit event in the repository

Table 1-5 Send Security Audit Event – Post-conditions

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

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

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.