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

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Description of Change</th>
<th>Name of Author</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Tiger Team</td>
<td>June 30, 2009</td>
</tr>
<tr>
<td>1.0</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Tiger Team</td>
<td>July 8, 2009</td>
</tr>
</tbody>
</table>

COPYRIGHT NOTICE

© 2009 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI’s copyright is clearly noted.
# Table of Contents

1.0 **Introduction** .................................................................................. 5
  1.1 Service Collaboration Context Overview and Scope .................. 5
  1.2 Service Collaboration Invocation ............................................... 5
  1.3 External View (i.e., "black box" diagram) ................................... 5
    1.3.1 Service Collaboration Source Constructs .......................... 6
  1.4 Internal View Diagram with Sequencing (i.e., "white box" diagram) ................................. 7
    1.4.1 Interface: Send Security Audit Event ................................. 7
    1.4.1.1 Sequence Details ..................................................... 7

2.0 **Document Updates** ....................................................................... 8
  2.1 June 30, 2009 .................................................................................. 8
  2.2 July 8, 2009 .................................................................................... 8
FIGURES AND TABLES

Figure 1-1 Security Audit External View Diagram........................................................................... 6
Figure 1-2 Send Security Audit Internal View .................................................................................. 7

Table 1-1 Service Collaboration Transactions and Data................................................................. 5
Table 1-2 List of Constructs ............................................................................................................. 6
Table 1-3 Send Security Audit Event – Pre-conditions .................................................................. 7
Table 1-4 Send Security Audit Event – Sequence of Constructs ....................................................... 7
Table 1-5 Send Security Audit Event – Post-conditions .................................................................. 7
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

<table>
<thead>
<tr>
<th>Service Collaboration</th>
<th>Service Collaboration Description</th>
<th>Interface</th>
<th>Interface Optionality¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>HITSP/SC109</td>
<td>Provides the mechanism to record security audit events</td>
<td>Send Security Audit Event</td>
<td>R</td>
</tr>
</tbody>
</table>

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
1.3.1 SERVICE COLLABORATION SOURCE CONSTRUCTS

Table 1-2 List of Constructs

<table>
<thead>
<tr>
<th>Construct</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HITSP/T15 - Collect and Communicate Security Audit Trail</td>
<td>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.</td>
</tr>
<tr>
<td>HITSP/T16 - Consistent Time</td>
<td>The Consistent Time Transaction provides a mechanism to ensure that all of the entities that are communicating within the network have synchronized system clocks.</td>
</tr>
</tbody>
</table>
1.4 INTERNAL VIEW DIAGRAM WITH SEQUENCING (i.e., “white box” diagram)

1.4.1 INTERFACE: SEND SECURITY AUDIT EVENT

![Diagram of Send Security Audit Internal View]

1.4.1.1 SEQUENCE DETAILS

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

<table>
<thead>
<tr>
<th>Pre-conditions</th>
<th>Uses SC, T, TP or C</th>
<th>Interface</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time has been synchronized</td>
<td>HITSP/T16 - Consistent Time</td>
<td>Time Client</td>
<td>To synchronize time with well known time source</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step Number</th>
<th>Uses SC, T, TP or C</th>
<th>Interface</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HITSP/T15 - Collect and Communicate Security Audit Trail</td>
<td>Audit Record Source</td>
<td>Record audit event in the repository</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Post-conditions</th>
<th>Uses SC, T, TP or C</th>
<th>Interface</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.