Digital Insight – SAML Integration Guide

Integration Guide

Revision 05/18/2015

© 2015
Table of Contents
Introduction ......................................................................................................................... 4
Content Integration Options ................................................................................................. 4
  Online and Mobile Pages and Online Widgets ................................................................. 4
    Online Banking Page ........................................................................................................ 4
    Mobile Page .................................................................................................................... 5
    Home Page Widget .......................................................................................................... 5
  Stand Alone Application SSO ........................................................................................... 5
SAML integration - Overview .............................................................................................. 5
  Identity ............................................................................................................................... 6
  Security ............................................................................................................................... 6
SAML 2.0 IdP Initiated Web Browser SSO Flow ................................................................. 7
1.1 Step 1 – User logs in and selects to SSO to partner web site ........................................ 8
1.2 Step 2 – Create SAML Assertion and route to Partner SAML Gateway ...................... 8
1.3 Step 3 – Process SAML Assertion and create web application security session ........... 8
SAML Consumer Options .................................................................................................. 10
Integration Checklist .......................................................................................................... 10
  Partner provides to Digital Insight: .................................................................................. 10
  Digital Insight provides to Partner: .................................................................................. 10
System requirements: .......................................................................................................... 11
Session Management ........................................................................................................... 11
Data Exchange ................................................................................................................... 11
User Accounts Data ............................................................................................................ 12
Using KEEP_ALIVE_URL ......................................................................................................................... 13
Logout Processing ................................................................................................................................. 13
Introduction

This document provides technical specifications for software developers at any Financial Institution or Third Party vendor, who are integrating custom content into their online and mobile applications with Digital Insight Products. Integration with Digital Insight’s Federation Gateway Services requires that the partner adhere to SAML (Security Assertion Markup Language) SSO (single signon) standards. This document describes the content integration options, as well as provides Digital Insight SAML assertion data and guidelines. This document does not supersede OASIS standards specifications. For more information about the SAML specification, please refer to www.oasis-open.org

Content Integration Options

**Online and Mobile Pages and Online Widgets**

Using SAML integration, the third party can develop custom feature pages or widgets specifically designed to run within the Digital Insight Online Banking environment. In general, this kind of integrations dictates that:

- The look and feel of the third party feature page or widget adhere to standards specified for Online Banking.
- The third party app should use the session keep-alive URL to make sure the Online Banking session does not timeout while the end user is engaged with the third party app.

UI style guides are available to assist developers in creating applications with a visual look and feel that matches online and mobile banking.

The custom feature pages or widgets are web applications hosted at the third party or FI. Any environment that can be used to build and host web applications can be used by the third party or FI.

**Online Banking Page**
Online banking SSO pages are launched when an end user clicks on a navigation item configured for the SSO. Navigation entries can be managed by the FI in the Admin Platform. An SSO navigation entry can be placed anywhere in the navigation structure. Every time an end user clicks on an SSO navigation link, the system will initiate a fresh SAML SSO sequence. There is no attempt made to cache earlier SSO session information. SSO pages are loaded by online banking in the main frame below the navigation area, and all content in the frame must be provided by the custom web application.

**Mobile Page**

Mobile banking SSO pages are launched when an end user clicks on a navigation item configured for the SSO. These navigation entries are on the ‘More’ page in the mobile application. ‘More’ page navigation entries can be managed by the FI in the Admin Platform. Every time an end user clicks on an SSO navigation link, the system will initiate a fresh SAML SSO sequence. There is no attempt made to cache earlier SSO session information. SSO pages are loaded by the mobile application in a web view, and all content in the view must be provided by the custom web application.

**Home Page Widget**

An SSO configured for a widget is launched when the enclosing page is loaded. So, an SSO configured for a widget on the home page will be launched every time the home page is loaded for an end user. When an SSO is built for use with a home page widget, it must be designed to support high volume since it will be loaded every time a user logs in. Every time the page loads, a new SAML SSO sequence will be initiated, there is no attempt to try and reuse earlier session information. The widget provides an empty iFrame, and all content for it must be provided by the SSO web application.

**Stand Alone Application SSO**

The other mode of integration that can be used with SAML is to provide SSO (Single Signon) to existing applications. This mode is commonly used when a need exists to provide a simple integration between Online Banking and the third party web app.

**SAML integration - Overview**

As an industry standard, SAML is the integration model that Digital Insight supports for securely passing authenticated user data from one application to another. SAML exchanges authentication and authorization between Digital Insight – the “identity provider” and the Partner – the “Service Provider”. This enables users to access Partner applications from the Digital Insight banking platform without having to sign in a second time.
Digital Insight currently supports the several SAML Profiles, while standardizing on the preferred SAML 2.0 POST Profile.

**Identity**

With respect to SSO SAML, Digital Insight is the Identity Provider (IdP) and the Partner is the Service Provider (SP). Consistent with the SAML specification, Digital Insight provides a unique and immutable (never changing) identity for the customer.

**Security**

The following requirements are consistent with the SAML specification and ensure full security during the SSO. The SAML interactions must confirm to the SAML specifications.

- SAML Post Profile 2.0 assertions must be encrypted in order to not leave PII data in plaintext on the browser
- SAML Post Profile 2.0 assertions must be signed
- All network traffic must go over SSL
- Public keys are exchanged across companies to support digital signing of the SAML assertions and the encryption of the sensitive attributes. Digital Insight requires certificates for production environments from trusted CAs (Certificate Authority). A self-signed certificate may be used in staging/test environments.
**SAML 2.0 IdP Initiated Web Browser SSO Flow**

1) Logged In User selects SSO
2) Send SAML Assertion
3) Validate SAML, create security session, and return content

**Description:** An online banking user selects an FI or 3rd Party application menu item from within online banking.

<table>
<thead>
<tr>
<th>Federation Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application</td>
<td>An online banking user selects an FI or 3rd Party application menu item from within online banking.</td>
</tr>
</tbody>
</table>
The goal is for a user that is logged in to online banking to access protected content from an external partner’s web application without having to explicitly login to the partner site. We utilize the SAML 2.0 Web Browser SSO Profile to federate the user’s Digital Insight identity securely to the partner. Upon validation of the SAML Assertion, the partner web site will establish an appropriate security session for that user in order for them to access its protected content. The use case begins with an un-authenticated user logging in to online banking.

1.1 **Step 1 – User logs in and selects to SSO to partner web site**
A user logs into Digital Insight’s platform and selects a feature to SSO to a partner web site. This triggers the Digital Insight platform to initiate the Federated SSO.

1.2 **Step 2 – Create SAML Assertion and route to Partner SAML Gateway**
Digital Insight SAML Gateway will generate a SAML Assertion and send it via a browser directed HTTP POST to the Partner SAML Gateway service. A browser directed POST is accomplished by returning a response back to the browser that contains Javascript that will immediately execute and auto-submit an HTTP POST with the SAML.

1.3 **Step 3 – Process SAML Assertion and create web application security session**
The Partner SAML Gateway first validates the SAML Assertion and then establishes an internal security session for the user at their site. The partner will also need to link the user pseudonym value passed as part of the SAML Assertion to its target user identity. The linking method should be defined mutually between Digital Insight and the Partner. The Partner system can then either redirect the browser to the protected web page or can just return the content directly in the response. The details of that will vary by Partner web application.
**SAML Consumer Options**

The following information is being provided as suggestions for partners to consider for SAML solutions. It is not meant to be a comprehensive list of alternatives but rather it is meant to give some basic direction. SAML is an industry standard for secure identity forwarding. Information included in this document is not meant to supersede SAML specifications, which can be found at [www.oasis.org](http://www.oasis.org).

The task of creating SAML gateway can be complex and daunting. It is highly recommended to utilize a 3rd party solution (e.g. PingIdentity, Oracle, Microsoft, Oracle or at a minimum an open source library (e.g. OpenSAML (Java implementation), ZXID (C implementation), SimpleSAMLphp (PHP implementation)...).

http://en.wikipedia.org/wiki/SAML_2.0

**Integration Checklist**

**Partner provides to Digital Insight:**

- SAML Assertion Consumer Service POST URL. (This URL must support HTTPS on port 443).
- An X509 Certificate from a trusted CA. This will be used for all connections when production (real user data) is being passed. Digital Insight also uses staging/test environments when testing, and these non-production environment will also require a certificate. The same certificate as is used in production may be used in test, or the partner may provide another certificate, which may be self-signed if desired. Digital Insight will use the certificate in each case for encrypting SAML assertions.
- Service Provider entity ID.

**Digital Insight provides to Partner:**

- Optional: Federation Registration meta data
- X509 Certificate. Partner will use the public key in that certificate to verify SAML signature. Note that demonstrating correct signature verification processing is a requirement for certification with Digital Insight.
- Identity Provider Entity ID
System requirements:
- System time of the partner SAML server is accurate (updated through time protocol) – this will ensure correct SAML semantics for timestamp validation.
- Security algorithms for encryption and digital signature:
  - Supported digital signature algorithms: RSA SHA1, RSA SHA256, RSA SHA384, RSA SHA512.
  - Recommended digital signature algorithm: RSA SHA256.
  - Supported encryption algorithms: AES-128, AES-256, Triple DES.
  - Recommended encryption algorithm: AES-128.

Session Management
The Digital Insight platform supports keep-alive messages from the 3rd party app through use of a keep-alive URL which is provided as a SAML attribute.

The third party app can receive the online banking session Id as part of the SAML payload if desired. The session Id can be used to tie activity in the third party app to activity recorded by online banking. The online banking activity records also include the session Id.

Data Exchange
The fields below are included as attributes in the SAML assertion. Note that the entire assertion (all attributes as one block) is encrypted.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Description/ Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FI_ID</td>
<td>Alphanumeric</td>
<td>This field is the DI internal ID for the subject Financial Institution.</td>
</tr>
<tr>
<td>USER_ID</td>
<td>Alphanumeric</td>
<td>The ID of the subject user on the Financial Institution’s host processing system.</td>
</tr>
<tr>
<td>USER_ACCOUNTS</td>
<td>XML Document</td>
<td>An XML document containing the list of accounts, and associated account nickname, for the user. See below for details of the data included. Note</td>
</tr>
<tr>
<td><strong>KEEP_ALIVE_URL</strong></td>
<td>URL</td>
<td>This URL can be used by the FI or 3rd party app to keep the main online banking session alive while the end user is interacting with the 3rd party app. See below for an example of how to use the URL in an application.</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>XML_DATA</strong></td>
<td>XML Document</td>
<td>This attribute is optional, and the structure of the document is determined during development and certification jointly by the third party and DI. The document can contain any additional user data needed for the functioning of the application that is not already provided by the standard attributes listed above. Note that this is base64 encoded and must be decoded by the third party.</td>
</tr>
<tr>
<td><strong>SESSION_ID</strong></td>
<td>Alphanumeric</td>
<td>The online banking session Id for the logged in user. This attribute is optional.</td>
</tr>
</tbody>
</table>

**User Accounts Data**

Below is a sample output of the USER_ACCOUNTS XML. The xsd describing the output can be provided on request.

```xml
<ns7:Accounts xmlns="http://schema.intuit.com/domain/banking/financialInfo/v2"
  xmlns:ns2="http://schema.intuit.com/domain/banking/financialInstitution/v2"
  xmlns:ns6="http://schema.intuit.com/domain/banking/notification/v2"
  xmlns:ns7=http://schema.intuit.com/domain/banking/account/v2">
  <ns7:account xsi:type="ns7:DepositAccount" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <ns7:id>vWlYcq3tIA3-BtsryKXRxVfcOd5tt9V152FCw7Gf5eg</ns7:id>
    <ns7:nickName>Checking</ns7:nickName>
    <ns7:accountNumber>
      <ns7:hostValue>XXX4444</ns7:hostValue>
      <ns7:displayValue>XXX4444</ns7:displayValue>
      <ns7:billPayValue>0XXX4444</ns7:billPayValue>
      <ns7:pfmValue>XXX4444</ns7:pfmValue>
  </ns7:account>
</ns7:Accounts>
```
Using **KEEP_ALIVE_URL**

The keep-alive URL needs to be used from the client side (within the browser) of the third party application to keep the online banking session active while activity is occurring in the third party application. Here is some example code to implement this:

```html
<script> (function (d) { var iframe = d.body.appendChild(d.createElement('iframe')), doc = iframe.contentWindow.document; iframe.style.cssText = "display: none;"; doc.open().write('<body onload="setTimeout(function() { window.location="$KEEP_ALIVE_URL" }, 0);">'); doc.close(); })(document); </script>
```

**Logout Processing**

A SAML SSO endpoint can be configured to receive a logout message whenever a user logs out of online banking. The message will be delivered from the end user’s browser as part of the logout process. Logout processing is only supported for online page and widget, it is not supported for mobile SSO sessions. Specific details about the logout message are as follows:

- The URL for the message is pre-configured and must be provided by the third party
- The request can only be sent as a GET.
- The URL will include the session Id as a query parameter added dynamically before sending the request.
The third party app should be programmed to handle the case of the logout message being posted for a session that has already timed out. This can occur if the end user spends a long time in the online banking session after having initiated the SSO application.