Setting up SAML-based Web SSO for a New Application

1/28/18

Contents

- Overview
- Technical Requirements
  - SP software
  - SP-specific information needed by NYU
  - IdP Metadata and related information needed by the SP Team
- Functional Notes
  - Authentication vs Authorization
  - Logout
  - Session management
  - Protecting different content areas with different session settings
  - Attributes available from the IdP
- Go-Live Checklist
- Other Documents & Contact Information

Overview

The NYU Login (SSO) service uses Shibboleth as its central software component. Shibboleth is a brand-name implementation of SAML, the XML-based open standard for exchanging authentication and authorization information. Originally developed for use in higher education by Internet2, a not-for-profit United States networking consortium led by members from the research and education communities, Shibboleth has since 2000 been among the world’s most widely deployed federated identity and SSO solutions. Shibboleth products are now developed and supported by the nonprofit Shibboleth Consortium¹ with members and users worldwide.

Web applications that are integrated into the NYU SSO infrastructure do not themselves need to use Shibboleth software specifically, but they do need to use either Shibboleth, another SAML-based product, or have built-in SAML capabilities.

Technical Requirements

NYU Single Sign-On uses the industry standard SAML protocol for integration between the central identity provider servers and application servers. More specifically:

- SAML version 2 is required, SAML v1.1 is not supported.
- The SP must support the authentication request protocol and send an <AuthnRequest> message, but IDP Initiated SSO (Unsolicited) may be used.
- The SP must send the <AuthnRequest> message using the HTTP-Redirect binding.
- The SP must accept the assertion from the IdP via the web browser and the HTTP-POST binding.

SP software

The SP web application must itself support SAML-based SSO integration, or must utilize a web server (e.g. Apache) configured with an authentication module providing SAML integration. For java-based applications

¹ http://shibboleth.net/
using a Java application server (e.g. Tomcat) it is common to set up an HTTP server such as Apache acting as a reverse proxy in front of the application server so that the Shibboleth Native SP for Apache can be deployed and used to manage the SAML interactions. Please consult your web application's technical documentation for information relating to SSO integration capabilities.

Recommended for web applications using the Apache web server is the Shibboleth Service Provider implementation available from the Shibboleth Consortium. For more information see the document Introduction to the Shibboleth SP for Application Managers and Developers at NYU.

**SP-specific information needed by NYU**

For integration purposes, the SP Team must provide SAML metadata specific to the SP, including the X.509 certificate used by the SP for encryption and digital signing. Since the IdP sends encrypted assertions to the SP it needs to have access to the public X.509 certificate for the SP. Since, as a rule, integration work will first be conducted in a test or development environment, separate metadata will be needed for both a test instance of the SP and for the production instance of the SP.

For production use, if the domain name for the destination site is of the form some_domain_name@nyu.edu, an NYU-provided InCommon certificate with a duration of five years is recommended over a self-signed certificate. If the domain is not nyu.edu, we suggest that the vendor supply a commercial-grade certificate as opposed to a self-signed certificate. For more information on certificates, please see the following Knowledge Base article, Requesting and managing SSL certificates at NYU, or visit https://www.nyu.edu/it/certificates/. A certificate must be signed with SHA256 and must have at least 2048 bits. For a self-signed certificate, the following command is an example of how to generate a private key and certificate meeting these requirements:

$ openssl req x509 sha256 newkey rsa:2048 keyout key.pem out cert.pem days XXXX

SP metadata may be provided via email; alternatively, in some cases, a URL may be provided allowing the IdP-Team to retrieve metadata for the SP. The IdP-Team can download the metadata from the InCommon Federation's metadata repository for vendors who have joined InCommon Federation.

The following SP information will be needed:

<table>
<thead>
<tr>
<th>SP Entity ID</th>
<th>This is typically a simple URI of the form &quot;<a href="http://yoursite.example.com">http://yoursite.example.com</a>&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP metadata</td>
<td>Information in XML describing details about the SP; the most common elements included would be present in the following order:  <a href="">md:KeyDescriptor</a> (can be omitted, but rarely)  <a href="">md:SingleLogoutService</a> (if any)  <a href="">md:NameIDFormat</a> (if any)  <a href="">md:AssertionConsumerService</a> (always at least one)  <a href="">md:AttributeConsumingService</a> (rare today, but good practice to include)</td>
</tr>
</tbody>
</table>

2 When the Shibboleth SP software is used, the self-signed certificate automatically generated during installation can be used for development/testing purposes.

3 [http://incommonfederation.org](http://incommonfederation.org)
The following questions will be need to be answered:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is SSO to be IdP-initiated or SP-initiated?</td>
<td>Most commonly, SSO is SP-initiated.</td>
</tr>
<tr>
<td>Needed attributes from NYU IdP</td>
<td>For example, EPPN (<a href="mailto:NetID@nyu.edu">NetID@nyu.edu</a>), firstname, lastname, etc</td>
</tr>
<tr>
<td>Will SAML requests be transmitted over HTTPS?</td>
<td>The NYU standard is to use HTTPS.</td>
</tr>
<tr>
<td>Are SAML assertions to be signed and/or encrypted?</td>
<td>The NYU default configuration is to not sign responses, to always sign assertions, to encrypt assertions conditionally (i.e. when compatible with the SP's capabilities) and to not encrypt NameIDs. This can be adjusted per SP.</td>
</tr>
<tr>
<td>Are SAML requests to be signed and/or encrypted?</td>
<td>The NYU standard is to neither sign nor encrypt SAML requests (the overall envelope containing SAML assertions).</td>
</tr>
<tr>
<td>QA URL for end-users to access the site</td>
<td>Provide this on questionnaire</td>
</tr>
<tr>
<td>PRODUCTION URL for end-users to access the site</td>
<td>Provide this on questionnaire</td>
</tr>
<tr>
<td>Do you need a test NetID?</td>
<td>If so, complete Test NetID request form</td>
</tr>
</tbody>
</table>

**IdP Metadata and related information needed by the SP Team**

NYU’s unique identifier (and computer username) is called the NetID. Our eduPersonPrincipalName is of the form: NetID@nyu.edu (example: abc1234@nyu.edu)

User principal name will be the eduPersonPrincipalName transmitted as the SAMLv2 NameID. Additional representations of the user may be presented via the attribute field.

QA IdP EntityID: https://shibbolethqa.es.its.nyu.edu/idp/shibboleth
QA IdP metadata can be found at: https://shibbolethqa.es.its.nyu.edu/idp/shibboleth
QA logout URL is: https://shibbolethqa.es.its.nyu.edu/idp/profile/Logout

Production IdP EntityID: urn:mace:incommon:nyu.edu
Production IdP metadata can be found at: http://shibboleth.nyu.edu/idp/shibboleth
Production logout URL is: https://shibboleth.nyu.edu/idp/profile/Logout

---

4 Note: if there are two certificates in this data, use the second certificate.
**Functional Notes**

**Authentication vs Authorization**

The NYU Login (SSO) service fundamentally provides *authentication* capabilities: NetID/password authentication. *Authorization* is the responsibility of the service provider and, while SAML-based SSO systems may be designed to provide authorization information, the NYU Login (SSO) service does this only to the extent that eduPersonEntitlement and eduPersonAffiliation information are useful to an SP for this function.

**Logout**

All SPs should prominently display a "Logout" link and redirect the user to the IdP logout page:

https://shibboleth.nyu.edu/idp/profile/Logout

where the IdP session will be terminated and a message to the user is presented, indicating that they may not be "logged out" of all applications they've been using, and that closing or exiting their browser is advised.

The following sequence of events, when an end-user hits the "Logout" link, is strongly recommended. The SP should perform these actions, in this order:

1. Any local application/session cleanup (e.g. saving files)
2. Terminate application session (if any)
3. Terminate the SP's single sign-on session
4. Redirect the user's browser to the central IdP logout page

(https://shibboleth.nyu.edu/idp/profile/Logout)

For example, using the Shibboleth SP, steps 3/4 can be accomplished by a single browser redirect to:

https://YOURSITE.nyu.edu/Shibboleth.sso/Logout&return=https%3A//shibboleth.nyu.edu/idp/profile/Logout

If the SP does *not* redirect the end-user's browser to the central IdP logout page, then it must display information stating that the browser must be “closed out” or exited to completely log out from all SSO-integrated applications.

**Session management**

Session management in an SSO environment occurs at two levels: at the IdP and at the SP. The specific settings used impact how often a person is prompted to login (entering their NetID and password).

At the IdP we set a maximum IdP session length of 10 hours. This means

- if a person logs into one application and then goes to another application within 10 hours, they will not need to reauthenticate with NetID/password
- if they go to another application, however, *after* 10 hours, they will need to reauthenticate
- if any application sends the person's browser to the IdP "logout" page, then the person's IdP session will be terminated; this will result in the need to reauthenticate if any SP sends the person's browser to the IdP

Each SP manages its own local sessions, quite independent of the IdP and its settings. Different applications will have different session management capabilities, and SP session settings (e.g. maximum length of an end-user's login session) are at the discretion of the SP Team.
Just as an example, the Shibboleth SP software provides three configuration settings relating to sessions:
- session lifetime = 8 hours (out of the box, adjustable)
- inactivity timeout = 1 hour (out of the box, adjustable)
- cache timeout = same as lifetime (adjustable)

Exceeding these thresholds (e.g. if idle for 2 hours and then the end-user clicks on a link within your application) will cause the user's browser to redirect back to the IdP.

To the extent that your settings are shorter than the IdP's settings, then reauthentication will not be required upon redirection to the IdP (since the IdP sessions for the end user will not have expired).

Note: an SP may force the user to reauthenticate using advanced SAML techniques; the NYU IdP supports the ForceAuthn and isPassive attributes in the authentication request.

**Protecting different content areas with different session settings**

Is it possible for specific pages within an SP to have different session settings, e.g. shorter than the default for the SP? Such a capability would have to be within the capabilities of the particular software used on the SP for SSO and session management. E.g. it is possible to do this with the Shibboleth SP software setting different session parameters for a designated set of URLs and requiring reauthentication upon access to those pages. Additional information can be found here: [https://wiki.shibboleth.net/confluence/display/SHIB2/FederatedSessionManagement](https://wiki.shibboleth.net/confluence/display/SHIB2/FederatedSessionManagement)

**Attributes available from the IdP**

At login time, information about the end user can be conveyed from the IdP to the SP.

The desired attributes need to be settled during the SSO integration process. You should only request those attributes needed by your application to function properly and provide the required user experience.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>aqe123</td>
</tr>
<tr>
<td>displayName</td>
<td>Albert Q Einstein</td>
</tr>
<tr>
<td>mail5</td>
<td><a href="mailto:aqe@nyu.edu">aqe@nyu.edu</a></td>
</tr>
<tr>
<td>NetIDEmail</td>
<td><a href="mailto:aqe@nyu.edu">aqe@nyu.edu</a></td>
</tr>
<tr>
<td>surname (also sn)</td>
<td>Einstein</td>
</tr>
<tr>
<td>givenName</td>
<td>Albert Q</td>
</tr>
<tr>
<td>NYUIdn</td>
<td>N2345789</td>
</tr>
<tr>
<td>eduPersonEntitlement</td>
<td>(rarely used)</td>
</tr>
<tr>
<td>eduPersonPrincipalName</td>
<td><a href="mailto:aqe123@nyu.edu">aqe123@nyu.edu</a></td>
</tr>
<tr>
<td>eduPersonPrimaryAffiliation</td>
<td>employee</td>
</tr>
<tr>
<td>eduPersonAffiliation</td>
<td>employee</td>
</tr>
<tr>
<td>eduPersonAffiliation</td>
<td>student</td>
</tr>
</tbody>
</table>

5 Please note, the mail attribute is not guaranteed to remain the same for an individual over time. If a unique and unchanging identifier for the individual is needed, the uid attribute (representing the person's NYU NetID) or the eduPersonPrincipalName (EPPN, representing the person's NetID@nyu.edu affiliation) should be used.
Go-Live Checklist

Please complete this checklist in advance of the agreed upon production go-live.

<table>
<thead>
<tr>
<th>Service Owner / Service Provider (SP)</th>
<th>Person Assigned</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the Project to Service Transition Checklist and Style Guide for guidance and requirements regarding Service Naming and User Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update shibboleth2.xml file by changing <code>&lt;MetadataProvider&gt;</code> element to use production IdP metadata (E.g. if using the Shibboleth SP software, update the shibboleth2.xml file, changing the <code>&lt;MetadataProvider&gt;</code> element to use production IdP metadata.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update shibboleth2.xml file by changing <code>entityID</code> attribute of <code>&lt;SSO&gt;</code> element to be equal to production IdP <code>entityID</code> (E.g. if using the Shibboleth SP software, update the shibboleth2.xml file, changing the <code>entityID</code> attribute of the <code>&lt;SSO&gt;</code> element to be equal to the production IdP's <code>entityID</code>).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The production IdP's <code>entityID</code> is: urn:mace:incommon:nyu.edu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide user friendly, short name (no more than 40 characters, including spaces) for login page (E.g. for the NYU's Google-based Email, the short name is &quot;NYU Google Apps&quot;).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have person ready to test when production changes have been made</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Production Go-Live must be scheduled in advance, in order to properly coordinate steps at SP and IdP. After the necessary exchange of SAML metadata, configuration and testing of SP and IdP development environments is complete, production go-live will be scheduled.

Other Documents

• SAML Integration Planning Questionnaire
• Operating Level Agreement template for NYU Login Service

Contact Information

All email communications with the IdP-Team (part of the NYU IT Identity Management group) should be sent to idm.services@nyu.edu