Shibboleth Authentication Overview

Section 1.1: Overview

This article provides information about University of Miami’s Shibboleth authentication service.

Shibboleth allows users to securely send trusted information about themselves to remote resources or applications. This information is used to authenticate and authorize users to access a particular application as well as content personalization and enabling Single Sign-on in a broad range of services from different providers or resources. This is the best option the University offers to provide Single Sign-on experience across different web applications.

For a list of LDAP user attributes, please see our complete list of attributes.

The University of Miami is a participant of the InCommon Federation. InCommon is an identity Federation serving the Higher Education community in the United States. InCommon is part of Internet2 and provides secure trust between Universities and other educational institutions. See complete list of InCommon Participants https://www.incommon.org/participants/.

If an application or external service belongs to the InCommon Federation, Shibboleth authentication is already available and there’s no need to do any further steps. Otherwise, the application or service provider will need to be integrated with our Shibboleth IdP (identity provider). This process of connecting to the Shibboleth/UM authentication service involves exchanging a file called a “metadata” (see IdP production metadata here, and test metadata here) between the service provider or SP (i.e application or resource) and our identity provider (IdP), which is our UM Single Sign-on login page. Both need to recognize and authenticate each other in order to allow the user access to the application.

We provide LDAP attributes as mentioned above as well as any other specified attributes, which require an agreement between the University of Miami and the application administrator.

For more InCommon Federation information, you may visit the InCommon website: https://www.incommon.org/.

Section 1.2: Initiating Integration and Support

UMIT provides services to support Shibboleth or SAML integrations. For new Shibboleth service providers, please contact umsso@miami.edu for further technical information on pre-requisites, recommendations, and technical instructions on how to integrate with Shibboleth.

Attributes released by default to all service providers are cn, mail, displayName, sn, givenName, employeeID, title, telephoneNumber, eduPersonPrincipalName (ePPN) and eduPersonScopedAffiliation as well as any customized attributes such as isMemberOf and affiliations.
Section 1.3: University of Miami Production Metadata

UM’s IdP entity Id: https://caneid.miami.edu/idp/shibboleth

IdP metadata location: http://caneid.miami.edu/idp/profile/Metadata/SAML

InCommon Federation metadata: http://md.incommon.org/InCommon/InCommon-metadata.xml

Section 1.4: Shibboleth Logout Recommendation

Shibboleth’s single logout (SLO) process can be tricky since various browsers work differently when the user logs out. One of the first issues with SLO is communicating to the user what will occur if they click “logout.” Users have already been taught that doing this will cause them to be logged out of the application that contained the logout button/link they used. They assume that all other applications will remain active. Therefore there must be some means to distinguish between application-level logout and SLO. Therefore the University has recommendations which will have applications redirect to a page that will prompt the user whether they would like to continue logged on to the application or whether they would like to completely logout. If the user clicks on continue with the application, he/she will be redirected to the application home page and their Single Sign-On (SSO) session will still be “on.” Otherwise, they will need to click on the choice to completely logout. If they would like to completely logout, they will be redirected to our logout page to end the SSO session. This page advises users to close their browser to avoid unauthorized access to their information.

See the University’s recommendation for login and logout.

Further Information
For a less technical overview of SSO, see Shibboleth and Single Sign-on Documentation.

References
https://wiki.shibboleth.net/confluence/display/CONCEPT/SLOIssues