Section 1.1: What is Shibboleth?

This article goes over the concept of Shibboleth at the University of Miami.

Shibboleth is a web-based single sign-on system made up of the following components:

- The **Identity Provider** (IdP) is responsible for user authentication and providing user information to the Service Provider (SP). It is located at the home organization, which is the organization maintaining the user's account.

- The **Service Provider** (SP) is responsible for protecting an online resource and consuming information from the Identity Provider (IdP). It is located at the resource organization or application.

Shibboleth allows you to log in once (for a preset period of time, which can vary from 15 minutes to 1 hour for the University) to any service integrated with Shibboleth that you are eligible to use and also have access to all other resources or applications to which you have access without having to re-enter your credentials to log in again.

For further information about Shibboleth SP and IdP, please visit Shibboleth’s Wiki: [https://wiki.shibboleth.net/confluence/display/SHIB2/Software+Concepts](https://wiki.shibboleth.net/confluence/display/SHIB2/Software+Concepts).

Section 1.2: What is Web (Passive) Single Sign-On (SSO)?

This article goes over the implementation of Single Sign-On (SSO) at the University of Miami.

Once you log into an SSO-enabled application such as UM’s Workday, CaneLink, MyUM, you will be able to conveniently access the University’s resources via the web without having to enter credentials each time for other web-based SSO applications. Hence the term “Single Sign-On.” For a complete list of SSO-enabled applications, please click here.

Section 1.3: How does it work with applications or web sites?

SSO utilizes Shibboleth, a SAML-based system which allows you to securely access sites across applications and organizations by using your University credentials. The user authenticates using the University’s login credentials and then he/she is re-directed to the application. Their access will continue until you close the browser or your session expires (depending on application, which can vary between 15 minutes to 1 hour).
**Section 1.4: How do I use SSO?**

You use your CaneID and password to login once when directed to our UM Single Sign-On login page. After logging in to one application that uses Single Sign-On (i.e MyUM, Workday), you will be able to access other applications that also use Single Sign-On as a way to authenticate. You will only be required to enter your CaneID and password credentials as usual.

We strongly recommend when accessing highly sensitive information or personal accounts, be sure to close your browser to log out of your Single Sign-On session when you are done to ensure that your information is not compromised or accessed by someone else. This will ensure that your information will remain private. If you would like to implement Web Single Sign-On, please follow these helpful technical guides for Linux or Windows operating systems. For more information, please email: umsso@miami.edu.

**Section 1.5: Is my application using the University of Miami’s Single Sign-On?**

This can be determined by looking over at the URL on the browser that starts with the link https://caneid.miami.edu/.