Single Sign-On Recommendations

Section 1.1: Recommendations

☐ **SSL-enabled application is a pre-requisite**
We need the Service Provider or application to enable SSL on their server as a pre-requisite to make sure all communication are over https instead of http.

☐ **SAML-integration**
We recommend to use SAML 2.0 in order to take advantage of Multi-factor Authentication (MFA) layer of security.

☐ **The recommended Unique Identifier is EmployeeID**
We recommend to use the EmployeeID (i.e. 500####) or ePPN (eduPrincipalPersonName) to identify the user and validate their account when they logon on. EmployeeID and ePPN will not change while an attribute such as email or caneid can change. For additional attributes, please refer to the list of attributes available from the University.

☐ **User access authorization lies within the application**
Single Sign-on will authenticate all users with a valid CaneID and password. However, the application should be able to allow or deny user access. The Shibboleth IdP can release specific customized attributes such as affiliation or Active Directory (AD) group information to service the application identify the user’s AD groups and therefore determine his or her level of access.

☐ **“No access allowed” Page**
If the user does not have access to the application, the user should be redirected to an “Access denied” page which should explain the user is not authorized to use the application and to contact user support.

☐ **Logout Page**
You should always let the user know that log out and exit the browser is recommended in order to prevent others from accessing / viewing your personal information, prevent unauthorized use of your CaneID and protect your privacy. User should receive a message similar to “To completely and safely logout and prevent others from accessing your account, please close/exit your web browser”.

☐ **Single Sign-On Session Testing**
We have a few test scenarios that will allow the application owner or users to make sure their Single Sign-on implementation works. This includes testing the session “sharing” across different applications and recommended logout process flow. Please refer to the following test cases documentation as a guide to test.

☐ **Single Sign-On (SSO) Integration Process Flow:**
1. Application owner requests Single Sign-on (SSO) integration by sending to SSO Support at umsso@miami.edu as an RFS (Request for Service). SSO services should be requested specifically on the Description of Service Requested.

2. The Middleware Identity Management Team starts assessing requirements and effort for SSO integration as well as recommendations listed on this page.

3. Request is approved by Middleware Identity Management Team.

4. Middleware Identity Management will coordinate with project manager/vendor to exchange metadata information and customized attribute requirements between the (service provider/application) SP and our Shibboleth (Identity Provider) IdP technical contact.

5. Testing is performed based on recommended test cases.

6. Once testing is successful, all parties agree on promotion to production with e-mail from application owner approving IdP promotion.

7. Middleware Identity Management Team receives request to promote and approves promotion to production IdP.

8. Once IdP promotion has been approved internally, a target date is set and we start coordinating promotion, usually done on Tuesdays or Thursdays at 8 p.m. The application owner/SSO integration requester is responsible for the application and obtaining approval for changes with the Change Advisory Board (CAB). The Clinical CAB is on Tuesdays and Non-Clinical CAB is on Wednesdays. The Middleware Identity group will submit request for the SSO integration to the Non-Clinical CAB.

9. Once CAB approvals have been obtained, promotion to IdP production will be coordinated between the SSO team and the application owner and/or vendor. Emails will be sent to all parties involved once promotion has been successfully completed.

10. IdP promotion is completed and user testing is performed in Production. User testing results will be provided by the application owner to the Middleware Identity Services Team to determine promotion has been successfully completed. Any issues with the promotion will be addressed immediately.