Responsibilities and Agreement

Agreement

Even if you integrate your application with the SAML or CAS SSO service without submitting a MyAccess Integration Request form, your use of the CAS or SAML SSO service affirms your agreement to the below statement.

> *I have read and understood all information available in the MyAccess Integration Kit and agree to the Identity Provider and Service Provider responsibilities listed in the Responsibilities and Agreement.*

Responsibilities

Identity Provider (IdP) - Identity and Access Management Team (Us)

The Identity and Access Management team is responsible for maintaining the UCSF MyAccess Identity Provider and related infrastructure, which consists of the following:

1. Supporting and updating Shibboleth IdP software on a regular basis.
2. Notifying departmental technical contacts of any updates and changes to the IdP and allowing adequate time for testing before changes are migrated to the production IdP.
3. Maintaining relationships with the InCommon and UCTrust federations, including registering IdP metadata updates as appropriate.
4. Configuring the IdP for both UCSF Service Provider applications and federated SP applications, which includes loading SP metadata into the IdP.
5. Submitting UCSF owned SP metadata to the InCommon Federation on behalf of UCSF application owners and enabling delegated administration of that metadata for the application owner.

Explanation:

The Identity and Access Management (IAM) team provides general consultation and documentation on how SAML and CAS works to help an application owner know how to integrate their application with MyAccess. See the MyAccess Integration Tool Kit for some of this documentation. The IAM team can make recommendations about what type of setup would be best for an application. However, it is up to the person responsible for integrating the application (you) to implement the setup, or to arrange for others to do so.

The Identity and Access Management team *cannot* provide programming or application customization services and *cannot* support Service Provider and CAS client software installation, configuration or maintenance. Here's why:

- **Scale.** There are hundreds of Service Providers, both on campus and off campus, already integrated with MyAccess, each with a unique system infrastructure and environment.
- **Scope.** Many applications require multiple servers, load balancing, database configurations, network configuration and firewall modifications which requires an in-depth understanding of that application's unique requirements. The people most familiar with the inner workings of the application are thus best suited to the task of making necessary changes to the application to support the MyAccess integration.
- **Security.** The Identity and Access Management team does not, and should not have access to the web servers on which the Service Provider or CAS client software runs. Only the application administrators and the system administrators for the application servers should have this level of access.
- **Resources.** Time requirements to learn all necessary information for all applications in all environments is beyond the staffing limitations of the Identity and Access Management team.

Service Provider (SP) - Application Owner (You)

Departments wishing to integrate with the MyAccess SSO login system will need at least some dedicated staff to support the integration efforts and to maintain the integration over time. If a department does not have internal staff with the necessary skills to support a SAML Service Provider or CAS client, it must enlist some outside service (be it another department or a contracting firm). Any application that is to be integrated with the production MyAccess login system must have a separate test environment in which any changes or updates to the application can be tested before being moved into the production environment.

The application owner or sponsoring department is responsible for the Service Provider. This includes the following aspects of the SSO integration:

1. Project management
2. Determining data needs
3. Submitting data release requests, including to other institutions when federation is appropriate. In the case of submitting your SAML SP metadata to the InCommon Federation, the IAM team will take care of this on your behalf.
4. Monitoring of the application to ensure it is running
5. Identifying, troubleshooting, testing, and resolving application issues. Of course, issues determined to be a result of the IdP configuration should be sent to the IAM team.
6. Developing and sending communications to end users
7. Providing a point of contact for end users experiencing problems

Explanation:

Since the Service Provider application (commonly referred to as an "SP") integrates with the application's web server, support for the Service Provider must be provided by the application owner's team.

The application owner's team should do the following:

1. Become well versed in how the SAML process works (this page is a good start)
2. If using the Shibboleth SP software, join the Internet2 Shibboleth users mailing list and post questions when there are issues
3. Monitor the SAML or CAS compatible process
4. Maintain a non-production version of the application to test patches and related software update processes, including future IdP changes using the stage IdP environment provided by the IAM team.