XSEDE Capability Delivery Plan
IDM-02 - Web Login to XSEDE User Portal with username/password
IDM-04 - Login to XSEDE User Portal with a non-XSEDE identity
Last revised 2017-11-22

Background

Use cases describe community needs, requirements, and recommendations for improvements to cyberinfrastructure (CI) resources and services. A Capability Delivery Plan (CDP) is an executive summary of the current gaps in our support for a use case, current plans to fill those gaps with new or enhanced capabilities, and the operational components that currently support the use case.

Use case summary

Use cases IDM-02 and IDM-04 describe how XSEDE community members need to login to the XSEDE user portal. IDM-02 describes logging in with an XSEDE username and password, and IDM-04 describes logging in with another identity, such as a campus ID. The full descriptions of these use cases are available in the CSR's use case registry.

CDP summary

The XSEDE system mostly supports these use cases as described, with one gap. Three critical components are in place: the XSEDE User Portal (XUP), where educators and their students can register with XSEDE and obtain XSEDE ID/passwords; Globus Auth, an OIDC-based public authentication service intended to enable XSEDE authentication to external services; and CILogon, a translation service that allows OIDC authentication using the InCommon (SAML-based) identity providers offered by colleges and universities.

Gap(s) that we currently plan to address:

- None

Gap(s) that will not be addressed at this time:

- Ability to specify trusted identity providers

Time and effort summary:

- **None**

Functionality gaps

1. Ability to specify trusted identity providers (suggested priority: medium)

Use case IDM-04 says that the XUP and XSEDE services should be able to choose which identity providers they trust for linked non-XSEDE identities. At present, this feature is not available in Globus Auth, so it's not available to the XUP or other XSEDE services.

Plans: We have no plans to add this feature until the research community organizes a classification system for OAuth2, OIDC, and/or InCommon/SAML identity providers. The classification system would group individual identity providers into classes based on their trustworthiness, giving XSEDE a choice of classes to allow (or not allow) for use with XSEDE's authentication services. At this time, such a classification system exists for X.509 certificate authorities (IGTF), but no equivalent system exists for the InCommon/SAML or OAuth2/OIDC spaces.

System components that support this use case

The following XSEDE operational components currently support this use case.

Component	Supported Functionality
XSEDE User Portal (XUP)	The front-end (web browser-based) user interface to the XSEDE system where individuals register with XSEDE, manage their user profile information, request allocations to use XSEDE SP resources, and manage membership in projects that have active allocations.
Globus Auth	XSEDE's public authentication interface, based on OpenID Connect (OIDC). Globus Auth provides the authentication interface that allows direct XSEDE authentication via 2-legged OAuth2 and indirect authentication via 3-legged OAuth2 and OIDC.
CILogon	An OpenID Connect (OIDC) service that translates InCommon (SAML-based) identity provider services into the OAuth2/OIDC universe. Globus Auth uses CILogon to allow users to authenticate using InCommon (SAML-based) identity providers, which are the authentication services provided by most colleges and universities.
XSEDE OIDC	XSEDE's OpenID Connect service, which provides an OpenID Connect 1.0 service interface for XSEDE's Kerberos service.
XSEDE Kerberos	XSEDE's Kerberos service, which stores all XSEDE usernames and passwords and provides simple username/password authentication.