XSEDE Capability Delivery Plan
CAN-6: Authenticate to one or more SP resources, SP services, and XSEDE central services
Last revised 2017-12-14

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 use case support gaps, of plans to fill those gaps with new or enhanced capabilities, and of existing operational components that already support aspects of a use case.

Use Case Summary

Users, groups, and services may need to authenticate themselves in order to access both XSEDE operated services and services operated by others. Rather than manually authenticating against each service before use, it is desirable to authenticate once and use some proof of authentication for subsequent interactions with the same or other services. This approach is sometimes known as single sign-on.

Use case document(s):

- https://software.xsede.org/use-case/can-06
- http://hdl.handle.net/2142/88830

CDP Summary

The functionality described in this use case is about 80% supported by the operational components listed later in the **System Components That Support This Use Case** section**.**

Gap(s) that we currently plan to address:

1. Web SSO is not supported by all XSEDE services (suggested priority: high)
2. XSEDE SSO Hub (login.xsede.org) does not support InCommon authentication (suggested priority: high)

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

- Zimbra briefcase feature to share files securely (zimbra.xsede.org; needed for IMAP and POP for some apps.)
- Searchable archives of XSEDE mailing lists (mhonarc.xsede.org)
- Sharepoint service (https://share.sdsc.edu/xsede)

Time and effort summary:

- TBD

Functionality Gaps

1. Web SSO is not supported by all XSEDE services (suggested priority: high)

XSEDE web services that need to be made available only to authenticated XSEDE users use different types of authentication. Some authenticate the user using XSEDE portal username/password. Some also provide an option to authenticate using the Globus Auth service which allows authentication using XSEDE username/password or other credentials that are linked to the user's XSEDE account. Since Globus Auth stores a cookie in the user agent's (typically a Web browser) session, and does not prompt the user for username/password again if the user had already authenticated, this provides a Web SSO (Single-SignOn) capability to XSEDE users. This capability has been made available via implementation of an 'XSEDE Login' button that uses Globus Auth, on the login pages of the Web services listed later in the **System Components That Support This Use Case** section**.**

The following additional web services currently do not support Web SSO as defined above. Unless specified otherwise, it is proposed that these services be modified to implement Web SSO using Globus Auth, via a new button (the name and style of which will be determined in the design phase, for uniform presentation and user-experience), using guidance in the below document on XSEDE Identity Management Client Application Setup: https://docs.google.com/document/d/1a2WXUnilBQkNla5d89dMAGur-j2M-ITs4y0A_c2qrLw

- User services
    - XSEDE User Portal (portal.xsede.org). Already supports XSEDE Login but needs to update the visual elements to conform with the Web SSO design (suggested priority: high) *Maytal Dahan <maytal@tacc.utexas.edu>*
    - Mobile version of XSEDE user portal (https://mobile.xsede.org/) (suggested priority: high) *Maytal Dahan <maytal@tacc.utexas.edu>*
    - Online training websites:
        - CI-Tutor (https://www.citutor.org//login.php): Instructions exist on this page for connecting XUP account with CI-Tutor account for automatic login to CI-Tutor. It would be good to replace this with an 'XSEDE Login' style SSO for uniform user experience. (suggested priority: high) *Sandie Kappes <skappes@ncsa.illinois.edu>*
        - Cornell Virtual Workshop (https://cvw.cac.cornell.edu/Registration/): Access via XUP for full access. It would be good to replace this with an 'XSEDE Login' style SSO for uniform user experience. (suggested priority: high) *Susan Mehringer <shm7@cornell.edu>*
    - XSEDE Resource Allocation System (https://xras-review.xsede.org/login and https://xras-admin.xsede.org/login) (suggested priority: high) *Steve Peckins <speckins@illinois.edu>*
    - XD Metrics on Demand (https://xdmod.ccr.buffalo.edu) *Ben Plessenger*

<bpless@buffalo.edu>, Rudra Chakraborty <rudracha@buffalo.edu>

- Staff services
    - Nagios monitoring and alerts for XSEDE services. (http://nagios.xsede.org/) (suggested priority: low) *Gary Rogers <grogers3@utk.edu>*
    - Inca monitoring for XSEDE services (https://inca.xsede.org/) (suggested priority: low) *Shava Smallen <ssmallen@sdsc.edu>*
    - https://rdr.xsede.org/ (central repository for resource information that is critical to XSEDE Central Services; accessed by SPs also.) (suggested priority: low) *Rob Light <light@psc.edu>*
    - Community Software Repository "CSR" (https://software.xsede.org/); Accessed by the UREP, XSEDE and SP staff, and some users. (suggested priority: medium) *JP Navarro <navarro@mcs.anl.gov>, Kate Kaya <kate@sdsc.edu>*
    - XSEDE source repository (https://software.xsede.org/svn/ and https://software.xsede.org/viewvc/xsede/; Accessed by XSEDE and SP staff.) (suggested priority: low) *JP Navarro <navarro@mcs.anl.gov>, Kate Kaya <kate@sdsc.edu>*
    - Information Services (https://info.xsede.org); Accessed by internal and external developers, services, and staff. (suggested priority: medium) *JP Navarro <navarro@mcs.anl.gov>, Eric Blau <blau@mcs.anl.gov>*
    - Index of XSEDE Enterprise Services. (https://sysops.xsede.org/xes-index; Accessed by XSEDE staff.) (suggested priority: low) *Gary Rogers <grogers3@utk.edu>*
    - XSEDE support tickets (https://tickets.xsede.org; used by staff; users have access to ticket info in XUP) (suggested priority: low) *Gary Rogers <grogers3@utk.edu>*
    - XSEDE SVN repository (software.xsede.org) *JP Navarro <navarro@mcs.anl.gov>, Kate Kaya <kate@sdsc.edu>*

Plans: https://jira.xsede.org/browse/XCI-315

2. Web SSO Style Inconsistencies (suggested priority: high)

XSEDE web services that support XSEDE federated login but do not conform to a uniform name and style for the SSO button. Once the name and style of the SSO button is determined in the design phase in addressing the previous gap, this style will be applied to the services below that currently support the feature using different naming/styles such as the "XSEDE Login" button, "Other Sign In Options" button (XUP) and "Xsede OpenID Connect" button (XSEDE courses website, moodle.xsede.org), for uniform presentation and user-experience.

- confluence.xsede.org
- jira.xsede.org
- software.xsede.org
- www.globus.org
- Moodle

Plans: https://jira.xsede.org/browse/XCI-317

3. XSEDE SSO Hub (login.xsede.org) does not support InCommon authentication

(suggested priority: high)

Currently the XSEDE SSO Hub requires XSEDE Kerberos authentication. CAN-6 states, "The authentication mechanism MUST be able to federate with other mechanisms such as those used by OSG, PRACE, EGI, and InCommon." Migrating the SSO Hub to Globus Auth will give users the option of using InCommon authentication (via CILogon) when logging in. Note that the XSEDE SSO Hub will likely be migrating to Globus Auth due to Globus Toolkit retirement (XCI-127).

Plans: https://jira.xsede.org/browse/XCI-318

System Components That Support This Use Case

The following XSEDE operational components currently support this use case:

Component	Supported Functionality
XSEDE User Portal (XUP)	portal.xsede.org. The frontend user interface to the XSEDE system where end users register with XSEDE, manage their user profile information, and request allocations to use XSEDE SP resources. Web SSO is provided via the 'Other Sign In Options' SignIn option, which uses 3-legged Globus Auth.
XSEDE Central Database (XCDB)	The repository that stores XSEDE user profile data, including everything except usernames and passwords (see Kerberos, below), user defined groups (currently unimplemented), and links with non-XSEDE identities (see Globus Auth, below).
Globus Auth	Provides the authentication service used by end users to login to XUP and obtain an XSEDE OAuth2 token that can be used with other XSEDE services, plus the ability for end users to link their XSEDE identities with non-XSEDE identities (e.g., InCommon campus identities, DOE and other agency identities, etc.). Activity XCI-2 produced a document that Science Gateways can use to support XSEDE authentication.
XSEDE Kerberos	The repository that stores XSEDE usernames and passwords and authenticates XSEDE identities for Globus Auth.
XSEDE Single Sign On (SSO) Hub	An SSH service hosted by XSEDE that allows XSEDE end users to login using their XSEDE user identity and connect to XSEDE SP resources (where they are authorized) without entering additional user credentials.

XSEDE MyProxy	A service hosted by XSEDE that translates XSEDE username and password (see Kerberos above) into X.509 proxy certificates required by some XSEDE and legacy TeraGrid services.
WS-Trust STS service	An externally supported service that translates XSEDE OAuth2 tokens (user identity, group membership) obtained from Globus Auth and XUP into the signed SAML chains required by XSEDE Genesis II and UNICORE services, including GFFS. The WS-STS helps provide SSO for SOAP web services and we have no gaps for WS-STS at this time. Also: "WSTrust Secure Token Service (STS) for translating OAuth 2.0 tokens into signed SAML assertions. This translation is used by Genesis II clients to obtain the signed SAML credentials needed to use Genesis II and UNICORE clients and services, including both GFFS and remote job submission. Note that Genesis II clients have a preexisting workaround that uses XSEDE's Kerberos services instead of the Globus Auth service, which produces a similar result but won't work with the user-defined group features mentioned above." FROM: Reference 3 below.
confluence.xsede.org	Web SSO is provided via the 'XSEDE Login' SignIn option, which uses 3-legged Globus Auth.
jira.xsede.org	Web SSO is provided via the 'XSEDE Login' SignIn option, which uses 3-legged Globus Auth.
software.xsede.org	Web SSO is provided via the 'XSEDE Login' SignIn option, which uses 3-legged Globus Auth.
www.globus.org	Web SSO is provided by use of Globus Auth natively.
Moodle	Web SSO is currently available via the 'Xsede OpenID Connect' button. This button could be restyled/renamed for uniform user experience. *Sandie Kappes <skappes@ncsa.illinois.edu> and Kate Cahill <kcahill@osc.edu>*

References

1. XSEDE Identity Management Client Application Setup: https://docs.google.com/document/d/1a2WXUnilBQkNla5d89dMAGur-j2M-lTs4y0A_c2qrLw
2. XSEDE Enterprises Service index: https://sysops.xsede.org/xes-index/?expand_all=1
3. XSEDE Capability Delivery Plan UCCAN6 and UCCAN9 Identity Management Last revised 20160601: https://software.xsede.org/svn/xci/plans/capability-delivery/CAN-6-and-CAN-9-2016-06-01.pdf