## Revision history:

<table>
<thead>
<tr>
<th>RELEASE/REVISION</th>
<th>RELEASE/REVISION DATE</th>
<th>SUMMARY OF CHANGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9</td>
<td>July 16, 2013</td>
<td>First draft of response to canonical use case nine – on hold pending review/approval of XSEDE identity management proposal</td>
</tr>
<tr>
<td>1.0</td>
<td>October 14, 2014</td>
<td>Complete first draft, incorporating new XSEDE identity management architecture &amp; design</td>
</tr>
<tr>
<td>1.1</td>
<td>October 24, 2014</td>
<td>Reviewed and approved by architects</td>
</tr>
<tr>
<td>1.3</td>
<td>January 31, 2015</td>
<td>Changes resulting from Active Design Review incorporated. Notably section 3.3 regarding thick/thin client authentication.</td>
</tr>
</tbody>
</table>
Table of Contents

Contents

1 Introduction ......................................................................................................................... 3
  1.1 Structure of this Document ......................................................................................... 3

2 Canonical Use Case 9 ......................................................................................................... 4

3 User identity and access management .............................................................................. 7
  3.1 The User creates an XSEDE identity ........................................................................... 7
  3.2 The User manages his/her XSEDE user profile. ......................................................... 8
  3.3 The User logs into any XSEDE-operated service using his/her XSEDE identity via either his/her XSEDE username/password or via a federated identity bound to his/her XSEDE identity ................................................................................................................. 9
  3.4 A project in which the User is a member receives an XSEDE allocation and the User uses his/her XSEDE identity to access the associated SP system(s)......................................................... 10
  3.5 A project in which the User is a member receives a non-XSEDE allocation and the User uses his/her XSEDE identity to access the associated system(s) ......................................................... 10
  3.6 The User manages XSEDE groups ............................................................................. 11
  3.7 Groups can appear in authorization policies controlling access to a resource (e.g., file or storage system or use of an allocation). The authorization policies are determined by the parties responsible for the services/resources in question ............................................................................................................. 11
  3.8 The User discovers a list of groups in which he/she has a specific role....................... 12
  3.9 The User discovers a group’s profile .......................................................................... 13
  3.10 An XSEDE identity can be disabled so that it can no longer be accessed. .............. 13

4 Quality of Service Attributes ............................................................................................... 14
  4.1 A User who does not currently have an XSEDE identity can establish an XSEDE identity in five minutes or less, without direct synchronous interaction with another human being. 14
  4.2 A User can bind a non-XSEDE identity (e.g., InCommon) to his/her XSEDE identity in five minutes or less, without direct synchronous interaction with another human being... 14
  4.3 The User’s interface to the XSEDE identity management system is fully accessible via commodity web browsers and Internet connections ........................................................................................................ 15
  4.4 The availability of the XSEDE identity management system for the purposes of authenticating and reading profiles is mission critical and must be 99.95%. The availability of the update mechanism is 99.9%. ................................................................................................................................. 15
  4.5 The User can adjust any user-editable fields in his/her XSEDE user profile with no direct interaction with another human being ........................................................................ 15
  4.6 The User can authenticate to their XSEDE identity using any of its bound non-XSEDE identities. The authenticated XSEDE identity can then be used with any XSEDE-operated service ........................................................................................................ 16
4.7 The User can complete the password reset process via email for his/her XSEDE identity in 5 minutes or less. A mechanism must exist that allows the User to accomplish this task without direct synchronous interaction with a human. ........................................ 16
4.8 The User can complete individual XSEDE group management tasks in five minutes or less and without direct synchronous interaction with another human being. .......................... 16
4.9 Groups are expected to scale to low degree thousands of members............................... 16
4.10 Group membership tests should take less than five seconds. .................................. 17
4.11 Changes to XSEDE group membership will take effect in the XSEDE identity management system in less than five seconds. Group membership changes may not be visible until an affected member re-authenticates. ......................................................... 17
4.12 (n/a).................................................................................................................................................. 17
4.13 (n/a).................................................................................................................................................. 17
4.14 Non-XSEDE relying parties will be able to use XSEDE group functions without direct synchronous interaction with XSEDE personnel. ......................................................... 17
1 Introduction

This document describes the realization of Canonical Use Case 9, User Identity and Access Management, using the XSEDE architectural components. See http://hdl.handle.net/2142/45237 for the use cases.

It is assumed that the reader has already read and is very familiar with the XSEDE Architecture Level 3 Decomposition (L3D), in particular sections 3 (Access Layer), 4.2 (The Web/Cloud Approach and XUAS), 6 (XUAS), and 8 (Deployment). The authors suggest that this document be open or on hand when reading this document.

This document also refers to [NEX1], the Globus Online “Nexus API Documentation,” http://globusonline.github.io/nexus-docs/api.html. This REST API is referred to primarily in sections covering application integration and Grid interoperability.

1.1 Structure of this Document

This document is organized as follows. Section 2 briefly describes the user identity and access management use case. Section 3 describes how XSEDE architecture components are used to implement the use case from section 2.
2 Canonical Use Case 9

Canonical use case 9 is “User identity and access management.” The description is “Enable an XSEDE user to establish, manage, and disable his/her XSEDE identity.”

The use case starts with two assumptions, specifically:

a) The User is aware of the existence of XSEDE.

b) The User has access to the Internet and a commodity web browser.

This use case describes the complete life cycle of an XSEDE user identity from initial registration with XSEDE through using XSEDE and, ultimately, de-activation of the user’s registration. This includes the user's ability to create and manage an individual user profile and also the user's ability to define and manage XSEDE groups: named lists of XSEDE identities that can be referred to in other operations. Beyond this, it describes a large number of actions that the user may take in the course of managing his/her XSEDE identity, most of which are optional and will be taken by the user only if they are appropriate for his/her needs. In Section 3 of this document, we respond to each specific action, one action per sub-section. The table of contents for Section 3 is a good summary of the actions described in the use case.

The quality attributes for the use case are shown below in Table 1. There are no variations expressed in the use case document. (This is because the use case directly describes all of the “optional” actions that the user may or may not take.)
Table 1: Quality attributes for XSEDE user identity and access management.

<table>
<thead>
<tr>
<th>UCCAN 9</th>
<th>XSEDE User Identity and Access Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>QAS-CAN9.1</td>
<td>A User who does not currently have an XSEDE identity can establish an XSEDE identity in five minutes or less, without direct synchronous interaction with another human being. Assumptions: The user starts at the XSEDE web page, xsede.org. Setting of any privileges is out of scope of the five minutes.</td>
</tr>
<tr>
<td>QAS-CAN9.2</td>
<td>A User can bind a non-XSEDE identity (e.g., InCommon) to his/her XSEDE identity in five minutes or less, without direct synchronous interaction with another human being. Assumptions: a) The user is already authenticated at the XSEDE web page, xsede.org; b) the non-XSEDE identity provider is trusted by XSEDE; c) the XSEDE federation mechanism supports the non-XSEDE identity provider’s authentication mechanism; d) the user is able to authenticate with the non-XSEDE identity provider; e) The non-XSEDE identity provider will release necessary attributes to XSEDE to allow authentication.</td>
</tr>
<tr>
<td>QAS-CAN9.3</td>
<td>The User’s interface to the XSEDE identity management system is fully accessible via commodity web browsers and Internet connections.</td>
</tr>
<tr>
<td>QAS-CAN9.4</td>
<td>The availability of the XSEDE identity management system for the purposes of authenticating and reading profiles is mission critical and must be 99.95%. The availability of the update mechanism is 99.9%. Assumptions: Availability is defined as the percentage of time in a given &lt;month&gt; that a service correctly responds. (NB: Correctness can include timing.)</td>
</tr>
<tr>
<td>QAS-CAN9.5</td>
<td>The User can adjust any user-editable fields in his/her XSEDE user profile with no direct interaction with another human being.</td>
</tr>
<tr>
<td>QAS-CAN9.6</td>
<td>The User can authenticate to their XSEDE identity using any of its bound non-XSEDE identities. The authenticated XSEDE identity can then be used with any XSEDE-operated service. Assumption: The non-XSEDE identity provider is available.</td>
</tr>
<tr>
<td>QAS-CAN9.7</td>
<td>The User can complete the password reset process via email for his/her XSEDE identity in 5 minutes or less. A mechanism must exist that allows the User to accomplish this task without direct synchronous interaction with a human. Assumption: a) The User is familiar with the password reset process; b) the User has access to that email address.</td>
</tr>
<tr>
<td>QAS-CAN9.8</td>
<td>The User can complete individual XSEDE group management tasks in five minutes or less and without direct synchronous interaction with another human being.</td>
</tr>
<tr>
<td>QAS-CAN9.9</td>
<td>Groups are expected to scale to low degree thousands of members.</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>QAS-CAN9.10</td>
<td>Group membership tests should take less than five seconds.</td>
</tr>
<tr>
<td>QAS-CAN9.11</td>
<td>Changes to XSEDE group membership will take effect in the XSEDE identity management system in less than five seconds. Group membership changes may not be visible until an affected member re-authenticates.</td>
</tr>
<tr>
<td>QAS-CAN9.12</td>
<td>n/a</td>
</tr>
<tr>
<td>QAS-CAN9.13</td>
<td>n/a</td>
</tr>
<tr>
<td>QAS-CAN9.14</td>
<td>Non-XSEDE relying parties will be able to use XSEDE group functions without direct synchronous interaction with XSEDE personnel.</td>
</tr>
</tbody>
</table>
3 User identity and access management

Assume that

1. The User is aware of the existence of XSEDE.
2. The User has access to the Internet and a commodity web browser.
3. The User has an existing email account capable of receiving standard Internet email.
4. The email address that the User enters as primary email address (in step 4 below) is not already linked to an XSEDE identity.
5. The Globus Online service (operated by XSEDE) is in its normal operating state.

Sections 3.2 and beyond assume that Section 3.1 (creating an XSEDE identity) has already been completed successfully and that Section 3.10 (disabling the XSEDE identity) has not been done or has been reversed by some other action.

This architectural response refers to the following elements of the XSEDE architecture, all of which are described in [L3D].

<table>
<thead>
<tr>
<th>Component or Service</th>
<th>L3D Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>XSEDE User Portal (XUP)</td>
<td>§3.1.1</td>
</tr>
<tr>
<td>Globus OAuth service</td>
<td>§3.1.2 and §4.2.4</td>
</tr>
<tr>
<td>Globus group management service</td>
<td>§3.1.3</td>
</tr>
<tr>
<td>XSEDE Kerberos service</td>
<td>§7.1.2 (and subsections)</td>
</tr>
<tr>
<td>XSEDE Central Database (XCDB)</td>
<td>§7.1.2 (and subsections)</td>
</tr>
<tr>
<td>XSEDE MyProxy service</td>
<td>§7.1.2 (and subsections)</td>
</tr>
<tr>
<td>XSEDE WS-Trust STS service</td>
<td>§4.1.9 and §5.1.5</td>
</tr>
</tbody>
</table>

3.1 The User creates an XSEDE identity.

XSEDE’s User Portal (XUP) provides a thin-client interface for this step.

Steps:

1. Launch a Web browser and open http://www.xsede.org/ (XUP).
2. Click the “Sign In” link.
3. Click the “Create an Account” link.
4. Enter the required information in the registration form. The User will be prompted for a user id and password and a primary email address, among other things.
5. Invisibly to the user, XUP passes the user’s information to Globus using Globus’s REST API to initiate creation of the account. Also invisibly, XUP passes the user’s information to XSEDE’s Kerberos service to set the user’s password. Finally, XUP passes the user’s information to the XCDB (XSEDE Central Database) to record extended attributes about the user.
6. Globus compares the user’s information to existing Globus identities and, if a likely match is found, offers to link the user’s new XSEDE identity to an existing Globus identity. (The user must successfully authenticate to the Globus identity to create such a link.)

7. Globus initiates the email verification workflow via email to the user. The email includes a hyperlink that the User should click on to verify that he/she has access to the email address.

8. When the User clicks the verification link, Globus notifies XUP via a Webhook that the user’s email address has been verified, Globus completes its registration process, and directs the user back to the XUP for login.

At this point, XSEDE’s Globus service, XCDB, and Kerberos services all contain an identity definition for the User containing a common XSEDE userid. The user’s password is stored in one-way encrypted form in Kerberos. Globus and XCDB have the user’s primary email address, which has been verified to be accessible by the User.

Having achieved this, XSEDE’s Kerberos services will subsequently accept this user id and password. Globus will use Kerberos for user authentication, and XUP will use Globus for user authentication. All other XSEDE services will use one of these three services to authenticate XSEDE users and will use the contents of XCDB and the Globus group management service for authorization decisions. More specifically, the XCDB will be consulted to determine whether or not the user has a current XSEDE allocation and, for example, should be permitted to retrieve an X.509 proxy from the XSEDE MyProxy service. The Globus group management service will be consulted to determine membership in Globus groups when needed to evaluate authorization policies (e.g., Globus’s “sharing” feature) or to perform credential translation (e.g., the WS-Trust STS service).

### 3.2 The User manages his/her XSEDE user profile.

XSEDE’s User Portal (XUP, the XSEDE Central Database (XCDB), Globus, and XSEDE’s Kerberos services enable this action.

Steps:
1. Launch a Web browser and open http://www.xsede.org/ (XUP).
2. Sign in to XUP using the “Sign In” link and submitting a valid user id and password.
3. The user’s full name will appear in the menu bar at the top of the page. Click the name.
4. The user’s profile will appear with appropriate user interface for changing profile data.

Step 2a in the use case description (pre-populating the profile with existing data from another identity) is not currently supported. (It is architecturally possible using the OAuth 2.0 mechanism in a slightly different way.)

If the user changes his/her email address (step 2.b) via this interface, XUP will notify Globus of the change and Globus will initiate the email verification workflow via email to the user. (As described above, the email includes a hyperlink that the User should click on to verify that he/she has access to the email address. When the User clicks the verification link, Globus notifies XUP via a Webhook that the user’s email address has been verified. Globus completes its email address change, and directs the user back to the XUP for login.)

If the user elects to bind one or more non-XSEDE identities with his/her XSEDE identity (step 2.c), XUP will redirect the user’s web browser to Globus, Globus will provide an XSEDE-skinned user interface for performing the binding, and on completion Globus will return the user to XUP.
If the user changes attributes other than the password (step 2.d), XUP will use the XCDB’s SQL interface to effect the changes in the user’s profile. (XCDB is where this data resides.)

If the user changes his/her password (step 2.e), XUP will use the administrative interface for XSEDE’s Kerberos service to change the user’s password in Kerberos. The change will apply immediately to Kerberos, Globus, and XUP logins.

3.3 The User logs into any XSEDE-operated service using his/her XSEDE identity via either his/her XSEDE username/password or via a federated identity bound to his/her XSEDE identity.

XSEDE-operated services include, but are not limited to: XUP, Globus, XRAS, and the centrally operated portions of GFFS, Genesis II, and UNICORE. (SP-operated services are covered below in Section 3.4.) Each of these services has been configured to support use of XSEDE user identities for login and basic user identification.

Each service presents a login interface to the user, requesting a user id and password. Thin-clients (web browser interfaces) present an alternate login link to allow users to make use of federated identity services such as InCommon member institutions. Thick-clients (locally installed applications) present this option to the user via the application interface.

If the user enters a user id and password in the default interface, the service will use Globus Online’s OAuth 2.0 interface to authenticate the user. Thin clients will use 3-legged OAuth 2.0 workflow, and thick clients will use the 2-legged OAuth 2.0 workflow. Globus in turn will use XSEDE’s Kerberos service to authenticate the user’s ID/password. If Kerberos authentication succeeds, Globus will return an OAuth token. The client, thin or thick, should store this OAuth token for later use.

3.3.1 Alternate login

If the user elects to use the alternate login interface, thin clients should redirect the user’s browser to Globus following the OAuth2 protocol, which will provide an XSEDE-skinned interface for selecting an identity provider and authenticating. Thick clients should query Globus to obtain the list of XSEDE-approved identity providers and present this list to the user via their own interfaces.

During thin-client authentication, when the user selects an alternate identity provider, Globus will redirect the user’s browser to the identity provider’s authentication interface. (Note that this redirect-and-authentication may use any of a variety of protocols, including OAuth1a+MyProxy, OAuth2+MyProxy, OpenID Connect, SAML via CILogin, etc. as determined by the identity provider.) Once authentication is successful, Globus, in conjunction with OpenID Connect\(^1\), will look up the XSEDE identity associated with it.

- Assuming there is an associated XSEDE identity, Globus will return an OAuth token to XUP along with additional fields that identify the XSEDE user. This will be treated as a successful authentication and XUP will store the user’s OAuth token for later use.
- If there is currently no XSESE identity associated with the OAuth identity, Globus will direct the user back to XUP to create a new account. Once the user has created and/or

---

\(^1\) [http://openid.net/connect/](http://openid.net/connect/)
logged into his/her XSEDE account, he/she may bind the identity and use it for subsequent logins.

During thick-client authentication, the client uses the OAuth2 two-legged workflow with Globus’s OAuth2 service, passing in the username and password for the chosen identity provider. Globus then attempts to authenticate the username and password with the identity provider’s authentication interface. (Like the thin-client interaction, this may use any of a variety of protocols, including OAuth1a+MyProxy, OAuth2+MyProxy, OpenID Connect, SAML via CILogin, etc. as determined by the identity provider.) Assuming authentication is successful, Globus, in conjunction with OpenID Connect, will look up the XSEDE identity associated with it and will return an OAuth2 token to the client along with additional fields that identify the XSEDE user. The client should treat this as a successful authentication and store the user’s OAuth2 token for later use.

### 3.4 A project in which the User is a member receives an XSEDE allocation and the User uses his/her XSEDE identity to access the associated SP system(s).

The XSEDE allocation process assigns XSEDE computing and data resources to individuals and teams for accomplishing specific, proposed and reviewed, scientific objectives. Systems on which these allocations are provided are operated by XSEDE Service Providers (SPs). These systems are usually high-performance or high-throughput computing systems and large-scale data services.

The XRAS service manages the allocation proposal, review, and decision-making process. As described in Section 3.3, users authenticate with XRAS using their XSEDE user identity. Thus, the allocation process begins with an XSEDE user identity requesting an allocation. If the allocation is approved, XCDB is updated to reflect the fact. XCDB sends an AMIE “packet” to the SP that operates the allocated service informing the SP of the approved allocation. The SP is responsible for translating the XSEDE user identity into a service-specific identity for the purpose of identification and authentication. The SP returns an AMIE packet to XCDB indicating the service-specific identity. Thus, XCDB contains a mapping of XSEDE identities to service-specific identities. The user receives a notice of his/her allocation and relevant information about his/her service-specific authentication credentials.

Once the allocation is established both in XCDB and at the SP resource, the user can use XSEDE’s interactive login services to access the system as described in UCCAN-4 (Interactive Login), transfer datasets to/from the resource as described in UCCAN-2 (Managed File Transfer), or submit computation jobs as described in UCCAN-1 (Run a Remote Job).

### 3.5 A project in which the User is a member receives a non-XSEDE allocation and the User uses his/her XSEDE identity to access the associated system(s).

This step explicitly involves a system that doesn’t participate fully in the XSEDE architecture. Consequently, XSEDE’s architecture provides multiple ways for this to be accommodated. All of the methods assume that the user already has an XSEDE identity established (§3.1) and that the non-XSEDE system will authorize use by someone who can certify his/her XSEDE identity via one of the credential types offered by XSEDE.

The types of credentials that XSEDE can provide to certify a user’s XSEDE identity are:
1. OAuth 2.0 token. Thin-client methods are supported via an OAuth 2.0. The non-XSEDE service must offer the user the ability to authenticate via an “alternate login” and to select XSEDE as the alternate identity provider. The user will be redirected to the XUP login page to authenticate, and, on success, an OAuth 2.0 token certifying the user’s XSEDE identity will be delivered to the non-XSEDE service.

2. Signed SAML chain. Thick-client applications are supported via signed SAML chains. The user must authenticate to XSEDE and use the method described in UCCAN-6 (Authentication) to establish a client-managed security context containing a signed SAML chain. Once this context is established, the user may use it to authenticate to non-XSEDE services that accept this form of credential.

3. X.509 proxy certificate. XSEDE also offers end users the ability to obtain an X.509 certificate signed by an IGTF-accredited certificate authority via the MyProxy service. The user must have a MyProxy client on his/her local system and must authenticate to XSEDE’s MyProxy service using his/her XSEDE userid and password (established as described in §3.1). The MyProxy client will delegate an X.509 proxy certificate to the user’s system, and the user may then use that certificate to authenticate to non-XSEDE systems.

3.6 The User manages XSEDE groups.

XSEDE’s User Portal (XUP) and XSEDE’s Globus Online service enable this action.

Steps:
1. Launch a Web browser and open http://www.xsede.org/ (XUP).
2. Sign in to XUP using the “Sign In” link and submitting a valid user id and password.
3. The user’s full name will appear in the menu bar at the top of the page. Click the name. XUP will present the user with the user profile interface. Within that interface, an option to manage groups will be present. Select that option. (At this point, the user will be redirected to an XSEDE-skinned Globus web interface for group management functions.)
4. At this point, the user interface will display groups in which the user has any role (member, manager, administrator) and will allow the user to create new groups, manage existing groups in which he/she has the manage role (edit profile information, change the member list), or deactivate/reactivate any groups in which he/she has the administrator role.

If the user makes any changes via this interface, these changes appear immediately in Globus Online and are available to all client services.

3.7 Groups can appear in authorization policies controlling access to a resource (e.g., file or storage system or use of an allocation). The authorization policies are determined by the parties responsible for the services/resources in question.

As described in UCCAN-6 (Authentication), all authorization decisions are made strictly on each resource, by resource-layer interfaces, using local policies set by the SP. In order to support this requirement, however, XSEDE provides (1) an XSEDE-wide group management function, described in §3.6, and (2) an XSEDE-wide credential system that includes group membership in-
formation in several of the supported types of credentials. SPs may use these XSEDE-wide mechanisms as part of their local authorization mechanisms, which has the effect of enabling their users to use XSEDE-wide group definitions in their access control functions.

Specifically, the types of XSEDE-wide credentials that support XSEDE group information are:

1. Signed SAML chains of the form returned by the XSEDE Nexus WS-STS service. In this form, the group information is stored as part of the SAML chain and thus is immediately available to any service that can access and verify the chain.

2. OAuth 2.0 tokens of the form returned by XUP/Nexus. In this form, the OAuth 2.0 token provides a reference to the security context managed by the Globus service, and group information can be queried by anyone with access to the OAuth 2.0 token.

The X.509 proxy certificates returned by MyProxy and the Kerberos tickets returned by the XSEDE Kerberos services do not include group information and so can not be used to support group-based authorization decisions.

3.8 The User discovers a list of groups in which he/she has a specific role.

The XSEDE architecture offers two ways for users to accomplish this: a thin client (web browser-accessible) interface and a thick client (downloadable software) interface. The thin client is best for users who occasionally need to check for groups they belong to. The thick client is best for users who need this functionality on a routine basis or who need to integrate this use case with their software applications and who need local control of the client configuration.

The thin-client interface is provided via XSEDE’s User Portal (XUP) and XSEDE’s Globus Online service.

Steps:

1. Launch a Web browser and open http://www.xsede.org/ (XUP).
2. Sign in to XUP using the “Sign In” link and submitting a valid user id and password.
3. The user’s full name will appear in the menu bar at the top of the page. Click the name.
4. The user’s profile will appear with appropriate user interface for changing profile data. Click “Manage groups” to enter the group management interface. (At this point, the User’s web browser is redirected to https://xsede.globusonline.org/ for the remainder of the steps.)
5. At this point, the user interface will display groups in which the user has any role (member, manager, administrator) and will allow the user to limit the display to groups in which he/she has a specific role.

The thick-client interface is provided by the GFFS interface as described in [L3D §5.1.5] and [GORM §G.1] “User and Group Management.” Specifically:

Steps:

1. Authenticate to XSEDE using one of the GFFS access mechanisms: GUI, FUSE, or command line tools.
2. Change your current working directory to /users/xsede.org/<your_XSEDE_ID> using one of the GFFS access mechanisms: GUI, FUSE, or command line tools. List the directory contents. The groups in which you have some role (usually membership) are listed.
3.9 The User discovers a group’s profile.

XSEDE’s User Portal (XUP) and XSEDE’s Globus Online service enable this action.

Steps:
1. Launch a Web browser and open http://www.xsede.org/ (XUP).
2. Sign in to XUP using the “Sign In” link and submitting a valid user id and password.
3. The user’s full name will appear in the menu bar at the top of the page. Click the name.
4. The user’s profile will appear with appropriate user interface for changing profile data. Click “Manage groups” to enter the group management interface. (At this point, the User’s web browser is redirected to https://xsede.globusonline.org/ for the remainder of the steps.)
5. At this point, the user interface will display groups in which the user has any role (member, manager, administrator). The interface will also present a search field in which the user can enter a search query to look up groups with a given name. When matching groups are found, the user may click the group’s name to view any details about the group that are accessible to the user. (Some details may not be available to the user if the group manager has restricted access to them.)

3.10 An XSEDE identity can be disabled so that it can no longer be accessed.

XSEDE’s User Portal (XUP), XSEDE’s Globus Online service, XCDB, XSEDE’s Kerberos service, and XSEDE’s MyProxy service enable this action.

Steps:
1. Launch a Web browser and open http://www.xsede.org/ (XUP).
2. Sign in to XUP using the “Sign In” link and submitting a valid user id and password.
3. The user’s full name will appear in the menu bar at the top of the page. Click the name.
4. The user’s profile will appear with appropriate user interface for changing profile data. Click “Disable this identity.”

If the user follows the prompts for disabling his/her user identity and completes the process, the user identity will immediately be marked in Globus Online as “disabled.” XUP will also update the XCDB and Kerberos services of the disabled status of the user. At this point, the XUP, Globus Online, and the XSEDE MyProxy service will no longer recognize the user id and password for login, and a query of XCDB will reveal the “disabled” status for the identity. Any client services that check the status of the identity in Globus Online will see that the identity has been disabled.
4 Quality of Service Attributes

4.1 A User who does not currently have an XSEDE identity can establish an XSEDE identity in five minutes or less, without direct synchronous interaction with another human being.

Establishing an XSEDE identity via the process described above (§3.1) requires all of the following actions to complete:

1. four web browser round trips to the XUP (Steps 1-4 of the process described in §3.1.),
2. a REST transaction between the XUP and Globus (Step 5),
3. delivery of email from Globus to the user’s mailbox (Step 7),
4. retrieval of the email message from the user’s mailbox to the user’s email client (Step 7),
5. a web browser round trip to Globus (Step 8),
6. a Webhook transaction between Globus and XUP (Step 8), and
7. an SQL transaction between XUP and XCDB (Step 8).

In addition, the user must interact with his/her web browser, complete and submit the registration form provided by XUP, and locate the email validation link in his/her email interface.

Item 4 above may take longer than five minutes, depending on the email system used by the user and the current volume of email (messages/sec) being sent by Globus. All of the other numbered items above—all together—will take a fraction of one minute.

The time required by the user to interact with the XUP web pages and to complete the registration form are beyond the scope of the XSEDE architecture.

4.2 A User can bind a non-XSEDE identity (e.g., InCommon) to his/her XSEDE identity in five minutes or less, without direct synchronous interaction with another human being.

Binding a non-XSEDE identity to one’s XSEDE identity is accomplished by a combination of XUP, Globus’s web interface, the Globus Nexus user database backend, and the non-XSEDE identity provider’s authentication interface. The process is described above in §3.2, in response to step 2.c of the use case.

The time required to accomplish this step is primarily dependent on the user’s ability to (1) navigate to the appropriate part of the XUP interface, and (2) react to (a) the XSEDE-skinned Globus user interface that guides the user through the identity binding process and (b) the authentication interface presented by the non-XSEDE identity provider. We assume that (2b) is not included in the five-minute time limit, since it is not accomplished via the XSEDE system. Both (1) and (2a) are web browser interfaces that require human interaction. Finding the identity-binding part of the XUP should be easy for end users. If not, this is a flaw in the user interface design of XUP. Similarly, walking through the Globus identity-binding interface should also be easy, and failure here should be dealt with as a flaw in the Globus user interface.

We expect that the part of the process most likely to consume time will be when the user needs to identify the external identity provider for the binding. This involves selecting the provider from a
list presented by Globus, and either name confusion (the provider is listed with an unexpected form of its name) or sorting issues (the provider’s name doesn’t appear at the place in the list that the user expects) may briefly trip the user up. The former is a user education issue, and the second is a user interface issue.

Despite the fact that the process involves communication between several XSEDE and non-XSEDE components, there is nothing in the proposed architecture that would cause these interactions to take longer than five minutes, or even close to it.

4.3 The User’s interface to the XSEDE identity management system is fully accessible via commodity web browsers and Internet connections.

With the notable exception of the email validation step, all of the user actions described in §3 use web-browser-accessible interfaces. The email validation step may also be accomplished via web browser if the user uses a web-browser-accessible email interface. However, the choice of the user’s email interface is beyond our control.

4.4 The availability of the XSEDE identity management system for the purposes of authenticating and reading profiles is mission critical and must be 99.95%. The availability of the update mechanism is 99.9%.

Service availability is the subject of [L3D §9]. In order to satisfy this quality attribute, it is critical that XSEDE operations deploy the Globus Nexus, Kerberos, WS-Trust STS, and MyProxy services in a manner described in the L3D for highly available services, using highly parallel/redundant service instances and highly scalable database backends. Failovers should be automatic based on continuously operating, automated system monitoring. This will ensure that these services—which are critical for obtaining the authentication and authorization tokens used by various XSEDE services—are available 99.95% of the time.

The update mechanism includes the user interface elements provided by the XUP and Globus. The quality attribute requirement is less stringent for updates than for authentication or reads, so it is sufficient for XUP and Globus web interfaces to be available 99.9% of the time. This again calls for redundant deployment, but in this case the failover process could be manual, as long as it is triggered by continuously operating, automated system monitoring.

4.5 The User can adjust any user-editable fields in his/her XSEDE user profile with no direct interaction with another human being.

The steps described in §3.2 satisfy these criteria.
4.6 The User can authenticate to their XSEDE identity using any of its bound non-XSEDE identities. The authenticated XSEDE identity can then be used with any XSEDE-operated service.

Sections §3.3 and §3.4 describe how end users can accomplish these things. The analogous steps for non-XSEDE-operated services are described in §3.5.

4.7 The User can complete the password reset process via email for his/her XSEDE identity in 5 minutes or less. A mechanism must exist that allows the User to accomplish this task without direct synchronous interaction with a human.

The XUP and Globus both provide password reset mechanisms, and the XUP’s is the primary mechanism that will be used by XSEDE users. Neither mechanism requires direct synchronous interaction with a human. Both mechanisms involve the user entering either a username or an associated email address, and the system sending an email message to the associated email address with a web URL link that will initiate the password reset process. The user must have access to his/her associated email mailbox in order to have access to that web URL. The web URL will be active only for a brief time following the email message’s generation.

The parts of the process most likely to consume time are (1) when the email message containing the password-reset web URL is delivered from XSEDE to the user’s email service and (2) when the user retrieves the email from his/her email service. XSEDE has no control over either of these parts of the process as they depend entirely on the user’s choice of email service.

4.8 The User can complete individual XSEDE group management tasks in five minutes or less and without direct synchronous interaction with another human being.

The steps described in §3.6 – §3.9 satisfy this criteria.

4.9 Groups are expected to scale to low degree thousands of members.

The Globus service uses highly scalable, commercial database technologies for storing the definitions of XSEDE groups. The storage space required for thousands of group definitions is trivial.

Globus also uses highly scalable web server tools to provide the user interface for manipulating groups. We are confident that we can satisfy the demand of O(10) – O(100) users interacting with the group management interface simultaneously.
4.10 Group membership tests should take less than five seconds.

In the proposed architectural response, there are two ways to test group membership. The first is a REST-style interaction between a client and the Globus Nexus group management interface using an OAuth token provided by the client and the contents of the Globus group database as the basis for the test. The second is an algorithmic test of the presence or absence of a group membership assertion in a SAML chain presented by the user to a software component.

The second mechanism is purely programmatic and does not involve any network or inter-process communication. It is effectively instantaneous.

The first mechanism is a RESTful web service transaction supported by a backend database query. In order to satisfy this quality attribute, it is vital that XSEDE operations deploy the Globus REST service components and backend group database service as highly available, high-throughput, transactional services. The techniques required for this are described in [L3D §9]. The proposed architecture is specifically designed to facilitate these techniques.

4.11 Changes to XSEDE group membership will take effect in the XSEDE identity management system in less than five seconds. Group membership changes may not be visible until an affected member re-authenticates.

As stated in 4.10, there are two ways to test group membership in our proposed architecture: a REST service transaction with Globus Nexus, or an algorithmic test on a chain of SAML assertions in a SAML-style credential. These SAML assertions originate in a WS-Trust STS service that queries the Globus group management service and returns SAML assertions based on the results of the query. Any change in the group membership state requires a database update in the Globus Nexus service.

In order to satisfy this quality attribute, it is critical that XSEDE operations deploy the Globus Nexus service as a highly available, high-throughput, transactional service as described in [L3D §9]. Also, the WS-Trust STS service should explicitly be configured to avoid caching results of queries to the Globus Nexus group management service.

If these are done, database updates should happen in less than five seconds. Once the database is updated, any query to the database will immediately show the state change, and any subsequent request for credentials from the WS-Trust STS service will return a set of SAML assertions that accurately reflect the state change.

4.12 (n/a)

4.13 (n/a)

4.14 Non-XSEDE relying parties will be able to use XSEDE group functions without direct synchronous interaction with XSEDE personnel.

Non-XSEDE relying parties have the following interfaces available to them for interacting with the XSEDE group functions.
1. The Globus group management REST API
2. The WS-Trust STS interface

Neither of these interfaces requires direct synchronous interaction with XSEDE personnel, either for initial setup or for ongoing use, as long as the services required are read-only (nothing is being changed) and as long as existing access control settings permit the requested services.

Services that involve changing data require authentication and rely on previously established access control settings.