# OSG Review of XSEDE Software & Services and Security Baseline for Service Providers

# General Observations

OSG is a federation of resources where a key principle is autonomy -- each resource independently makes decisions on what software and versions of that software that they implement and how they configure those software packages. There are some requirements for sites but they are minimal. Within this framework, OSG is planning to serve as an XSEDE SP by providing a submit host that will provide an abstraction layer to shield XSEDE users from some of the diversity in the OSG resources; this will mitigate but not remove exposure to the diversity of OSG resources. This submit host, configured as a virtual Condor cluster, will enable OSG to address some of the “common environment” needs, especially those that are common to high throughput computing (HTC) environments.

Since the OSG team is still learning the TeraGrid/XSEDE environment, there may be misunderstandings here that will need to be clarified via collaboration. OSG staff is available to further discuss and review these items with XSEDE to clarify the operating environment provided by OSG for XSEDE users.

# Review of XSEDE Software and Services Baseline (Mats Rynge)

In general, OSG is working to provide the capabilities listed below in section 2.1. Since the OSG environment will not be identical to the XSEDE common services environment, an important area of consideration is on the software version differences between the XSEDE and OSG software stacks that could impact shared operations.

## 2.1 Planned capabilities for the OSG-XSEDE submit host

**Capability Availability Publishing** – Support for publishing capabilities (e.g. GridFTP)

**AIME** – Custom development will be required to share accounting information with Gratia, and to group job data into “summary” chunks in order to not overwhelm the XSEDE central accounting database. (Today Gratia produces a record for each job.)

**Data Movement Servers** – GridFTP is planned, but the OSG may utilize a different version than specified in the capabilities document. The same GridFTP server will be used for data staging between the OSG-XSEDE submit node and remote OSG compute nodes.

**Single Sign On / Remote Access** – GSI-SSH is planned. We are still not sure yet if we will be able to provide a full common user environment (CUE).

**Data Movement Clients** – Multiple versions will be available, both from OSG and XSEDE software stacks.

**Local Compute** – Scheduler provided by Condor environment

**Workflow Support** – Provided by Condor Dagman

## 2.2 Possibilities for future integration include:

**Capability Verification and Validation** – Inca integration would require some custom development in order to make the probes fit the submit host.

**Application Development and Runtime Support** – This is a little bit of a gray area due to the virtual cluster part. We will be able to provide application development support, but runtime support will probably not be available because we do not control the resources on which we run.

**Distributed Programming Services** – SAGA, being evaluated under the Engagement VO.

**Remote Compute** – GRAM interface for submitting jobs to the submit host – this could be useful for science gateways.

**Science Gateway Support** – Remote compute could be available, but I doubt we be able to support community shells

## 2.3 Features not anticipated to be available on the OSG-XSEDE submit host include:

**Local HPC Software Publishing** – No HPC software will be available

**Meta-Scheduling Support** – The virtual Condor cluster across a set of OSG resources is already a form of meta scheduling

**Co-Scheduling Support** – co-scheduling will probably not work alongside of glideinWMS

**Parallel Application Support** – No parallel application support will be available

**WAN Lustre** – No shared file-systems will be available

# Review of XSEDE Technical Security Baseline (Mine Altunay)

**General:** This document only discusses the case that XSEDE users access and utilize OSG resources. It does not discuss the case where OSG users send jobs to XSEDE resources.  
  
**XSEDE projects vs. OSG VOs:** XSEDE has a project concept that is similar to OSG VOs; they both allow a group of scientists to manage their membership and privileges associated with an experiment. One difference from OSG VOs is that an XSEDE project does not assign specific “roles” or “privileges” to project members. Every XSEDE member has a username/password and a certificate. The membership information is contained in the XSEDE Central Database. Currently OSG and XSEDE use different membership technologies.  OSG resources download the VO membership information from VOMS servers. OSG needs further investigation on how to synchronize and distribute membership information from XSEDE projects to OSG resources.  
  
**XSEDE User Responsibility Form**: XSEDE users are required to sign this form upon registering with XSEDE portal. In OSG, we have the OSG Acceptable Use Policy that we expect OSG VOs and users to agree with. The OSG AUP is in alignment with WLCG AUP. The concern here is that the XSEDE policy may not be in alignment with OSG AUP.

Based on a quick review of the XSEDE Policy, it appears similar to the OSG AUP, but XSEDE has a broader coverage and addresses some topics such as Publication, Software Development and Licensing that we do not address in OSG. Also, there is no mention of other policies in the XSEDE document regarding SPs behavior, such as incident response, service provider responsibilities, etc. While common policies are not necessarily the goal, a discussion of policy differences between OSG and XSEDE could prove beneficial to both groups.

**Account Management Information Exchange System (AMIE)**: XSEDE has its own account management system to track individual usage. It is only discussed for a short paragraph in this document.  OSG has plans to implement a subset of AMIE functionality at the OSG-XSEDE submit host.  
  
**TeraGrid CAs**: The TeraGrid working group required all CAs who wants to be approved by TeraGrid to be first accredited by IGTF. Currently, except for SDSC CA, all of the CAs approved by TeraGrid are already IGTF-accredited. Therefore, TeraGrid approved CAs are already distributed by OSG and trusted by OSG resources. We request clarification from XSEDE of the SDSC CA with respect to IGTF accreditation and whether it is needed by XSEDE users to be included in OSG CA bundles.  
  
**InCommon Integration Account Linking and Federation:** XSEDE allows its users who are associated with InCommon member institutions to use their campus authentication credentials to access XSEDE resources. From the OSG perspective, there are no technical problems with this XSEDE authentication system; it can work with OSG resources readily. However, there is a potential policy issue that we need to investigate. XSEDE has a list of InCommon Identity Providers that XSEDE accepts credentials from (<https://go.teragrid.org/>); we may need to ensure that OSG resource providers are OK with these IdPs. The document says that XSEDE Security Operations Group reviews and adds new IdPs to this list. We recommend that OSG examines the XSEDE policy for adding new IdPs and investigate how this aligns with local policies of OSG resource providers.   
  
Just as an example, the XSEDE IdP list currently includes ProtectNetwork as an accepted IDP. We know that this IdP is not accepted at Fermilab. The XSEDE also notes that ProtectNetwork membership will be removed in January 2012 (although it is not removed yet?); so this particular IdP most likely will be a non-issue.   
  
**Science gateways and OAuth protocol**: The document says that when science gateways are used to access “community accounts” with shared credentials, XSEDE gateways generates a proxy for each user and adds a SAML assertion into the proxy. This is done for accounting purposes. I assume that the XSEDE accounting system will know how to process the SAML assertion. On the other hand, OSG accounting system will most likely need some new capabilities developed to process the assertion. I recommend that a person from accounting team should evaluate this issue.