XSEDE Certificate Authority Requirements, Use Cases and Proposed Implementation

January 24, 2012

Victor Hazlewood, CISSP
victor@utk.edu

Jim Marstellar
jam@psc.edu

Introduction

The XSEDE project, begun in July 2011 and the successor to the NSF funded TeraGrid Cyberinfrastructure project, has identified the need for the development and implementation of a Certificate Authority for the XSEDE project that will satisfy the requirements and use cases of the XSEDE cyberinfrastructure into the future. This future includes a wider expansion of users and service providers to be part of a coordinated national cyberinfrastructure who provide any number and type of resources and services to a local, regional and/or national cyberinfrastructure. This can and likely will include NSF and other federally sponsored high performance computing centers and resources, university or campus computing centers and resources, private and/or public research and medical centers, industrial high performance computing centers and resources, special purpose research devices and various other current and future resources that could connect to a cyberinfrastructure.

The XSEDE cyberinfrastructure will likely will be a larger set of organizations than existed in the TeraGrid and will likely continue to grow in the future due to the national cyberinfrastructure and campus bridging goals of the XSEDE project. These goals and the requirements and use cases described below give support to the recommendation that the XSEDE project, lead by the Cybersecurity group of the XSEDE Operations division, should develop, document, accredit and implement an XSEDE Certificate Authority. This XSEDE CA should have the flexibility in its design and implementation to meet the current and expected future needs of the XSEDE project including existing and future XSEDE users and service providers. The XSEDE CA design should have the capability, flexibility and be implemented to support the current and future XSEDE user and XSEDE Service Provider certificate needs defined by the requirements and use cases outlined below.

Requirements

Understanding stakeholder requirements is an important part of the XSEDE cyberinfrastructure planning, design and implementation processes. The XSEDE proposal process included high-level requirements collection and derivation and a subset of these requirements give insight into the high-level requirements for an XSEDE CA. The XSEDE proposal included stakeholder requirements identified by a number of methods. These requirements were compiled into a Systems Requirements Specification (SRS) document, XSEDE document XSEDE-PD3.7-SRS.pdf, which is continuously updated and maintained by the XSEDE Systems and Software Engineer. The following table details the subset of the XSEDE requirements related to an XSEDE CA.

Table 1: XSEDE High-level Requirements related to an XSEDE CA

ID	Requirement title and short description
Security Requirements	
XR99	C.3.2.1 Secure Access
	Provide secure access to resources that protect both user and resource
XR101	C.3.2.3 Strong Authentication
	Provide at least one strong authentication mechanism.
XR102	C.3.2.4 Interoperability with Federated Identity Systems
	Provide the capability to integrate with academic/research organizations for identity management and authentication (e.g., build on the InCommon Federation)

	to establish collaborative trust.
XR104	C.3.2.6 Authorization
	Ensure access control throughout the XSEDE using appropriate access control rules for data files, applications, services, storage systems, computational systems and other devices or resources.
XR105	C.3.2.7 Secure Interfaces for Gateways
	Support access from Gateways to the XSEDE file system through "mount" operations, to Web services via a services access layer, and to XSEDE resources in general via standard APIs (e.g., SAGA).
XR106	C.3.2.8 Identity Management and Delegation
	Users shall be able to select one or more identities and corresponding credentials (individual or institutional) and produce a delegated credential that provides access to resources.
Workflow requirements	
XR27	C.1.4.4 Workflow integration with Job Managers
	Support interoperability between the workflow environment and the job management systems available in XSEDE
XR28	C.1.4.6 Extensive Menu of Supported Workflow Tools
	Provide graphical user interface (GUI), command line, and application programming interfaces (APIs) to supported workflow capabilities.
XR29	C.1.4.7 Workflow Management
	Provide mechanisms to manage work and data flows across XSEDE resources
Portals, Gateways and Campus Federation requirements	
XR73	C.1.8.2 Mechanisms for Federating Campus Clusters
	Provide consistent mechanisms for federation with campus clusters
XR74	C.1.8.3 Integration with Local Computing Resources
	Provide a mechanism for a user to attach a local compute or storage resource, that satisfies a defined protocol standard, to the common user environment so that the user can exploit it from the common user environment as if it were an XSEDE resource.
XR75	C.1.8.4 Mechanisms for Federating Independent Data Grids
	Identify standards and mechanisms to support the federation of independent data grids
External Interface, User interface requirements	
XR78	C.2.1.1 Workflow Graphical User Interface Tool
	Provide a workflow graphical user interface (GUI) for use by XSEDE users
XR79	C.2.1.2 Workflow Client Command Line Tool
	Provide a client command line tool for use by XSEDE users
XR80	C.2.1.3 Workflow Application Programming Interface
	Provide access to application programming interfaces (APIs) for supported workflow engines
Useability, Common Environment requirements	
XR124	C.3.5.1.6 Client-Side Toolkit
	Provide access to XSEDE client-side resources (including data access) from Linux, Macintosh and Windows desktops, including easy-to-download clients, e.g., GridFTP, XSEDE/Unicore command line interface.
XR132	C.3.5.8 Seamless Federation
	Support seamless federation between on-campus and system resources: in particular, and to the greatest extent possible, common authentication and user environments shall be used.
Enterprise Requirements, Training, Education and Outreach requirements	
XR168	D.1.6 Provide campus bridging

	Provide campus bridging for users to access XSEDE resources; assist campuses in balancing the use of local, regional and national resources.
Advanced User Support requirements	
XR186	D.2.2 Provide Advanced Community Capabilities Support
	Support efforts to optimize, harden and deploy the software systems necessary for research communities to collaborate and create new knowledge using XD resources and related technologies. Facilitate the effectiveness of research groups whose members are geographically distributed but are pursuing common research and education objectives
Coordination and Mgmt Service requirements	
XR233	D.3.3.2 Support Interoperability
	Support interoperation of national cyberinfrastructures worldwide and incorporate campus centers as well as national, corporate, and individual research laboratories.
XR234	D.3.3.3 Protect XSEDE Users
	Provide an environment that is open but at the same time protects user confidentiality, integrity and availability. (e.g., to their data and resources). Provide a security model that maps to the XSEDE architecture and is understandable by stakeholders.
XR201	XR201 D.3.4.2 Provide Online Services
	Provide an XSEDE User Portal, automatic distributed accounting and account management, authentication services, XSEDE website, documentation, tools for the use of distributed XSEDE resources including science gateway support and the ability to submit work through a single system view of XSEDE resources
XR204	XR204 D.3.4.5 Provide Deployment and Monitoring
	Provide support for software deployment and continuous monitoring of XSEDE Capabilities including acceptance testing and monitoring of production resources and services
XR206	XR206 D.3.4.7 Implement Best Cybersecurity Practices
	Implement best cybersecurity policies and procedures including an available, shared certificate authority spanning all XD Service Providers, if possible

Use Cases

XSEDE use cases include those use cases identified in the XSEDE proposal document Architecture Use Cases (XSEDE-PD3.6-ArchUseCases.pdf), the use cases continuously being discovered by the XSEDE Systems and Software Engineering process, and by other methods. The XSEDE Architecture Use Case document is included in Appendix A and includes nine use cases for XSEDE. The three XSEDE proposal use cases listed in Appendix A and indicating use of grid technologies that relate to the need for an XSEDE Certificate Authority include the following

- D.1 Workflow/Science Gateway/Problem Solving Environment
- D.2 Data Grid Application
- D.9 Grid Interoperability

Specific examples of the three use cases listed above include: the thirty-five XSEDE Science Gateway projects which are examples of D.1; MotifNetwork, Ocean Observatories Initiative, Large Synoptic Survey Telescope and the uses of iRODS (http://www.irods.org) are examples of D.2; the interoperability of XSEDE with local university resources and local research centers and institutes are examples of D.9. Examples of grid interoperability includes the interoperability of Open Science Grid (OSG) with XSEDE and the interoperability of PRACE, the Partnership for Advanced Computing in Europe. These examples, however, illustrate examples of interoperability with grids that already have their own certificate authorities and do not require the implementation of an XSEDE CA for interoperability.

In the XSEDE resource environment and in the XSEDE campus bridging initiatives the XSEDE Software and Services that employ X.509 Public Key Infrastructure technologies would provide the grid technology toolsets for use by these use cases. The XSEDE Software and Services capabilities include, but are not limited to, Globus technologies (Globus toolkit, gridftp and gram) and Unicore technologies (Unicore BES, Unicore command-line client, and Unicore Rich Client). The issuance of X.509 user, host and service certificates in this cyberinfrastructure is needed to implement the use cases.

Additional use cases determined recently and not yet incorporated into the XSEDE Architecture Use Cases document include the use cases determined as a result of the XSEDE Call for Proposals for the Early Adopter Program for Campus Bridging. Seventeen proposals were submitted as a result of the call for proposals. These proposals identify grid interoperability between local and XSEDE resources or use of XSEDE grid technologies that would benefit from an XSEDE CA and significantly reduce the universities and/or research centers need for accrediting and implementing their own CAs. These proposals are not available for inclusion into the Appendix, but the following use cases are a few translated, representative examples from the seventeen proposals that demonstrate grid interoperability or use of grid technologies:

- Submission 1: Integration of a medical center compute cluster with regional biomedical HPC resources
- Submission 2: Integration of compute resources at two state universities supporting 600 researchers and the ability to scale up to XSEDE resources from the state resources
- Submission 3: Development of a university research institutes capability in using grid technologies for data management to reuse, share and avoiding multiple copies of the same data including university researchers using their data located on local and/or on national supercomputing facilities from their desktops
- Submission 4: Use grid technologies starting with a single researcher familiar with the TeraGrid to access university and XSEDE HPC resources, then expand the use of XSEDE grid technologies to other researchers using the university HPC resources, finally expand the use of XSEDE grid technologies for university research across the university and XSEDE resources
- Submission 12: Computational biology and computational chemistry are mature methods for investigating the atomic and molecular properties of materials. Many of the tools for conducting such studies (e.g.NAMD, Amber, Gaussian, GAMESS) have been optimized for parallel and/or high throughput execution on shared XSEDE resources, as well as, execution on local, possibly sole user, cluster and interactive workstation environments. The problem for the computational materials scientist is thus not so much one of capability but simply ability and making use of grid technologies to efficiently utilize widely distributed heterogeneous cyberinfrastructure to conduct thousands to tens of thousands of high-performance computations

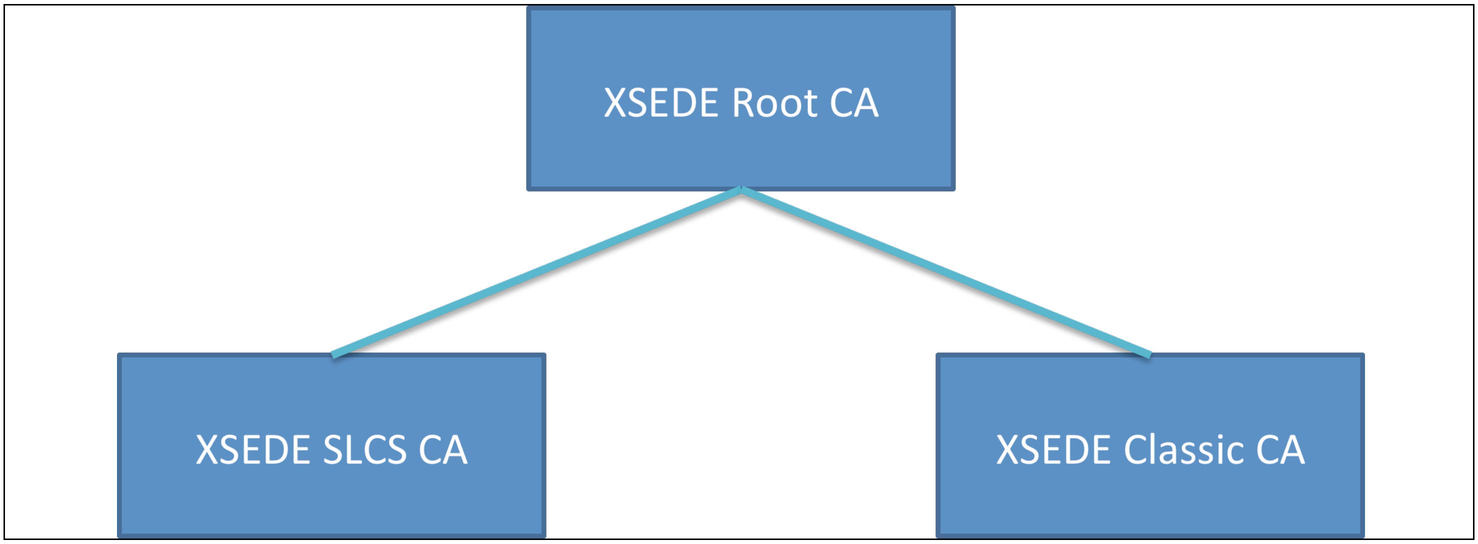
Implementation

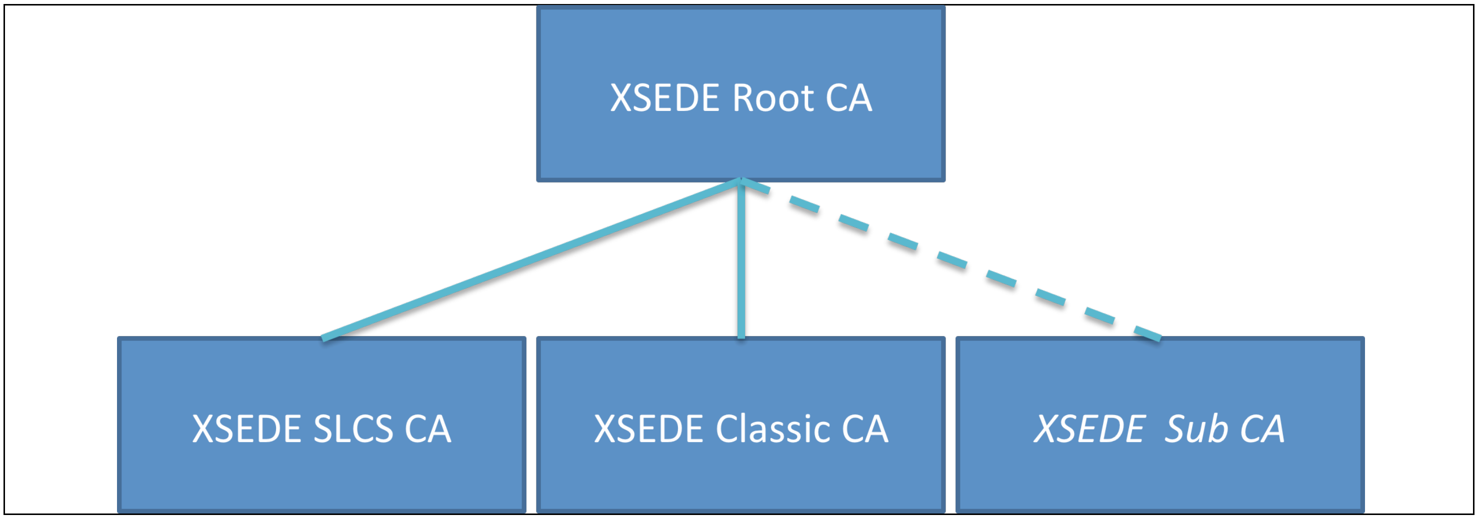
The XSEDE requirements and use cases identify the need for the issuance of X.509 user, host and server certificates for use with Globus and Unicore technologies as mentioned previously. If the solution to the XSEDE use cases and deployment of grid technologies for XSEDE Service Providers and campus bridging initiatives involves each Service Provider and each campus bridging organization to develop, design, accredit and implement their own Certificate Authorities (CAs), it is expected that there will be a significant increase in the number of separately accredited CAs. In order to reduce the number of CAs that will be needed in this new research cyberinfrastructure being deployed by XSEDE, XSEDE proposes to implement a CA with multiple Registration Authorities, an XSEDE root CA with one or more subordinate CAs as necessary similar to the CA hierarchy of the DOEGrids CA. The DOEGrids CA CP/CPS describes this CA hierarchy in section 1.3.1

"…A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. CAs may be organized in a hierarchy in which an organization's CA issues certificates to CAs operated by subordinate organizations, such as a branch, division, or department within a larger organization."

It is proposed that XSEDE initially have one XSEDE root CA and two subordinate CAs: a subordinate classic CA for issuing long lived host and service certificates and one subordinate short lived certificate service (SLCS) for issuing short lived user certificates. This is shown in Figure 1. XSEDE is expected to grow by adding service providers at different Tier levels: Tier 1 is the NSF mandated service providers, Tier 2 is the voluntary service providers who provide some allocatible resources to XSEDE and Tier 3 which includes voluntary service providers who wish to join the national cyberinfrastructure as a convenience without having to deploy a separate non-interoperable cyberinfrastructure. As XSEDE continues to grow by adding formal Service Providers and extending the cyberinfrastructure by campus bridging initiatives it is expected that the organizations can use the XSEDE CA and the issued certificates to interoperate with the XSEDE cyberinfrastructure as a Service Provider, Virtual Organization or campus bridging participant. Each of the organizations when they join XSEDE can become an XSEDE Registration Authority to help with identification and authorization of certificate applicants. In very infrequent cases, one or more organizations that participate in XSEDE may be able to define requirements and use cases that lead to the clear need for the XSEDE partner to have its own SLCS CA for issuing user certificates and/or, perhaps, their own classic CA for issuing host certificates. It is proposed that the XSEDE CA would be able to issue these CAs as subordinate CAs to the XSEDE root CA following the XSEDE CP/CPS when this need arises. It is expected that XSEDE Service Providers may even be able to retire existing organizational CAs and use an XSEDE CA instead. For example, if the XSEDE CA issues an SLCS that implements two factor authentications, NICS may decide to retire their NICS SLCS two factor CA.

Figure 1: XSEDE CA





Appendix A

XSEDE Architecture Use Cases