OSG Certificate Authority Implementation Plan

Von Welch

March 6th, 2012

*** * DRAFT * ***

Executive Summary

The Open Science Grid (OSG) operates a public key infrastructure (PKI) as part of its identity management system to allow for authentication of users and services, and to allow for the expression of virtual organization (VO) membership. A key component of the OSG's PKI is a certificate authority (CA) operated by ESnet: the DOE Grids CA. DOE is transitioning out of the business of operating the DOE Grids CA. OSG evaluated its options and concluded it needed a CA whose policies were tailored to its needs.

The OSG performed a Pilot evaluation between November 2011 and February 2012. The Pilot and its recommendations are captured in a separate document. This document describes the plan looking forward for OSG establishing its own CA and transitioning users from the DOE Grids CA to OSG's new CA.

The plan includes contracting with DigiCert, a commercial company, to operate a CA for OSG interfaced to a web application front-end developed and maintained by OSG for its user community. The phases of the project, looking forward, include: A Planning phase to enact the detailed technical and project planning through to stable operations; a Development phase to construct the OSG front-end and integrate the end-to-end solution; a Deployment phase to deploy the OSG front-end in conjunction with the DigiCert CA, complete and exercise the operational processes; a Transition phase in which OSG users are migrated from the DOE Grids CA to the new OSG CA; and an Operations phase during which OSG fully supports their CA in production and the DOE Grids CA can begin the process of ceasing to provide services to the OSG user community.

Table of Contents

1 INTRODUCTION 3

2 GOALS 4

3 NON-GOALS 4

4 PROPOSED TIMELINE 5

5 PLANNING PHASE 5

6 DEVELOPMENT PHASE 7

7 DEPLOYMENT PHASE 7

8 TRANSITION PHASE 8

9 OPERATIONS PHASE 8

10 REFERENCES 8

1 Introduction

The Open Science Grid (OSG) operates a public key infrastructure (PKI) as part of its identity management system to allow for authentication of users and services, and to allow for the expression of virtual organization (VO) membership. Unlike the identity management (IdM) system of most cyberinfrastructure projects, OSG's IdM system is, following OSG's Blueprint for community organization [6], VO-centric – that is membership, registration and other IdM functions are initiated and managed by the VOs rather that OSG itself. This creates unique challenges for OSG IdM and the PKI supporting it.

A key component of the OSG's PKI is a certificate authority (CA) operated by ESnet: the DOE Grids CA. DOE is transitioning out of the business of operating the DOE Grids CA [2]. OSG evaluated its options [1] and concluded it needed a CA whose policies were tailored to its needs and can not at this time rely on an existing (or combination of existing) CA operated by a third party. Given this decision, the two options apparently available to OSG were choosing between setting up its own CA, or contracting with DigiCert[1], a commercial company, to operate a CA for OSG.

A pilot, running from November 2011 through January 2012, was initiated to determine if contracting with DigiCert is a viable option for OSG. Additionally, if contracting with DigiCert is a viable option, could OSG establish a front-end service that both put the user[2] experience under the control of OSG and could allow OSG, at some unspecified later date, to migrate from DigiCert to another CA without changing the user experience? The Pilot Report [13] concluded that contracting with DigiCert and establishing an OSG-operated front-end are viable options.

This document builds from that recommendation to lay out a plan for establishing a new OSG CA and front-end web application, transitioning OSG users from the DOE Grids CA to the new OSG CA, and ceasing services from the DOE Grids CA to OSG.

The implementation plan will be regularly evaluated during its execution and any significant changes in timeline and delivery expectations communicated to all parties (including the agencies).

The implementation of this plan will be regarded as complete at a date during the Operations Phase when the OSG CA is in stable operations, and users are routinely able to receive and use the certificates. These metrics will be defined in detail in the Planning Phase.

---

[1] http://www.digicert.com/

[2] The term "user" in this document is used to indicate a user of the OSG PKI, which includes members of OSG VOs, VO registration authorities agents and administrators of contributed resources (aka "GridAdmins").

2 Goals

There are a number of goals for the implementation of the OSG CA. Goals are listed in no particular ordered, but are numbered to allow for reference.

1. Allow for the cessation of ESnet's DOE Grids CA services to OSG as soon as reasonably possible, congruent with other goals. Make decisions cognizant of the total costs during the implementation and transition.
2. Provide a high-quality usable dependable OSG CA service that is owned and operated by the OSG project for the for-seeable future.
3. Keep the OSG user community well informed during the transition and ensure they have sufficient training and knowledge to use the new CA service.
4. Allow OSG to control the user interface to it's CA service, allowing it to both provide the most user friendly experience possible and change providers in the future with minimal disruption to its user community.
5. Given that OSG has interest in exploring other identity management options, create no new barriers to doing so.
6. Allow for the support, based on specific agreements, of user communities currently using the DOE Grids CA but who are not part of the OSG user community.
7. Minimize disruption to OSG user communities by avoiding disruptions during critical times in their science schedules. E.g., LHC runs [14].
8. Ensure ongoing capture, storage and retrieval by the OSG services of all relevant logging and request information available from DigiCert.
9. Ensure controls and management in place to monitor the contract with DigiCert and give ample warning of and time for any changes needed (e.g. if the maximum number of certificate authorizations is above some threshold).
10. Define metrics that will mark the end of the Implementation Project (the project defined by this document.

3 Non-Goals

1. It is not a goal to support automated transition of certificates registered with the ESnet DOE Grids CA to the OSG CA.
2. It is not a goal at this time to provide a generalized service for all DOE or NSF science communities or facilities.
3. It is not a goal to serve OSG user communities outside of the U.S.

4 Proposed Timeline

In this section we propose a timeline for development and deployment of the new OSG CA, and transition of the OSG user community from the DOE Grids CA to that new CA. The timeline is composed of discrete phases: Planning, Development, Deployment, Transition and Operations. A Pilot phase has already been completed.

Factors that were taken account in this timeline include the desire to cease OSG's use of ESnet services as soon as reasonable, OSG's desire to create a usable, reliable, well-tested CA service, and the desire to avoid changes to the OSG LHC user community during their current run, which goes until Nov 23, 2012 [14].

The proposed timeline is graphically depicted in Figure 1 with the phases described in the subsequent sections. The depicted timeline includes a one month delay of the Development and subsequent phases requested by OSG and DOE in order to establish funding for those phases.

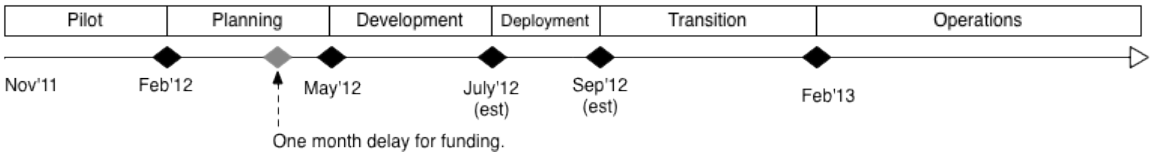

Figure 1: Proposed Timeline for OSG CA Deployment and Transition

5 Planning phase

The planning phase should commence as soon as possible with the goal of completing by the end of April 2012. The goals of the planning phase are:

- Develop a technical plan, timeline with milestones, and acceptance test plan for development, deployment and transition to stable operations of the OSG CA front-end web service and supported clients (e.g. certificate require scripts). This plan needs to take into account:
    - OSG's audit, accounting, and access control requirements.
    - Acceptance testing should consider Integration TestBed (ITB) of certificate from the new OSG CA.
    - What client software needs to be modified, who will do it, and what support they need.
- Develop a training plan for OSG Registration Authorities and Grid Administrators. This includes an initial one-hour presentation at the OSG All Hands Meeting in March 2012 and the development of a short YouTube video on how to use the front end.
- Develop a communications plan for OSG users.
- Develop a plan for how OSG and DigiCert will interact, in terms of technical issues (REST API changes), user support issue resolution, security

incidents/alerts and business processes (e.g. change management, reporting and planning).

- Develop a plan for handling the change in user's distinguished names that results from a change in CA[3].
- Understand the impact of the change in CRL lifetime from the DOE Grids PKI (1 month) to DigiCert CA (1 week) will have on the OSG and develop a plan to cope with that change.
- Define the administrative operational services (monitoring, alarming) to be developed and deployed for operation of the OSG CA.
- Document what operational changes will come about from the CA transition and plan for addressing those changes.
- Document what policy and contingency plan changes need to be made and develop a plan for addressing those changes. See Appendix A for a list of known issues to be addressed in the Contingency plan.
- Develop a transition plan with a list of users (current OSG users and any agreed upon identified DOE Grids user communities) who should be invited to try out the new OSG CA and a timeline for their invitation.
- Document any users of OSG that are currently using the DOE Grids CA whom should be transitioned to another CA, and develop a plan for transitioning those users. E.g., users in Korea [15].
- Develop a project plan for the all these activities. This should include a detailed timeline for the Development, Deployment and Transition phases and the transition to Operations.
- Complete the execution of legal and policy agreements with DigiCert started during the Pilot phase.

A Planning Team will be assembled for the planning phase. This team will include:

- A representative of ESnet.
- A representative from DigiCert.
- One or more representatives from the OSG Operations, including minimally the OSG RA.
- Representatives of production teams for major OSG VOs including US ATLAS and US CMS.
- Personnel experienced with web application development to complement the Pilot team's expertise with the DigiCert API.

[3] Both the UK NGS and Fermi National Laboratory have undergone similar name transition and we will leverage their experiences in the Planning phase.

- Communications liaison.
- A member from OSG's ITB team.

A connection will also be made to the OSG Software Team lead, since any software developed will be owned and maintained by the OSG software area.

6 Development Phase

The development phase should commence as soon as planning is sufficiently complete. The length of this phase will be determined by the Planning phase. The goals of this phase are:

1. Develop the OSG CA web service front-end and integrate with the DigiCert CA through the REST API and the administrative components to be used in operation of the service.
2. Review by the OSG software area of the resulting code and support documentation.
3. Commence work on operational, policy and other changes defined in the Planning phase.
4. Commence the implementation plan for the Contingency Plan for the event that the DigiCert CA becomes unavailable for an extended period (to be defined in the planning phase) for any reason.
5. Perform acceptance testing as defined in the Planning Phase.
6. Revisit the deployment and transition plan based on lessons learned in the initial testing.

7 Deployment Phase

The Deployment phase should commence as soon as development of the CA web service front-end is complete. The goals of this phase are:

1. Deploy the OSG CA - the OSG web front-end and operations components, in conjunction with the DigiCert CA - such that it is available for the start of Transition.
2. Complete work on operational, policy, and other changes defined in the Planning phase.
3. Complete the implementation plan for the Contingency Plan and have an internal OSG review of the plan.
4. Refine the software components based on the experience of the deployment phase. Transition the software to production and maintenance under the responsibility of the OSG software area.

At the end of this phase, a meeting will be held between OSG, DOE and ESnet at which a recommendation will be presented to initiate the transition phase.

8 Transition Phase

The goals of this phase are:

1. Transition, gradually, all OSG users and other identified DOE Grids user communities from using the DOE Grids CA to the new OSG CA.
2. Correct usability and other flaws as exposed.
3. Perform an end-to-end test of the contingency plans and address exposed flaws.
4. Have an external review of contingency plans performed.

9 Operations Phase

The goal of this phase is the continued operation of the new OSG CA. Once this phase is reached, the OSG will not long require certificate issuance from the DOE Grids CA. OSG will require a one-year period where the DOE Grids CA continues to issue CRLs and then will have no dependencies on the DOE Grids CA.

1. OSG operations will maintain responsibility for operations and monitoring of the service and the Registration Authority.
2. OSG operations will measure the metrics defined in the Planning Phase.
3. OSG software will maintain all code developed.
4. OSG security will monitor the security of the services and execute the contingency plan if/as required.
5. OSG will promote the re-registration with the OSG CA of existing DOE Grids Certificates, thus making the dependence on the DOE Grids CA end as soon as possible.

Once the operations metrics defined as “End of the OSG CA Implementation Project” are achieved a recommendation will be made to the OSG Executive Team to declare the project complete. At this time we expect a final meeting and discussion between ESNET, DOE and OSG.

10 DOE Grids PKI Perspective

The following table shows the relationship between this implementation plan and the requirement for operation of the DOE Grids PKI.

Phase(s)	Changes for requirement of operation of DOE Grids PKI

Planning, Development and Deployment	None
Transition	Issuance load will begin to lessen as users are shifted to OSG PKI.
Operations Phase	No new certificates will need to be issued, but regular revocation procedures and CRL issuance needs to continue.
One year after Operations Phase commences (when all DOE Grids PKI certificates have expired)	DOE Grids PKI can be shut down.

11 References

1. James Basney, Mine Altunay, Von Welch. *Options and Recommendation for Replacement of the DOE Grids CA in the OSG PKI*. OSG-doc-1077, 2011.
2. Lauren Rotman. "DOE Grids Certificate Service update/transition." Email communication, December 2, 2011.
3. Information System Contingency Plan (ISCP): DigiCert CA Service. https://twiki.grid.iu.edu/bin/view/Security/DigiCertContingencyPlan2012
4. DigiCert-Grid Repository. http://www.digicert-grid.com/
5. DigiCert Managed PKI Pilot Agreement. Signed contract between DigiCert and Indiana University (on behalf of OSG), November 1, 2011.
6. OSG Blue Print. OSG Document 18-v12. March 4, 2011. http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=18
7. DOEGrid-statistics-by-agency-correct-2.xls. Provided by ESnet staff.
8. OSG Registration Authority Information. https://twiki.grid.iu.edu/bin/view/Security/OsgRaOperations
9. OSG Registration Authority Agents. https://twiki.grid.iu.edu/bin/view/Security/OsgRaAgents
10. Testing of new CA distribution format on ITB. https://twiki.grid.iu.edu/bin/view/Security/ITBDigicertTesting
11. Personal email correspondence with Brian Bockelman.
12. Personal email correspondence with Rob Quick.
13. Mine Altunay, Jim Basney, Jeremy Fischer, Chander Sehgal, and Von Welch. OSG DigiCert Pilot Report Draft. Feb 18th, 2012.
14. 2012 LHC Schedule V1.1. January 17, 2011. https://espace.cern.ch/be-dep/BEDepartmentalDocuments/BE/LHC_Schedule_2012.pdf

15. Personal email correspondence with Maria Dimou, OSG LHC Registration Authority Agent.

Appendix A Known Contingency Plan Issues to address.

This gives a first list of the issues identified with the current contingency plan draft. As part of the OSG CA Implementation Project we will complete the plan, perform internal and external reviews and test its implementation under realistic conditions. This last might not happen until the beginning of 2013.

- A step-by-step process for a compromised CA, RA or other trusted entity.
- Under what circumstances does OSG 'shut down'?
- Is one week enough to deal with lack of CRLS?
- Establish contingency agreements for use of alternate CA providers in emergencies.
- Replicate DigiCert certificate information in an OSG hosted database to enable recovery when DigiCert is unavailable.
- Establish processes to notify and request certificate holders to renew certificates at least one month in advance of expiration, to minimize disruption during short-term CA service outages.
- Clearly define processes for compromised of trusted parts of the OSG PKI infrastructure, including RAs, GridAdmins, the CA itself, and, assuming the relevant route is chosen, the OSG front-end.
- Does the contingency plan include recovery or is that a separate plan?
- The role of Deputy Security Officer is currently vacant.
- Responsibilities of actions should be clearly assigned to different groups in OSG.
- Consider implications of and alternatives solutions to the issue of DigiCert CRLs having a one-week lifetime (as compared to one month with DOE Grids PKI).
- The plan should include notification of the Fermilab Office of Communications in the event of incidents severe enough to attract attention of the press.
- Does XSEDE have a plan we could leverage?