New OSG PKI Transition Plan

DRAFT May 15th, 2012 DRAFT

Von Welch, Jim Basney

# Introduction

This document lays out a transition plan with a list of users (both current OSG users and other identified DOE Grids user communities) who should be invited to try out the new OSG CA and a timeline for their invitation.

The Transition Phase will start in October 2012 and run through January 2013, after which the DOE Grids PKI stops issuing new certificates and the OSG PKI enters Operations Phase. After that time OSG users will use the new OSG PKI instead of the DOE Grids PKI for their certificate needs.

# Goal for Transition Phase

The goal for the Transition Phase is to develop confidence in the OSG PKI by demonstrating that it can handle OSG certificate needs by shifting an increasing fraction of the user community’s requests for new certificates over the period from the DOE Grids PKI to the OSG PKI.

It is not a goal during the Transition Phase to force anyone to utilize the OSG PKI instead of the DOE Grids PKI or to forcibly remove DOE Grids PKI certificates from use. The expectation is that as users need new certificates, either renewals or for new entities, they will choose to use the DOE Grids PKI or the OSG PKI, with increasing encouragement over the Transition Phase to use the OSG PKI.

Of note is that September and October are historically peak months for DOE Grids PKI certificate requests [3] and given that the OSG PKI will be relatively newly providing service in October, it would be unwise to drive too much usage to it during a peak month.

After the Transition Phase completes and the Operations Phase is entered, the DOE Grids PKI will cease issuing new certificates and as DOE Grids PKI certificates expire, entities will need to use the OSG PKI to obtain new certificates. Again, there will be no attempt to force replacement of DOE Grids PKI certificates; it will be allowed to happen as desired by the OSG user community (presumably on natural expiration of the certificates).

Given that the DOE Grids PKI handles roughly a 1000 certificate requests in an average month (September and October aside) [3], it is the goal of the Transition to reach that level of service by February if not earlier. Working backwards from that goal, the following goals for monthly issuances during the Transition Phase are proposed:

|  |  |
| --- | --- |
| Month | Issuance Goal |
| October | 250 |
| November | 500 |
| December | 750 |
| January | 1000 |

Table : Issuance goals for new OSG PKI by month.

Summing up the per-month issuances indicates that the goal for total issuances during the Transition Phase is 2500 certificates, or slightly less than a quarter of the total issuances in a year by OSG.

# The Need for Trusted Agents

Before a user can use the OSG PKI, there must be a Registration Authority Agent (RAA) or Grid Admin (GA) that is authorized to vet request for user or host certificates, respectively, submitted by the user. This means that the establishment of appropriate Trust Agents must precede the use of the PKI by each user group. The registration process for Trusted Agents for the OSG PKI will be very similar to the registration process used by DOEGrids:

* Applicants for Trusted Agent roles must first obtain a user certificate from the OSG CA following normal procedures.
* Then, the applicant must send a digitally signed email message requesting authorization. Email request templates will be provided. The message must be digitally signed with the applicant’s OSG user certificate.
* If the applicant’s request is in order, the OSG Registration Authority (RA) approves the Trusted Agent authorization in the OSG Information Management System, which serves to authorize the specific OSG user certificate to act in the approved Trusted Agent role. For Grid Admin requests, the OSG RA registers the approved DNS domain(s) as needed.
* The OSG RA notifies the applicant that the request has been approved and that the applicant can now act in the Trusted Agent role.

To bootstrap this process, the OSG Registration Authority (RA) will approve issuance of user certificates to an initial set of Trusted Agent candidates. The OSG RA will contact the current RAAs and GAs for each VO/site one month prior to the transition phase for that VO/site, per the below transition timeline, and request that the RAAs and GAs obtain user certificates and apply for their current TA status per the above process using their new certificates. The OSG RA will identify current RAAs and GAs using OSG RA records.

# OSG User Communities and Domains

OSG is composed of VOs and resource providing domains. A list of current OSG VOs can be found at [2] and [3] provides an indication of the size of each VO. A list of domains, as determined by certificates issued by the DOE Grid PKI, can be found in [3].

As described in the Communications plan [4], the PKI team will start engaging the VOs and domains in the June/July 2012 timeframe to ensure they are prepared for the transition.

# OSG Transition Timeline

We group the users as follows:

* Internal: This group will be made up from PKI developers, GOC staff, other who have been involved with the PKI development and select members of the OSG User Community. This group will start testing near the end of the deployment phase (July 20th, 2012) and their experiences will be a major factor in deciding the system is ready to enter Transition Phase.
* First Wave Friendly Users: This group is composed of major stakeholders from the OSG community. This group will start testing the PKI at the start of the Transition Phase (October 1st, 2012). It is expected that within each stakeholder group there will be a self-selection of most tolerant users to test first.
* Second Wave Friendly Users: This group is composed of other large stakeholders within the OSG community and communities currently not formally part of OSG (e.g. ESG, NFC).
* General OSG user community: The entirety of the OSG user community.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Phase | Date | Registration Authority Agents | Grid Admins | User Community |
| Internal Testing (August) | Sep 19, 2012 | OSG GOC, Security staff | Open science grid, Indiana, Illinois, and FNAL domains | PKI developers, GOC staff, others involved with PKI development. |
| Friendly Users, First Wave (September) | Oct 1, 2012 | ATLAS, CMS, LIGO, other friendly VOs TBD | BNL, wisc.edu, ucsd.edu | Technical and friendly users from major stakeholders. |
| Friendly Users, Second Wave (October) | Oct 15, 2012 | NERSC, NFC, TBD | Remaining top ten OSG domains (mit.edu, ultralight.org, chicago.edu, ufl.edu, caltech.edu, unl.edu) | Technical and friendly users from other large stakeholders. |
| General OSG User Population | Oct 29, 2012 | Approach remaining VOs by size | Approach remaining domains by size | All OSG PKI users. |

As described in the Communications plan [4], one month before OSG andESnet encourage users of a VO to use the OSG PKI, the PKI team will engage with the VO or site to ensure it is ready.

# What are Priorities for Testing during Transition?

Top priority, required to leave Friendly User Testing:

* User certificate requests, both web and CSR-based
* Host certificate request, both individually and in bulk
* Revocation required by OSG Security Team
* Auditing of issuance

Low priority, can be addressed later in the process:

* Renewal
* User-requested revocation

# References

1. Virtual Organization Summary. http://myosg.grid.iu.edu/vosummary?all\_vos=on&active=on&active\_value=1&datasource=summary
2. VOMS Status. http://myosg.grid.iu.edu/vovomsstatus?all\_vos=on&active=on&active\_value=1&datasource=vomsstatus
3. Von Welch. OSG Certificate Usage Analysis. Draft. https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG-certificate-usage-analysis-3.pdf
4. DOE Grid Cert CA/OSG Transition Outreach and Communications plan, version 3. ESNET and OSG. https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/doegrid.transition.v3.doc