OSG PKI Transition Final Report

OSG-DocDB #1156
https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1156

Von Welch (vwelch@indiana.edu)
OSG PKI Transition Project Manager

Representing work by the OSG PKI Transition Team:
Mine Altunay, James Basney, Tim Cartwright, Keith Chadwick, Alain Deximo, Jeremy Fischer, Soichi Hayashi, John Hover, Viplav Khadke, Christiane A. Ludescher-Furth, Ruth Pordes, Rohan Mathure, Robert Quick, Alain Roy, Chander Sehgal, Mátyás Selmeci Anthony Tiradani and John Volmer

And PKI staff and management at ESNet:

Greg Bell, Patti Giuntoli, Dhiva Muruganantham, Lauren Rotman,

June 27th, 2013

Abstract

This report summarizes outcome of the OSG PKI Transition project spanning November 2011 through March 2013.

Executive Summary

The Open Science Grid (OSG) operates an 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 identity management system is a public key infrastructure (PKI) and certificate authority (CA), which generated certificates for users and services that are vetted by a set of trusted agents.

Since 2003, the OSG has utilized a CA operated by ESnet: the DOE Grids CA. In 2011, ESnet announced it would be shutting down the DOE Grids CA, and ESnet and OSG proceeded to work in collaboration to establish a replacement CA in the OSG suite of services. This effort was called the OSG PKI Transition Project.

The PKI Transition Project ran from November, 2011 through March, 2013 and involved establishing a replacement OSG PKI build around a commercial CA offering from DigiCert. As of March 23rd, 2013 the DOE Grids CA, stopped issuing new certificates and the OSG PKI is now successfully supporting the PKI needs of that community.

The Transition took about 2 FTE years of effort, which was about 10% over projections.

As part of the transition, collaboration with XSEDE on a joint PKI was explored, but not pursued due to programmatic and technical misalignment.

Contingency planning was undertaken to mitigate the risk posed by relying on DigiCert.

1 PKI Transition Project Overview

The Open Science Grid (OSG) operates an 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 identity management system is a public key infrastructure (PKI) and certificate authority (CA), which generated certificates for users and services that are vetted by a set of trusted agents.

Since 2003, the OSG has utilized a CA operated by ESnet: the DOE Grids CA. In 2011, ESnet announced it would be shutting down the DOE Grids CA, and ESnet and OSG proceeded to work in collaboration to establish a replacement CA in the OSG suite of services. This effort was called the OSG PKI Transition Project, though we note it was more a transition of responsibility than technical infrastructure, since a new CA was established in OSG.

The PKI Transition Project ran from November, 2011 through March, 2013 and involved establishing a replacement OSG PKI build around a commercial CA offering from DigiCert[1]. It was composed of six phases: a Pilot phase to prototype the planned PKI [11], a Planning phase to create a detailed project plan [12], a Development Phase to develop PKI software, services, policies and procedures [13], a Deployment Phase [14], a Transition Phase in which the new PKI started serving users [15], and an ongoing Operations phase.

2 Transition Project Outcome Highlights

- As of March 23rd, 2013 the DOE Grids CA, stopped issuing new certificates and the OSG PKI is now successfully supporting the PKI needs of that community.
- The DOE Grids CA will continue limited operations until March 2014 in order to provide revocation of existing certificates.
- The following communities, which were previously clients of the DOE Grids PKI but not participants in OSG, joined the OSG in order to utilize the PKI service: Argonne National Laboratory, Earth Systems Grid Federation, National Fusion Collaboratory, NERSC, and the Oak Ridge National Laboratory. The LIGO community chose not to transition for the DOE Grids PKI to the OSG PKI, and instead set up its own PKI infrastructure.
- The OSG PKI has met the requirements laid out in the Planning Report [11], namely compatibility with VDT, LHC interoperability/IGTF accreditation, supporting 2500+ users certificates vetted by 36 registration authorities, supporting 5000+ host certificates at over 80 sites, and ability to be sustained into the foreseeable future. A requirement to support secure web (https)

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

certificates was removed as it was determined it made policy requirements overly onerous by bringing in CAB Forum[2] compliance.

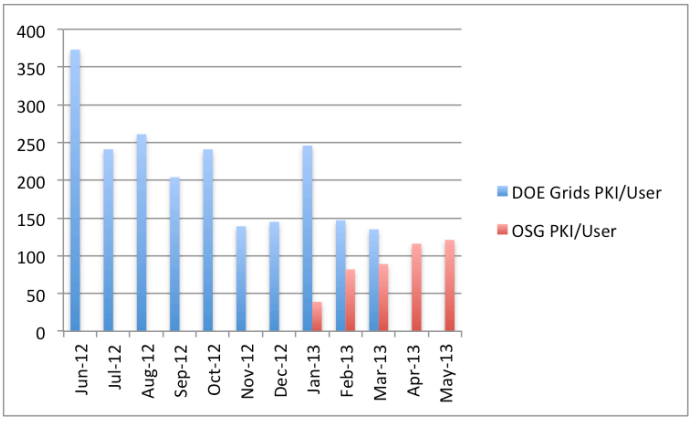

Figure 1: DOE Grids PKI and OSG PKI User Certificates Issued.

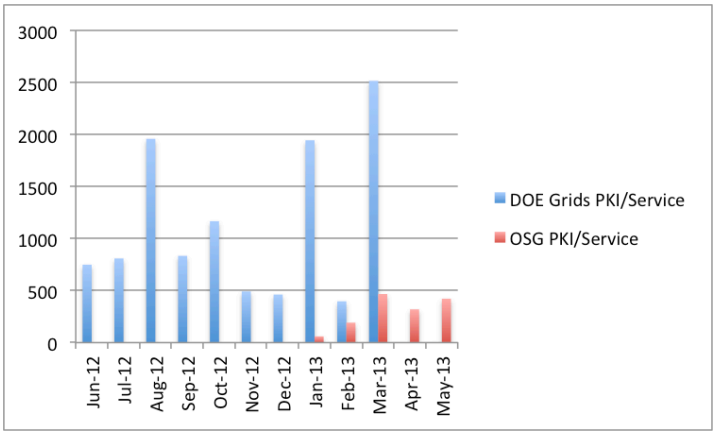

Figure 2: DOE Grids and OSG PKI Service/Host Certificates Issued.

3 Effort, Cost and Project Management Summary

The total effort for the Transition was approximately 2 FTE years, or about 10% over projection. Project management and effort details may be found at [15].

This does not count effort provided by ESnet. ESnet staff and personnel participated in regular calls with OSG to manage the transition, and

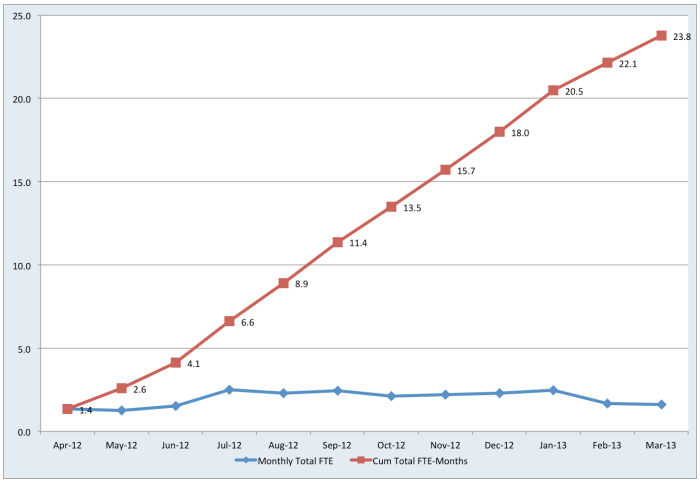

Figure 3: OSG PKI Effort by month and cumulative.

[2] https://www.cabforum.org/

provided invaluable statistics and other information on past PKI usage. It also does not count effort by the OSG VOs to update their procedures, policies and documentation.

Transition effort included existing OSG staff, plus additional effort at Indiana U. for management and software development. The additional effort at Indiana U. cost approximately $110,000 and was paid for via sub-contracts from Fermilab. (This amount includes a small contract with DigiCert for some initial services for evaluation.)

On going operational effort by OSG will be .5 FTE, an increase from .1 FTE utilizing the DOE Grids CA. The other major ongoing expense is a contract with DigiCert to provide CA services. The current contract is for two years (6/2012-5/2014), with an annual cost of $87,500. This cost is being split by US ATLAS and US CMS.

4 Notable Transition Events

4.1 XSEDE Collaboration Explored

During the transition, OSG and XSEDE held a meeting to explore collaboration in establishing a common PKI for the two projects [16]. It was decided not to pursue this collaboration at this time, primarily due to two factors:

1. Differences in timeline: at the time, OSG was 6+ months into the transition, with a firm deadline before the DOE Grids CA ceased providing service while XSEDE was just beginning their planning process.
2. Differences in identity management architecture: OSG and XSEDE have difference approaches to identity management that drive differences in PKI implementation and policy that were not obvious how to reconcile and would take more time to explore.

4.2 Contingency Planning

It was understood that reliance on DigiCert constituted a risk. To mitigate this risk, OSG undertook an analysis of contingency options [17] and developed plans [18] in the event DigiCert were unable to provide service.

4.3 DigiCert Audit

Part of OSG's obligations to DigiCert under the contract are participate in audits when requested. In early 2013, DigiCert requested OSG complete a self-audit, which OSG has done. It has been returned to DigiCert and we await their response.

5 Future Plans

5.1 Adopting Federated Identity and Other Solutions

OSG's PKI operates at a high level of assurance (IGTF[3]) to meet OSG's collaboration needs with the WLCG. A significant subset of the OSG community doesn't need this level of assurance and could adopt solutions with greater ease-of-use and lower cost. OSG is in the process of exploring federated identity (through CILogon) as a means of improving ease-of-user for its user community and reducing are ongoing[4].

5.2 DigiCert Contract Renewal

The current DigiCert contract expires in May 2014 and we expect to commence negotiations for a follow-on contract later in 2013 to have it place before it becomes a risk.

6 Lessons Learned

1. The process of breaking the project down into roughly three month phases, each with a report out and checkpoint for proceeding at the end worked well. One phase, at a month long, was too short and ended up being merged into another phase effectively. The checkpoint process does require stakeholders to be prepared to review in a timely manner or the project will be forced to progress without their feedback.
2. The VOs are extremely important to the operation of the PKI and hence were so for the transition. In retrospect, more effect should have been made to engage them earlier in the transition. The general process of holding a weekly phone call to engagement them, along with the OSG wiki[5] to keep notes and track progress, worked well.
3. The relationship with DigiCert to provide the back-end CA service for the OSG PKI worked well. Key to this was DigiCert's flexibility, both from a technical and policy standpoint, in support OSG's need for unusual (for a typical enterprise PKI) needs for bulk host certificates and a Trust Authority system distributed among many VOs.
4. Having the historical information and other insights from ESNet was critical to planning the transition. This allowed OSG to plan for anticipated usage, something that would not otherwise have been possible. A key insight during the transition is that the OSG would have benefits from knowing more about how all the various VOs used the PKI certificates in their workflows, and

[3] http://www.igtf.net/

[4] https://twiki.grid.iu.edu/bin/view/Management/Nov2012Newsletter#CILogon_Identities_gaining_broad

[5] https://twiki.grid.iu.edu/bin/view/Operations/OSGPKITransitionCallNotes

which of those workflows had a tendency to have the most problematic software stacks in terms of PKI (e.g., we would have tested the ATLAS Panda system earlier).

5. At the start of the project, OSG has requirements for the transitioned PKI to support both their Grid and Web (https) needs. It was decided to drop the requirement for Web needs as supporting secure web certificates would have meant meeting the more stringent Certificate Authority/Browser (CAB) Forum[6] policies (as opposed to just the IGTF[7] policies common to the LHC and other Grid communities).
6. The OSG chose not to use built-in browser functionality for PKI due to cross-browser variances in that functionality (this was based in part on recommendations from the CILogon project). This decision has worked out well.
7. As part of the transition, sites such as Argonne and Oak Ridge, joined the OSG and, for lack of a better model, were treated as OSG treats all of its scientific VOs. This approach worked without obvious problem.
8. OSG's need to support bulk host certificate requests (mainly for large clusters) is an unusual case and required significant effort during the transition to handle.
9. The OSG is primarily a software integrator as opposed to developer, this meant that services and polices that a development organization would have were lacking. In retrospect, the Transition Team could have benefited from more effort and/or expertise in software releases (QA/testing, and documentation), communication with the VOs, contracts (the arrangement between CMS/FNAL, ATLAS/BNL, IU and DigiCert took some effort to put into place), and PKI policies (mapping DigiCert's existing policies intended for an Enterprise to OSG's distributed structure was non-trivial).
10. OSG and ESnet had a different level of understanding about the Subscriber Data captured by DOEGrids CA. The underlying software used for DOEGrids CA doesn't provide tools for reporting and data analysis. OSG was gracious to accept the raw data from DOEGrids to do data analysis, such as volume of certificate expiration per month per virtual organization.

[6] https://www.cabforum.org/

[7] http://www.igtf.net/

7 References

11. Mine Altunay, Jim Basney, Jeremy Fischer, Chander Sehgal and Von Welch. *OSG DigiCert Pilot Report*. OSG-doc-1097, March2012. http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1097
12. OSG PKI Planning Phase Report. http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1120
13. OSG PKI Development and Deployment Phase Report. http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1145
14. OSG PKI Transition Phase report. http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1148
15. Transition Project WBS. https://twiki.grid.iu.edu/bin/view/Operations/OSGPKIProjectWBS
16. OSG-XSEDE Meeting Notes. https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1114
17. OSG PKI Contingency Analysis. http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1121
18. OSG PKI Contingency Plan. http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1115