OSG PKI Planning Phase Report

Von Welch <vwelch@indiana.edu>

Representing work by:
Mine Altunay, James Basney, Keith Chadwick, Alain Deximo, Jeremy Fischer,
Soichi Hayashi, Ruth Pordes, Robert Quick,
Lauren Rothman, Alain Roy, and Chander Shegal

Draft June 11th, 2012 Draft

Abstract

This report summarizes the activities of the OSG PKI Planning Phase
that officially completed on May 18th, 2012. The Planning Phase
included participants from ESnet, DigiCert, the ESGF, US CMS, US
ATLAS, the OSG Software Team, the OSG Security Team, the OSG RA,
the OSG ET and the OSG GOC. Participants convened weekly by
teleconference and used the OSG Twiki to share progress.

1   OSG PKI Planning Phase Goals and Accomplishments

This section lists the planning phase goals from the Implementation Plan [1], and
the progress achieved on each goal. A snapshot of the project management plan is
captured in Appendix A. More details can be found on the OSG Twiki [2].

1. 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 must be written and approved by the OSG Software Team
   (Alain Roy and team). 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.

   Completed: In summary, the OSG Information Management (OIM) system
   will be extended to act as the CA front-end. The interface is been kept as

1

similar to the DOE Grids PKI interface as possible, with the only substantial change being the shift of key generation from being in the user's web browser to the server to improve usability (see "OSG PKI key generation changes" document for details).

- OSG PKI System Design
    - https://docs.google.com/document/pub?id=1-noGy_JKaXP218k3jxtlbl--iuOUCNarL5vBDbxbSk
- OSG PKI key generation changes: Discussion of change from in-browser to in-server private key generation.
    - https://docs.google.com/document/pub?id=1j3EAe4J32SI5VGSCePi3WYzp6PUEFQjc1lJYo3DQt08
- OSG-PKI-Acceptance-Criteria: Acceptance criteria for new OSG PKI, with contributions from the OSG Software Team
    - https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG-PKI-Acceptance-Criteria-2.docx

A list of outstanding technical issues is being maintained in JIRA: https://jira.opensciencegrid.org/browse/OSGPKI

2. 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.

Completed: Presentation at AHM meeting was given and training plan is available at https://opensciencegrid.org/bin/view/Security/DigiCertTrainingPlan

3. Develop a communications plan for OSG users.

Completed:

https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/DOE_Grids_-_OSG_PKI_Transition_Communications_Plan_v4.doc

4. 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).

Underway, not completed: Clarification in how OSG will internally handle requests from DigiCert has been called for and will be addressed in the Development Phase. Current draft of the document is at: https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG-DigiCert-Interactions-3.docx

5. Develop a plan for handling the change in user's distinguished names that results from a change in CA.

    Completed:
    https://twiki.grid.iu.edu/bin/view/Security/DOEGrids2DigiCertDNTransition

6. 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.

    Removed as a task: DigiCert changed their CRL lifetime from one week to 30 days, making it equivalent to the DOE Grids CRL lifetime and removing the need for this task. Significant work was done with regards to this task, and is archived at:
    https://twiki.grid.iu.edu/bin/view/Operations/CRLChangeImpact

7. Define the administrative operational services (monitoring, alarming) to be developed and deployed for operation of the OSG CA.

    Not completed: Due to restrictions on personnel time this task has not been initiated and is scheduled for the first week of June.

8. Document what operational changes will come about from the CA transition and plan for addressing those changes.

    Completed:
    https://twiki.grid.iu.edu/bin/view/Operations/OSGPKIOperationalChanges

9. Document what policy and contingency plan changes need to be made and develop a plan for addressing those changes.

    Underway, not completed: This task has been initiated and is underway. A separate weekly call has been established to provide increased management oversight of this task. The responsibility for this task has also been shifted to the OSG Security Officer. The current version can be found at:
    https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1109

10. 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.

    Completed:
    https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG-PKI-Transition-Plan-5.docx

11. 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.

Completed:
https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG-certificate-usage-analysis-3.docx

12. 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.

Completed:
https://twiki.grid.iu.edu/bin/view/Operations/OSGPKIProjectWBS

13. Complete the execution of legal and policy agreements with DigiCert started during the Pilot phase.

Not completed, nearing completion[1]: A version of a contract has been agreed to by OSG project personnel, DigiCert and IU procurement. It is pending input from the OSG Executive Director and then those changes will be reviewed by IU Procurement and DigiCert, and assuming their acceptance, executed. Other agreements can be found at:
https://twiki.grid.iu.edu/bin/view/Operations/OSGPKIAgreements

14. Develop a plan for vetting all the current OSG RAs and Grid Admins as RAs for DigiCert.

Completed: This can be found as part of the previously mentioned Transition Plan.

15. Monitor progress on the XSEDE CA and look for opportunities to leverage.

Ongoing activity: Discussions between XSEDE and OSG CA project staff are ongoing as XSEDE continues to refine their requirements. A meeting at NCSA is scheduled for June 7-8th to formally discuss collaboration.

2   Additional Accomplishments

1. OSG PKI Use Policy:
   https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG-PKI-Use-Policy-1.docx

3   Tasks to be carried over to the Development Phase

As described in Section 1, the following tasks are carried over from the Planning Phase to the Development Phase:

1. Monitor progress on the XSEDE CA and look for opportunities to leverage.

---

[1] Completed as of June 4th, 2012.

2. Complete the execution of legal and policy agreements with DigiCert started during the Pilot phase.

3. Develop a plan for how OSG and DigiCert will interact.

4. Define the administrative operational services (monitoring, alarming) to be developed and deployed for operation of the OSG CA.

5. Document what policy and contingency plan changes need to be made and develop a plan for addressing those changes.

6. Complete OSG-DigiCert interactions document with clarification in how OSG will internally handle requests from DigiCert has been called for and will be addressed in the Development Phase.

4 Personnel Adjustments

- A replacement for Jeremy Fischer, who will be departing the project to another position at IU at the end of June (despite project management's efforts) is being hired. He is responsible for client side software and if progress continues will that complete to a large extent before he departs. No change in budget is requested.

- Project management effort during the Planning Phase was greater than expected due to coordination of a meeting with XSEDE and unanticipated effort in finalizing the DigiCert contract. With those two events completed, it is expected to return to planned levels. No change in budget is requested.

- During the Planning Phase, it was determined that the burden for DN transition will largely fall on the VOs. Jim Basney is currently underutilized in the Development and Deployment Phase project plans. It is proposed that Jim's effort in those two phased be directed towards working with key OSG VOs to spearhead transitions and assist all VOs by identifying and working out issues they will encounter. No change in budget is requested.

- The Contingency Plan has not made suitable progress. Project management is addressing this in part by a separate weekly call for this activity. A recent change making this the responsibility of the Mine Altunay is also expected to help. This will be Mine's primary focus in the project during the Development phase. We believe this is on course now, but would like OSG Management to be aware in case another correction is request. No change in budget is requested.

5 Additional Issues for Consideration by OSG Management

5.1 Software Sustainability

Currently there is a single expert in the OIM software that will form the basis for the OSG PKI front-end which leaves OSG with a "bus factor" of one. Related to this,

maintenance of the client-side scripts is a previously identified issue with the previous DOE Grids scripts having been unmaintained, so there is no natural owner for the new OSG PKI scripts once development stops.

It is possible that the new hire to replace Jeremy Fischer could evolve into a potential solution for this problem, but it is too early to gauge how reasonable an expectation this is.

In order to ensure sustainability, it is requested that OSG Management consider this issue when addressing maintenance of the OSG PKI software by ensuring a second software developer (or fraction there of) is brought onto the OSG project with responsibility for OIM.

6 References

1. Von Welch. OSG Certificate Authority Implementation Plan. March 6th, 2012. https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG_CA_Implementation_Plan-4.pdf

2. OSG PKI Planning, Development, and Implementation. https://twiki.grid.iu.edu/bin/view/Operations/DigiCertPlanningDevAndImplementation

Appendix A Project Management Report

ID	WBS	TaskName	InCharge	Duration	Predecessors	Start_Date	Finish_Date	Percent
0	0	New OSG PKI Project	Welch	481 days		3/12/12	1/27/14	16%
1	1	Planning Phase	Welch	50 days		3/12/12	5/18/12	91%
2	1.1	Development and Deployment Plan	Hayashi, Fischer	30 days		3/12/12	4/20/12	100%
3	1.2	Document Acceptance Test Plan	Welch, Roy	15 days	2	4/23/12	5/11/12	100%
4	1.3	Document Transition Plan	Welch, Pordes	15 days	2	4/23/12	5/11/12	100%
5	1.4	Document Communications Plan	Pordes	10 days	2	4/23/12	5/4/12	100%
6	1.5	Document Training Plan	Altunay	10 days	2	4/23/12	5/4/12	100%
7	1.6	Define Contingency Plan (for the event that the DigiCert CA becomes unavailable)	Chadwick	15 days	2	4/23/12	5/11/12	50%
8	1.7	Baseline WBS and Timeline	Sehgal	5 days	6,2,3,4,5,7	5/14/12	5/18/12	100%
9	1.8	Finalize & Sign Contract between DigiCert & Indiana	Welch	20 days	2	4/23/12	5/18/12	85%
10	2	Development Phase	Welch	80 days		5/21/12	9/7/12	0%
11	2.1	Develop the OSG CA web service front-end and integrate with the DigiCert CA	Hayashi	65 days		5/21/12	8/17/12	0%
12	2.1.1	Develop software and associated documentation	Fischer, TBD	30 days	1	5/21/12	6/29/12	0%
13	2.1.2	Develop and package new CLI scripts	Fischer, TBD	10 days	12	7/2/12	7/13/12	0%
14	2.1.3	Review by the OSG software area of the resulting code and support documentation.	Roy	10 days	12,13	7/16/12	7/27/12	0%
15	2.1.4	Developer Testing of New Solutions	Hayashi, TBD	15 days	14	7/30/12	8/17/12	0%
16	2.2	Define changes to operational procedures, policy and other changes defined in the Planning phase.	Quick	15 days	1	5/21/12	6/8/12	0%
17	2.3	Conduct Acceptance Testing of System	Hayashi, Deximo, TBD, Roy	15 days	11	8/20/12	9/7/12	0%
18	2.4	Update Transition Plan	Welch	3 days	11	8/20/12	8/22/12	0%
19	2.5	Update Training Plan	Altunay	3 days	11	8/20/12	8/22/12	0%
20	2.6	Update Communications Plan	Pordes	3 days	11	8/20/12	8/22/12	0%
21	3	Deployment Phase	Welch	55 days		7/16/12	9/28/12	0%
22	3.1	Deploy the OSG CA - the OSG web front-end and operations components	Hayashi	55 days		7/16/12	9/28/12	0%
23	3.1.1	Procure Hardware	Quick	15 days	13	7/16/12	8/3/12	0%
24	3.1.2	New Server Setup	Quick	5 days	23	8/6/12	8/10/12	0%
25	3.1.3	Install Software	Hayashi	5 days	17,24	9/10/12	9/14/12	0%
26	3.1.4	Friendly User Testing	Hayashi, Welch, Deximo, TBD	10 days	25	9/17/12	9/28/12	0%
27	3.2	Execute Training Plan for OSG Staff	Altunay	15 days	10	9/10/12	9/28/12	0%
28	3.3	Implement changes to operational procedures, policy and other changes defined in the Planning phase.	Deximo	10 days	10	9/10/12	9/21/12	0%
29	3.4	Implement contingency Plan elements for the event that the DigiCert CA becomes unavailable	Altunay	10 days	10	9/10/12	9/21/12	0%
30	3.5	Transfer new software packages ownership to OSG Software team	Hayashi, TBD, Roy	5 days	10	9/10/12	9/14/12	0%
31	4	Transition	Welch	75 days		10/1/12	1/25/13	0%
32	4.1	Complete Execution of Communications Plan	Pordes	4 days	21	10/1/12	10/4/12	0%
33	4.2	Execute Training Plan for User Community	Altunay	20 days	21	10/1/12	10/26/12	0%
34	4.3	Issue DigiCerts certs for "friendly" user community	Hayashi, TBD	5 days	21	10/1/12	10/5/12	0%
35	4.4	Regression test OSG functionality using new Certs	Altunay	50 days	34	10/8/12	12/19/12	0%
36	4.5	Perform test Audits with DigiCert	Welch	5 days	34	10/8/12	10/12/12	0%
37	4.6	Test End-to-End Contingency Plan	Altunay, Deximo	20 days	34	10/8/12	11/2/12	0%
38	4.7	Management Readiness Review	Welch	20 days	35,37	12/20/12	1/25/13	0%
39	5	First Year of Operations	Quick, Welch	261 days		1/28/13	1/27/14	0%
40	5.1	Start issuing new and renewal certs from DigiCert	Hayashi, TBD	1 day	31	1/28/13	1/28/13	0%
41	5.2	"Drain" all active certs from DOEGrids CA	Esnet	260 days		1/28/13	1/24/14	0%
42	5.2.1	Stop issuing new certs from DOEGrids	Esnet	1 day	31	1/28/13	1/28/13	0%
43	5.2.2	Continue issuing CRLs for DOEGrids Certs	Esnet	260 days	31	1/28/13	1/24/14	0%
44	5.3	Shut off DEOGrid CA	Esnet	1 day	42,43	1/27/14	1/27/14	0%