

# OSG PKI Transition Phase Report

Von Welch [vwelch@indiana.edu](mailto:vwelch@indiana.edu)  
OSG PKI Transition Project Manager

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

February 19<sup>th</sup>, 2013

## **Abstract**

This report summarizes the activities, accomplishments of the OSG PKI Development Phase that spanned September 29<sup>th</sup>, 2012 through January 28<sup>th</sup>, 2013.

<b>1</b>	<b><u>SUMMARY</u></b>	<b><u>3</u></b>
<b>2</b>	<b><u>DOE GRIDS CA SHUTDOWN SCHEDULE UPDATE</u></b>	<b><u>3</u></b>
<b>3</b>	<b><u>OSG PKI TRANSITION PHASE TASKS</u></b>	<b><u>4</u></b>
3.1	ORIGINALLY PLANNED TASKS	4
3.2	TASKS CARRIED OVER FROM DEPLOYMENT PHASE	5
<b>4</b>	<b><u>TASKS CARRIED OVER TO OPERATIONS</u></b>	<b><u>6</u></b>
4.1	DIGICERT AUDIT	6
4.2	PKI CLIENT DEVELOPMENT AND TRANSFER TO SOFTWARE TEAM	7
4.3	UPDATE SLA FOR OIM	7
<b>5</b>	<b><u>STATUS OF COMMUNITY TRANSITION</u></b>	<b><u>7</u></b>
5.1	USER CERTIFICATES BY VO	8
5.2	ATLAS	9
5.3	CMS	9
5.4	FERMI NATIONAL LABORATORY	9
5.5	OTHER VOs	10
<b>6</b>	<b><u>ISSUES OF NOTE FOR OSG MANAGEMENT</u></b>	<b><u>11</u></b>
6.1	VO PREPAREDNESS	11
6.2	PKI SUPPORT FOR POTENTIAL VOs AND CAMPUS SUPPORT	11
6.3	TEST END-TO-END CONTINGENCY PLAN	12
6.4	SHA-2 TRANSITION	12
6.5	OPERATIONS IMPACT	12
<b>7</b>	<b><u>SIGNIFICANT RESOLVED ISSUES</u></b>	<b><u>12</u></b>
7.1	ATLAS PANDA ISSUE	12
7.2	CMS GLEEXEC/GUMS ISSUES	13
7.3	LCMAPS	14
7.4	VO CONTEXT FOR HOST CERTIFICATES	14
<b>8</b>	<b><u>BUDGET AND PERSONNEL ADJUSTMENTS</u></b>	<b><u>15</u></b>
<b>9</b>	<b><u>PLANS FOR OPERATIONS PHASE</u></b>	<b><u>15</u></b>
<b>10</b>	<b><u>REFERENCES</u></b>	<b><u>15</u></b>

## Executive Summary

This report summarizes the activities, accomplishments of the OSG PKI Development Phase that spanned September 29<sup>th</sup>, 2012 through January 28<sup>th</sup>, 2013. During this phase the primary emphasis has been on enrolling OSG virtual organizations (VOs) and preparing them for the upcoming DOE Grids CA shutdown on March 23<sup>rd</sup>, 2013. Significant progress was made with 26 VOs issuing 369 production certificates.

All planned Transition Phase tasks were completed with the following exceptions:

- The test audit with DigiCert is underway and expected to complete by the end of February.
- The transfer of software packages to the Software team is pending the final planned release (1.2) and scheduled for mid-March.
- The SLA for OIM needs to be updated to include change management and notification for the OSG PKI community. This will be completed by the end of February.

Issues raised for OSG management to consider are:

- There continues to be concern that VOs are not fully prepared and communications efforts continue.
- A decision is needed on the level of support OSG should provide for host certificate at sites not associated with OSG directly, but involved with OSG's campus outreach or participating in evaluating OSG as a potential VO
- Prioritizing and resourcing the deferring contingency testing.
- Being informed about the upcoming SHA-2 transition.
- Operations impact continues to be as predicted, an increase from .1 FTE under the DOE Grids PKI to .5 FTE under the OSG PKI.

A number of technical issues were encountered in terms of incompatibility between DigiCert certificates and various software stacks (PANDA/GridSite, LCMAPS, GUMS). These have all been fixed at this time.

There were no major budgetary or personnel adjustments. The subcontract to IU has been extended through April to provide support to the Software Team to complete transition of the software.

The day-to-day management of the PKI is transitioning to the Operations team with the Transition Lead, Welch, saying involved to oversee changes do not conflict with policy or best practices.

## 1 DOE Grids CA Shutdown Schedule Update

During the Transition period, specific dates were selected for the DOE Grids CA de-activation:

- On January 30<sup>th</sup>, 2013 the DOE Grids CA started encouraging, but not requiring, users to use the OSG PKI in preference to the DOE Grids CA. This was both on the website and in emails sent to users with certificate expiration notifications. This date has past with no problems noted.
- On March 23<sup>rd</sup>, 2013 the DOE Grids CA will stop issuing new certificates. This date was selected to be after the LHC shutdown and the OSG All Hands Meeting.

## 2 OSG PKI Transition Phase Tasks

### 2.1 Originally Planned Tasks

The following tasks were schedule in the Transition Phase.

#### 2.1.1 Complete Execution of Communication Plan

Owner: Ruth Pordes

Status: Completed.

OSG and ESnet staff continued to coordinate communications throughout the Transition phase to inform DOE Grids CA and OSG VOs and sites about the upcoming DOE Grids CA shutdown, the availability of the OSG PKI, and issues that they would need to undertake to transition.

#### 2.1.2 Produce Documentation for User Community

This task was previously “Execute Training Plan for User Community.” It was changed as it was decided it was infeasible to train OSG’s large and diverse user community. Instead documentation has been produced.

Owner: Alain Deximo

Status: Complete

Documentation for the OSG user community has been produced and is available (along with documentation for OSG sites and VOs) via:

<https://www.opensciencegrid.org/bin/view/Security/PKIDocumentationIndex>

#### 2.1.3 Issue DigiCert certifications for “friendly” user community

Owner: Soichi Hayashi

Status: Complete

The OSG PKI has issued 369 production certificates to end users throughout the Transition period. For comparison, the DOE Grids CA issued 183 certificates the week of February 4<sup>th</sup>, and 22 certificates the week of February 11<sup>th</sup>.

On December 19<sup>th</sup>, OSG staff (with volunteered help from the National Fusion Collaboratory staff) conducted a successful stress test of the OSG PKI system. Over the course of an hour, 1470 test host certificates were issued while normal PKI operations were unimpeded.

#### **2.1.4 Regression test OSG functionality using new Certs**

Owner: Mine Altunay

Status: Complete

Building on previous testing with ITB<sup>1</sup>, both ATLAS and CMS have done specific workflow testing. Some issues were discovered and resolved as described in Section 6.

#### **2.1.5 Perform test Audits with DigiCert**

Owner: Von Welch

Status: In Progress

DigiCert provided OSG with a self-audit to complete on January 31, 2013. Portions have been assigned to appropriate OSG staff (Security Officer, Operations Lead, and PKI Transition Lead) with an initial draft to be completed by February 22<sup>nd</sup>. The team will then assess the results and plan on how to address any shortcomings (e.g., by changing OSG practices or discussing policy modification with DigiCert). The final result will be circulated to the Executive Team for comment before being sent to DigiCert. After receiving the audit, DigiCert will report any concerns back to the OSG.

#### **2.1.6 Management Readiness Review**

Owner: Von Welch

Status: In progress

Acceptance of this report by the OSG Executive Team represents successful completion of the Management Readiness Review task.

### **2.2 Tasks Carried Over from Deployment Phase**

The following tasks were carried over from the Deployment Phase into the Transition Phase.

#### **2.2.1 DN Transition Planning**

Owner: Von Welch

---

<sup>1</sup> <https://twiki.grid.iu.edu/bin/view/Security/ITBDigicertTesting>

Status: Complete

With completion of testing by ATLAS and CMS, we believe we now understand all the issues involved with users changing DNs and have them documented<sup>2</sup>. A new issue with GUMS was discovered by CMS and is described in Section 6.2.

### **2.2.2 Communications Planning**

Owner: Ruth Pordes

Status: Complete

Please see Section 2.1.

### **2.2.3 Transfer new software packages ownership to OSG Software team**

Owner: Von Welch, Tim Cartwright

Status: In progress

We continue to delay this ownership hand-off until development activities by the OSG PKI Transition team complete. At this time development of the OSG PKI client scripts is in the final phase. A 1.1 release, which addresses a number of bugs and adds support for VO context to host certificates requests as requested by FNAL, is frozen and pending packaging. Development for a 1.2 release will be complete by mid-March and will add certificate renewal capability and consolidate common code amongst the scripts into a single module for increased maintainability. The PKI Transition and Software teams continue to work collaboratively to produce these RPM releases as they did with the initial 1.0 RPM.

After the 1.2 release, no new development is planned and ownership of the client software will transition officially to the

Software Team. Under a no-cost extension (see Section 7), the developers at Indiana U. (Mathure, Khadke) will be available to assist as requested by the Software Team through April, 2013.

## **3 Tasks Carried Over To Operations**

For clarity, the following tasks described in Section 2 were not completed.

### **3.1 DigiCert Audit**

As described in Section 2.1.5, the self-audit by OSG for DigiCert is ongoing. We expect to conclude it by the end of March.

---

<sup>2</sup>

[https://www.opensciencegrid.org/bin/view/Security/PKIDocumentationIndex#Documentation\\_for\\_VO\\_s](https://www.opensciencegrid.org/bin/view/Security/PKIDocumentationIndex#Documentation_for_VO_s)

### **3.2 PKI Client Development and Transfer to Software Team**

As described in Section 2.2.3, this task is ongoing and expected to complete by mid-March.

### **3.3 Update SLA for OIM**

Given that that OSG Information Management (OIM) system is now serving a broader role in serving as a fundamental part of OSG's PKI, adjustments are needed to its SLA. Specifically the SLA should be extended to include notifying PKA RAs and Grid Admins when user interface changes will impact them or their user communities, and coordination with the Software Team to test the command line clients when changes occur to the REST interface that supports those clients.

Von Welch will propose changes to the Operations Team and once agreed upon, the changes will get approved through normal OSG processes for modifying SLAs. This task will be completed by end of February.

## **4 Status of Community Transition**

In addition to the establishment of the OSG PKI itself, a key factor to a successful transition from the DOE Grids PKI is work by OSG VOs to prepare for the transition by enrolling RAs and updating documentation. OSG has been communicating this need to the VOs and supporting them by providing training<sup>3</sup> and documentation<sup>4</sup>. In this section we provide reports provided by three of the larger VOs, ATLAS, CMS and Fermilab, and the status of RA enrollment of the other VOs, which while not conclusive they are completely transitioned, does provide evidence they are aware and making progress at least.

---

<sup>3</sup> <https://twiki.grid.iu.edu/bin/view/Security/OSGPKITraining>

<sup>4</sup> <https://www.opensciencegrid.org/bin/view/Security/PKIDocumentationIndex>

#### 4.1 User Certificates by VO

User certificates issued by VO as of February 19<sup>th</sup>, 2013.

<b>VO</b>	<b># Certificates</b>
ALICE	1
ATLAS	7
Belle	5
CIGI	1
CMS	6
CSIU	2
DES	1
DREAM	1
DZero	3
ESGF	1
Fermilab	36
FusionGrid	15
GLOW	5
GlueX	8
HCC	7
IceCube	1
LBNE	1
LBNL	2
MIS	6
NERSC	3
NYSGrid	1
ORNL	3
OSG	12
SBGrid	1
STAR	1
SURAggrid	4



## 4.2 ATLAS

Report from John Hover of ATLAS:

Several select users have already been issued (and are using) OSG CA personal certificates without problems.

We have OSG CA certificate documentation for users in place:

<https://www.racf.bnl.gov/docs/howto/grid/osg-certificates>

A general announcement describing the switch will be sent soon to our US users mailing list. Most of our users have already dealt with multiple DNs (either through non-identical DOEgrids certs, or having CERN certificates in addition to DOEgrids), so we don't expect dramatic user support issues. We intend to handle OSG CA certs like any "new-DN" certificate.

We have tested our production framework end-to-end with OSG CA certificates.

All our Tier 2 sites have already upgraded to the latest GUMS version, or will be doing so shortly. ATLAS doesn't have any special user mapping requirements, so the new DNs shouldn't be an issue.

## 4.3 CMS

Report from Mine Altunary of CMS:

CMS is almost ready to make the transition to OSG CA. We still have a few issues although none of them are major roadblocks.

- We are ready for transitioning our end users and in fact have been doing this with a small number of users.
- We decided on a path for transitioning our sites and communicated this with our site admins. In terms of account mapping, we will provide some generic documentation and allow site admins to do this in the most reasonable way for their sites. We realized it is difficult for all sites to follow a single recipe. On GUMS update, we are constantly watching and pinging our sites. All of our Tier3s have either upgraded or have plans to upgrade their GUMS to rpm version. We still have 2 Tier2s that have not updated, but we are keeping an eye on those sites as well.
- All of our important central CMS services such as CMS VOMS and CMSWEB are aware of the changes and are tested with OSG CAs. We still have some services, not critical to grid jobs, data analysis, or production, that we need to ensure that they are ready. I will take care of these as soon as possible.

## 4.4 Fermi National Laboratory

The Fermilab Service Desk directly supports a number of OSG VOs and is coordinating their transition to the OSG PKI.

These Fermilab-managed VOs have registration authorities (RAs) registered with the OIM PKI and hence appear to be ready to handle requests from their users for certificates: DES, FermiLab, LBNE, LSST.

These Fermilab-managed VOs do not have RAs registered at this time: Accelerator, Argoneut, CDF, Cdms, GIGI, COUPP, FermiGrid, gm2, ILC, map, mars, MicroBooNE, Minerva, Miniboone, Minos, Mipp, Mu2e, Nova, Numi, Patriot, Theory.

Report from John Benson of Fermilab:

It is the responsibility of the Fermilab PKI Transition project to ensure that all Virtual Organizations (VOs) and Service providers associated with Fermilab are ready to transition to new PKI CA providers (OSG & others) as DOEGrids' certificates are phased out up through March, 2014. This includes providing new PKI Documentation, fully testing the use of personal and host/services certificates, Service Desk Readiness, and the Transition to Operations.

The project is in the final stages of putting in place the necessary PKI elements to ensure the readiness for 39 VOs currently registered with OSG, 7 Service Areas, 31 Service Offerings, DocDb users, and the FermiGrid. The project is scheduled to fully transition to Fermilab Operations by March 14, 2013. The transition has already begun with all new/revised PKI related documentation published and the Fermilab Service Desk Registration Authorities and Grid Administrators already processing requests for new personal and host/services DigiCert certificates.

#### **4.5 Other VOs**

The following OSG VOs have RAs registered with the OSG PKI and appear to be ready to handle requests from their users for certificates: ALICE, Belle, CSIU, DOSAR, DREAM, DZero, ESGF, FusionGrid, GLOW, HCC, IceCube, LCG, MIS, nanoHUB, NEBioGrid, NEES, NERSC, NYSGRID, ORNL, OSG, OSGEDU, SBGrid, STAR, SURAGrid, UC3.

The following VOs do not have RAs registered with the OSG PKI: ANL<sup>5</sup>, CompBioGrid, DayaBay, Engage, GCEDU, GCVO, GPN, GROW, i2u2, LBNL, NWICG, VLab.

The following VOs have indicated they will not be registering an RA with the OSG PKI: GlueX, LIGO<sup>6</sup>, Ops, RSV.

The following non-U.S. VOs are expected to find certificates for their user communities from a PKI specific to their country or geographic region: enmr.eu, geant4, GridUNESP, superbvo.org.

---

<sup>5</sup> In process.

<sup>6</sup> LIGO is establishing their own PKI.

## 5 Issues of Note for OSG Management

### 5.1 VO Preparedness

We continue to be concerned that not all VOs understand the level of effort they will need to commit to the transition (e.g., with user identities changing). FNAL and CMS have been transitioning and CMS lessons learned have been shared<sup>7</sup>. We request the ET support our communications by emphasizing this when opportunities present.

### 5.2 PKI Support for Potential VOs and Campus Support

An issue arose during the Transition Phase that merits Executive Team input in terms of its relatively priority.

The specific request was from an OSG staff member (Mats Rynge) wanting to get utexas.edu host certificate for the iPlant project as part of a test integration in consideration for joining the OSG project.

From the point of view of the PKI, the process would be for a iPlant staff member to register as a Grid Admin for the utexas.edu domain and approve their certificate requests.

Rynge countered that this raised the bar for potential VOs and, in the context of OSG's campus outreach, campuses exploring joining OSG as well. His request is that OSG Operations staff take on handling these certificate requests.

It is difficult to gauge at this time how much additional effort this would be for the Operations staff as each request would not be much effort, but they cumulative effort could add up. It also puts the Operations staff in judging certificate requests for domains that we have no direct relationship with, which could lead to complications (e.g. different people requesting the same certificate, local IT staff inquiring why we are issuing certificate for their domain).

XSEDE project staff are working with InCommon to allow the InCommon Certificate Service to issue IGTF-accredited host certificates, which would be a potential solution to this issue, but due to uncertainties in process and number of parties involved, a timeline for completion is not determined.

A non-exhaustive set of options for OSG are:

1. The Operations Team takes on handling these requests and we closely monitoring the situation. This could be awkward if we find the effort too high and decide to discontinue offering this service.
2. Make no change and require potential VOs and sites to register as Grid Admins in the PKI. This may dissuade some of these entities from joining the OSG.

---

<sup>7</sup> <https://www.opensciencegrid.org/bin/view/Security/PKIDocumentationIndex>

3. Explore a hybrid model where the Operations Team issue a limited number of certificates for a potential VO or campus, but the expectation is they enroll as a Grid Admin if the relationship persists.

Related JIRA issue: <https://jira.opensciencegrid.org/browse/OSGPKI-232>

### **5.3 Test End-to-End Contingency Plan**

As decided at the August 22-23, 2012 OSG Council meeting<sup>8</sup>: "Apart from Action Items identified [presenting the contingency plan to the WLG, as was done], further work on the Contingency Plan can be delayed until following completion of the PKI Transition."

It is recommended that the ET evaluate the priority of this task and, if they decide to proceed, create a project to undertake it.

### **5.4 SHA-2 Transition**

Independent of the transition to DigiCert, the OSG is preparing for transition of the certificate hash algorithm from SHA-1 to SHA-2<sup>9</sup>. DigiCert has already made SHA-2 certificates available to OSG, both through their web interface (MPKI) and the REST API. Members of OSG's SHA-2 team have obtained SHA-2 certificates for testing.

In August of 2013, OSG should modify its PKI to issue SHA-2 certificates by default. This is not expected to be a substantial technical change (modification of a parameter in the calls from OIM to DigiCert), but some preparatory testing should be accomplished.

### **5.5 Operations Impact**

Previously, an Operations Impact Assessment was completed [11]. The estimate it describes continues to appear valid, namely that Operations staffing requirement for the OSG PKI will be .5 FTE, an increase from .1 FTE under the DOE Grids PKI.

## **6 Significant Resolved Issues**

### **6.1 ATLAS Panda Issue**

In testing USATLAS workflows with new OSG PKI/DigiCert credentials, John Hover encountered errors in connections from worker nodes to the GridSite software hosted at CERN as part of the Panda server. The specific error message was: "SSL routines:SSL3\_READ\_BYTES:tlsv1 alert unknown ca"

Investigation revealed that this was an instance of a previously encountered bug with GridSite also experienced by the Terena eScience Personal CA<sup>10</sup> and FNAL KCA.

---

<sup>8</sup> <https://www.opensciencegrid.org/bin/view/Council/Agenda2012Aug22-23>

<sup>9</sup> <https://www.opensciencegrid.org/bin/view/SoftwareTeam/Sha2Support>

<sup>10</sup> [https://ggus.eu/tech/ticket\\_show.php?ticket=67040](https://ggus.eu/tech/ticket_show.php?ticket=67040)

A bug in the process (path validation) caused 2nd-order proxy certificates (i.e. a delegation from a delegation) to be improperly rejected as invalid when the root CA certificate used the 'pathlen=0' security constraint<sup>11</sup>.

Oscar Koeroo provided a patch to the GridSite developers, who released gridsite-1.7.25 (via EMI 1 Update 22 & EMI 2 Update 7 on December 21, 2012). This was installed by Panda administrators at CERN and subsequently successfully tested by John Hover.

A subsequent problem discovered by John with LFC that looked similar turned out to be a configuration issue (missing CA certificate) and was unrelated to the GridSite problem.

For more information:

- <https://jira.opensciencegrid.org/browse/OSGPKI-249> DigiCert certificates not working with PANDA
- <https://jira.opensciencegrid.org/browse/SOFTWARE-822> Create and maintain test instance of PANDA on ITB for testing
- [https://ggus.eu/tech/ticket\\_show.php?ticket=87573](https://ggus.eu/tech/ticket_show.php?ticket=87573) DigiCert certificate proxies rejected by mod\_gridsite
- <https://twiki.grid.iu.edu/bin/view/Security/ITBDigicertTesting> Testing of new CA distribution format on ITB
- <http://software-witchcraft.blogspot.nl/2011/07/cream-did-it-using-bugs-in-path-length.html> CREAM did it, using bugs in path length constraints, in OpenSSL/Globus
- [https://ggus.eu/tech/ticket\\_show.php?ticket=67040](https://ggus.eu/tech/ticket_show.php?ticket=67040) Terena Grid Certificate not working with WMS
- <https://jira.opensciencegrid.org/browse/OSGPKI-296> LFC not working with DigiCert certificates

## 6.2 CMS glxec/GUMS Issues

In CMS, currently every worker node has a host certificate and calls from glxec to GUMS via the lcms use this certificate to authenticate. CMS is looking to reduce the number of host certificates it utilizes and explored two methods to do so. The first was to create a proxy certificate from a host cert and push that to every worker node. For various reasons, this method was not pursued.

The second, and chosen, option is to use the delegated pilot proxy certificate to authenticate the glxec-GUMS connection. In this mode, glxec still passes three pieces of information but the contents of each are different. Instead of the host cert DN, the pilot proxy DN is passed. The service name is now the FQDN of the machine rather than the DN. The final piece is still the payload proxy.

---

<sup>11</sup> The pathlen parameter in the CA certificate prevents accidental or malicious creation of subordinate CAs. While not common in IGTF CAs it is common in other CAs and is considered by many to be a valuable security feature. There is strong resistance from both DigiCert and members of the community to removing it.

Supporting this mode requires potentially three changes described below. Details are available from Anthony Tiradani and the CMS project.

1. Versions of GUMS shipped using Pacman relied on a patched Apache webserver to perform GSI authentication. This version fails using DigiCert certificates. The recommended solution is to upgrade to any version of GUMS shipped via RPM.
2. GUMS must be configured to allow queries from being based on host certificate identity (DN) to being based on the identity of the pilot proxy. This appears to be possible in all versions of GUMS currently in use.
3. GUMS must be configured to allow glxexec to lookup any mapping within a group. This appears to require the latest version (1.3.18) of GUMS.

### **6.3 lcmaps**

Similar to GridSite, lcmaps-plugins-verify-proxy prior to 1.4.12 were found to have compatibility issues and update to 1.5.0 is strongly recommended.

### **6.4 VO Context for Host Certificates**

During the Transition Phase, staff at Fermilab raised concerns with a design choice made by the Transition Project, namely that Grid Admins were responsible for approving host certificates and Grid Admins did so outside the context of a VO.

This model was not working well for Fermilab because a large number of Grid Admins approve host certificates in the fnal.gov domain and they do so under the context of different VOs. This was causing them operational problems in that their Grid Admins were seeing a number of host certificates requests not relevant to them, which was making filtering requests difficult, increasing the changes a request would be missed and reducing the PKI's level of user service.

In response, the PKI Transition team added the ability to have a Grid Admins and host certificates requests operate in the context of a VO, allowing requests in a particular domain to be directed based on the VO context, meaning Grid Admins would only see requests relevant to them.

This feature will be fully operational with the 1.1 release of the command line clients (see Section 2.2.3).

In retrospect, the Transition Team's decision has worked well outside of the fnal.gov domain, but this was a significant use case which was not realized until the Transition Phase and ideally would have been accounted for earlier.

For more information:

- <https://jira.opensciencegrid.org/browse/OSGPKI-266> Can email to Grid Admins be filtered by VO?
- <https://jira.opensciencegrid.org/browse/OSGPKI-273> Add VO to Grid Admin request form

- <https://jira.opensciencegrid.org/browse/OSGPKI-298> Allow specifying vo name in OSG PKI for host\_certs\_request

## 7 Budget and Personnel Adjustments

No major personnel changes occurred during the Transition phase.

Indiana University is about \$20k under budget on its \$86k subcontract from Fermilab to support the PKI Transition. A no-cost extension was requested and granted, extending the subcontract through April. Indiana U. will use this to support the Software Team as requested in supporting the command-line clients, and to participate in the OSG All Hands Meeting.

At the end of the Transition Phase Welch changes from 20% to 5% time on the OSG project, with that time being spent maintaining the PKI policies and contracts, helping with any issues that may arise with the PKI, and providing leadership to the OSG identity management area, specifically starting with the creation of a roadmap for OSG identity management.

The student programmer (Khadke) hired during the Deployment Phase at Indiana U. has worked out well and their development efforts will be in the 1.2 release of the command line tools. Indiana U. expects to continue to maintain the student's employment after the Transition under other funding.

## 8 Plans for Operations Phase

With the completion of the Transition Phase and the presumed eventual acceptance of this report, the OSG PKI is now in Operations. As previous described, the DOE Grids CA will cease issuing new certificates on March 23, 2013, so efforts to communicate this to VOs will continue, both by OSG and ESnet staff.

The Transition Team will be maintained until tasks described in Section 2.2 complete and the weekly calls will be maintained at least through March and then evaluated weekly and discontinued when no longer needed. At this time, the Operations staff is already handling day-to-day operation of the PKI.

At this point any new problems will be evaluated by the Operations and/or Software team and prioritized as appropriate. Welch, with responsibility for the contract and the PKI overall, will continue to consult with those teams and oversee and approve major changes.

## 9 References

1. Von Welch. OSG Certificate Authority Implementation Plan. March 6<sup>th</sup>, 2012. [https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG\\_CA\\_Implementation\\_Plan-4.pdf](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>
3. OSG PKI Acceptance Criteria.  
<https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG-PKI-Acceptance-Criteria-2.docx>
4. OSG-DigiCert Interactions. <https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1135>
5. OSG PKI Contingency Analysis. <http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1121>
6. OSG PKI Contingency Plan. <http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1115>
7. OSG-XSEDE Meeting Notes. <https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1114>
8. OSG Certificate Analysis. <http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1116>
9. OSG Planning Phase Report. <http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1120>
10. Transition Project WBS.  
<https://twiki.grid.iu.edu/bin/view/Operations/OSGPKIProjectWBS>
11. Operations Impact Document  
<https://twiki.grid.iu.edu/bin/view/Operations/PKIOpsImpact>
12. OSG Identity Management via DigiCert CA. Preliminary Project Estimate. September 21, 2011



# Appendix A Project Management Report

ID	WBS	Task Name	InCharge	Duration	Predecessors	Start	Finish	% Complete
0	00	New OSG PKI Project	Welch	521 days		Mon 3/12/12	Mon 3/24/14	56%
1	11	Planning Phase	Welch	50 days		Mon 3/12/12	Fri 5/18/12	100%
2	21.1	Development and Deployment Plan	Hayashi, Fischer	30 days		Mon 3/12/12	Fri 4/20/12	100%
3	31.2	Document Acceptance Test Plan	Welch, Roy	15 days	2	Mon 4/23/12	Fri 5/11/12	100%
4	41.3	Document Transition Plan	Welch, Pordes	15 days	2	Mon 4/23/12	Fri 5/11/12	100%
5	51.4	Document Communications Plan	Pordes	10 days	2	Mon 4/23/12	Fri 5/4/12	100%
6	61.5	Document Training Plan	Altunay	10 days	2	Mon 4/23/12	Fri 5/4/12	100%
7	71.6	Define Contingency Plan (for the event that the DigiCert CA becomes unavailable)	Altunay	15 days	2	Mon 4/23/12	Fri 5/11/12	100%
8	81.7	Baseline WBS and Timeline	Sehgal	5 days	6.2,3,4,5,7	Mon 5/14/12	Fri 5/18/12	100%
9	91.8	Finalize & Sign Contract between DigiCert & Indiana	Welch	20 days	2	Mon 4/23/12	Fri 5/18/12	100%
10	102	Development Phase	Welch	80 days		Mon 5/21/12	Fri 9/7/12	100%
11	112.1	Develop the OSG CA web service front-end and integrate with the DigiCert CA	Hayashi	65 days		Mon 5/21/12	Fri 8/17/12	100%
12	122.1.1	Develop front-end software and associated documentation	Hayashi	30 days	1	Mon 5/21/12	Fri 6/29/12	100%
13	132.1.2	Develop and package new CLI scripts	Mathure, Selmezi	10 days	12	Mon 7/2/12	Fri 7/13/12	100%
14	142.1.3	Review by the OSG software area of the resulting code and support documentation.	Roy	10 days	12, 13	Mon 7/16/12	Fri 7/27/12	100%
15	152.1.4	Developer Testing of New Solutions	Hayashi, Mathure	15 days	14	Mon 7/30/12	Fri 8/17/12	100%
16	162.2	Define changes to operational procedures, policy and other changes defined in the Planning phase.	Quick	15 days	1	Mon 5/21/12	Fri 6/8/12	100%
17	172.3	Conduct Acceptance Testing of System	Hayashi, Deximo, Mathure, Roy	15 days	11	Mon 8/20/12	Fri 9/7/12	100%
18	182.4	Update Transition Plan	Welch	3 days	11	Mon 8/20/12	Wed 8/22/12	100%
19	192.5	Understand and document impact of DN changes	Basney	15 days	11	Mon 8/20/12	Fri 9/7/12	100%
20	202.6	Update Training Plan	Altunay, Basney	3 days	11	Mon 8/20/12	Wed 8/22/12	100%
21	212.7	Update Communications Plan	Pordes	3 days	11	Mon 8/20/12	Wed 8/22/12	100%
22	223	Deployment Phase	Welch	27 days		Thu 8/23/12	Fri 9/28/12	99%
23	233.1	Deploy the OSG CA - the OSG web front-end and operations components	Hayashi	15 days		Mon 9/10/12	Fri 9/28/12	100%
24	243.1.1	Install Software	Hayashi	5 days	17	Mon 9/10/12	Fri 9/14/12	100%
25	253.1.2	Friendly User Testing	Hayashi, Welch, Deximo	10 days	24	Mon 9/17/12	Fri 9/28/12	100%
26	263.2	Develop and deploy training for OSG Staff	Altunay, Basney	25 days	20	Thu 8/23/12	Wed 9/26/12	100%
27	273.3	Implement changes to operational procedures, policy and other changes defined in the Planning phase.	Deximo	10 days	10	Mon 9/10/12	Fri 9/21/12	100%
28	283.4	Transfer new software packages ownership to OSG Software team	Hayashi, Cartwright	5 days	10	Mon 9/10/12	Fri 9/14/12	95%
29	293.5	Gate Report for completion of Development/Deployment phase	Welch, Sehgal	3 days		Wed 9/26/12	Fri 9/28/12	100%
30	304	Transition	Welch	75 days		Mon 10/1/12	Fri 1/25/13	89%
31	314.1	Complete Execution of Communications Plan	Pordes	4 days	22	Mon 10/1/12	Thu 10/4/12	100%
32	324.2	Execute Training Plan for User Community	Altunay	20 days	22	Mon 10/1/12	Fri 10/26/12	100%
33	334.3	Issue DigiCerts certs for "friendly" user community	Deximo	5 days	22	Mon 10/1/12	Fri 10/5/12	100%
34	344.4	Regression test OSG functionality using new Certs	Altunay	50 days	33	Mon 10/8/12	Wed 12/19/12	100%
35	354.5	Perform test Audits with DigiCert	Welch	5 days	33	Mon 10/8/12	Fri 10/12/12	25%
36	364.6	Management Readiness Review	Welch	20 days	34	Thu 12/20/12	Fri 1/25/13	60%
37	375	First Year of Operations	Quick, Welch	301 days		Mon 1/28/13	Mon 3/24/14	10%
38	385.1	Start issuing new and renewal certs from DigiCert	Deximo	1 day	30	Mon 1/28/13	Mon 1/28/13	100%
39	395.2	Update SLA for OIM	Quick, Welch	10 days	30	Fri 2/15/13	Thu 2/28/13	0%
40	405.3	"Drain" all active certs from DOEGrids CA	Esnat	300 days		Mon 1/28/13	Sun 3/23/14	10%
41	415.3.1	Stop issuing new certs from DOEGrids	Esnat	40 days	30	Mon 12/8/13	Sat 3/23/13	10%
42	425.3.2	Continue issuing CRLs for DOEGrids Certs	Esnat	300 days	30	Mon 12/8/13	Sun 3/23/14	10%
43	435.4	Shut off DEOGrid CA	Esnat	1 day	41,42	Mon 3/24/14	Mon 3/24/14	0%

Project New OSG PKI Project  
Date: Thu 2/14/13

Task Split Milestone Summary Project Summary

External Task External Milestone Inactive Task Inactive Milestone Project Summary

Manual Task Duration-only Manual Summary Rollup Manual Summary Start-only

Finish-only Progress Deadline

Page 1