OSG DigiCert Pilot Report

Mine Altunay, Jim Basney, Jeremy Fischer, Chander Sehgal, Von Welch

February 20th, 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 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, 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 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 recommendations from the Pilot team are

1. DigiCert could provide CA services suitable for OSG and utilizing DigiCert is a better option opposed to OSG establishing its own CA.
2. While it would be possible for OSG to use DigiCert directly, establishing a front-end web service would give OSG control of the user experience, provide better service for large number of host certificates, and provide the ability to change CA in the future while minimizing change for its user community.
3. OSG should support three other DOE Grids CA user communities (Fusion Grid, ESG, NERSC) that approached OSG to do so during the Pilot as it does not appear to require obvious additional effort. If the required effort turns out to be significant (>5% of total), this recommendation should be revisited.

This document captures the Pilot activities, outcomes and the recommendations of the Pilot team based on those outcomes that DigiCert is a viable and best option for OSG in terms of replacement PKI. It describes a plan for next steps and a timeline to complete implementation of an OSG PKI based on a DigiCert CA and an OSG-developed front-end by end of CY 2012.

A set of lessoned learned and a project management post mortem are also included.

Table of Contents

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, a commercial company, to operate a CA for OSG.

2 Pilot Goals

A pilot, running from November 2011 through January 2012, was initiated to determine if contracting with DigiCert[1] 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? This document captures the Pilot activities, outcomes and the recommendations of the Pilot team based on those outcomes. High-level requirements of meeting this goal are:

Requirement #0: Certificates Must Work with VDT

Any issued certificates need to work with the VDT Software stack[3]. In theory, this means certificates need to comply with RFC 5280 and other relevant standards. In practice, determining compliance is best achieved through extensive testing under real world conditions, such as on the OSG Integration Testbed (ITB)[4]. Hence, while

[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").

[3] http://vdt.cs.wisc.edu/

[4] https://twiki.grid.iu.edu/bin/view/Integration

we believe all alternatives under consideration satisfy this requirement, the prudent course of action is to extensively test any candidate replacement with VDT.

Requirement #1: LHC Interoperability/IGTF accreditation for the CA

Members of the OSG user community participating in the LHC VOs require IGTF[5] accredited certificates for interoperability. DOE laboratory users may as well, an open question.

Some subset of this group may potentially not need IGTF accredited certificates at some time in the foreseeable future (worker node certificates, service certificates, DOE Lab resource users), and a second subset (LHC users) could be directed to use other PKIs (the CERN CA[6]). However, the authors felt it was too high of risk to assume that the OSG PKI could issue certificates from a non-IGTF accredited CA and allow this subset of its user community to maintain compatibility with the LHC.

Requirement #2: Ability to provide certificates to roughly 2500 OSG users distributed across the USA, vetted by 36 registration authorities agents.

This is based on historical numbers from the DOE Grids CA [7].

Requirement #3: Ability to provide host certificates for 300+ gatekeepers plus 5000+ worker nodes to 40 grid administrators at roughly 80 OSG sites.

This is based on historical numbers from the DOE Grids CA [7].

Requirement #4: Ability to supply web and other service certificates.

While the majority of OSG's certificate usage is for VDT, there is a small amount of usage for non-commercial web servers (approximately 30-35 certificates [15]). OSG also uses "service" certificates in a manner unique to the computational grid community, e.g. with Glide-in systems.

Note: as discussed in the Findings in Section 4.3, it was determined during the Pilot that this requirement was best satisfied by commercial PKI services outside of OSG's PKI, hence it was removed as a requirement during the Pilot.

Requirement #5: Ability to sustain operation into the foreseeable future.

Many of the considered alternatives have uncertainty about when they would be available and/or for how long they would continue operation. Any solution needs to support OSG for at least 2-3 years while longer-term options are explored.

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

[6] https://ca.cern.ch/ca/

3 Pilot Tasks and Results

3.1 Initial Agreement with DigiCert to gain Access for Testing

Completed [5].

3.2 Initialize: Get credentials and Issue DigiCert certificate for testing

Completed.

3.3 Validate Suitability of DigiCert Certificates via Web Interface

3.3.1 Monitor IGTF accreditation process of DigiCert

Accreditation has finished and the DigiCert CAs will appear in the January 2012 IGTF v1.44 distribution[7]. OSG distribution of the DigiCert CAs will follow as per usual IGTF update procedures.

3.3.2 Demonstrate ability of DigiCert certificates (user, host, service) to function properly with VDT and other OSG software

Completed successfully [10].

3.3.3 Ensure DigiCert is compatible with LHC Job Submission

This is pending our ability to access DigiCert Production certificates, which is pending completing the negotiation with DigiCert of OSG RA Policies and Practices (see Section 3.8.2). This was an unforeseen dependency at Pilot inception and we did not initiate work on the dependencies early enough to complete this.

3.4 Validate Suitability of DigiCert processes to support OSG Workflows

3.4.1 Prototype OSG front-end to DigiCert CA back-end

Description: Prototype and demonstrate ability for OSG to front DigiCert CA backend with own frontend issuance process (components 2-4) by prototyping those processes (type 3 outsourcing). Evaluate possibility of using COTS software (RedHat, Fedora, OpenCA, confusa.org) to implement those interfaces.

Goal: Determine the feasibility of an OSG front-end to the DigiCert CA back-end. Learn the DigiCert API. Evaluate required changes the API will drive OSG scripts/software. Evaluate costs.

What is unusual about OSG?

- Bulk host certificates
- Grid Admins (host certificates for particular domains)

[7] https://dist.eugridpma.info/distribution/igtf/current/accredited/

Results:

Our initial testing of the DigiCert API found it to be lacking in many regards. This API seems to have been developed organically in response to customer request as opposed to designed to provide all the functionality of the web UI. As such we found the DigiCert REST API not as complete as we hoped. Also, aspects of it were also tailored for commodity web-based workflows (e.g. user certificate API requests initiated a workflow requiring a web browser). Hence, it was initially lacking some features needed to support OSG workflows.

We provided feedback to DigiCert on these shortcomings and they agreed to and successfully addressed the most important shortcomings of these during the Pilot. At this point, the API has calls for all standard functions except for generating CRLs and certificate renewal, which is sufficient to support the OSG use cases needed in the first year.

More details of this testing can be found in Appendix D.

3.4.2 Demonstrate ability for users and RAs to revoke certificates in a timely manner

Description: Test DigiCert API and web based tools to revoke an existing certificate. Ensure the published CRL is compatible with OSG infrastructure.

Results: Pilot team successfully issued and revoked multiple service certificates by using DigiCert's web interface. It took less than 24 hours for DigiCert to generate new CRL files. The revoked certificates were correctly included in the new CRL files. ITB sites had no problems with processing the CRL files.

We found out that DigiCert has appropriate security controls that ensure that only authorized personnel can request and approve revocations. DigiCert allows a full-privileged admin (i.e. OSG RA) to revoke any certificate he/she wishes. Whereas, a GridAdmin is only allowed to manage (i.e. revoke, issue, renew) certificates within his/her assigned domain. Finally, an end user can request revocation of certificates, but the request has to be approved and executed by a GridAdmin or an RA Agent.

We found DigiCert's security controls to be sufficient to meet OSG's needs.

3.4.3 Demonstrate ability for OSG RAs to gather statistics about certificate issuance and ability to intervene when number of certificate requests exceeds allotted number in the contract

Description: OSG is allowed a certain number of user and host certificates that will be issued by DigiCert. We will test the existing tools in DigiCert portal to ensure that OSG does not exceed the maximum allotment.

Result: DigiCert has a web UI called "My certificates" that allows OSG RA to list all issued certificates per business unit. Business unit represents an OSG site in DigiCert terminology. The DigiCert UI meets OSG needs at a basic level that it provides a list of issued certificates. However, it requires someone to periodically check the web pages and do some calculations across all OSG sites (business units) to understand if the maximum limit is reached. More sophisticated alert mechanisms, such as

sending an alert when OSG gets closer to its maximum number or when a GridAdmin issues an unusually large number of certificates, would need to be implemented via and OSG front-end to the DigiCert API. DigiCert stated that they would be willing to put this into API enhancement matrix. Since we clearly do not want to exceed our certificate quota and human errors are likely to happen, we recommend that DigiCert should implement a mechanism that send OSG automated alerts if OSG chooses to use the DigiCert web UI as its primary interface.

3.4.4 Demonstrate ability for OSG RA to monitor Agent and GridAdmin actions for auditing purposes

Description: OSG RA should ensure that all RA Agents and GridAdmins would act according to the OSG RA operational procedures. OSG RA will need monitoring abilities to ensure that such procedures are followed. Determine whether DigiCert provides sufficient monitoring capabilities.

Results: OSG policies require RA Agents and GridAdmins to document their actions along with a short explanation for these actions. The DigiCert web UI provides an Audit Trail, available to OSG RA, which keeps track of every action taken by a OSG RA Agent or a Grid Admin. The Audit Trail logs include login times, login accounts, actions taken (e.g. approve request, download certificate, log out and so on), IP addresses, certificate CN, and request id. In addition, the DigiCert web page "Requests" keeps a list of all requests issued by RA staff. Each request has a comment/notes field where an Agent/Admin can fill out a short explanation for their actions.

Our conclusion is that existing DigiCert capabilities are sufficient for OSG to perform audits. DigiCert technical capabilities in this area are better than what OSG has currently.

3.4.5 Demonstrate ability for storing and archiving artifacts (auditing) from certificate issuance workflows

Description: OSG RA process and policies require certain information from certificate issuance workflows to be stored and archived for audit purposes. Ensure that DigiCert has the capability to store the required information.

Result: DigiCert audit trails are kept indefinitely. The stored information is described in 3.4.4 and is sufficient for OSG purposes.

3.5 Evaluate DigiCert Availability

Description: Evaluate DigiCert ability to provide redundant and highly available services.

In progress[8]. Nothing we have uncovered alarms us, but evaluation of the uncovered information is pending. A key challenge here is how to go about that evaluation in any objective manner.

3.6 Mid-term Management Meeting between OSG and DigiCert

This meeting was held January 19th at Fermi National Laboratory. A preliminary version of this report, including anticipated recommendations, was presented to the OSG Executive Team. A representative from DigiCert (Aaron Watson, VP of Sales) attended the latter half of the meeting to answer questions from the Executive Team. Other than suggestions on some additional content to add to this report, there was approval expressed of the Pilot progress.

3.7 Update OSG IdM Contingency and Risk Plan

The new draft contingency plan for OSG use of the DigiCert CA service enumerates changes resulting from a migration from DOE Grids to DigiCert [3]:

- DigiCert CRLs only have a one-week lifetime (as compared to one month with DOE Grids PKI), which would necessitate an earlier move to disabling CRL checking in the event of a CRL service disruption. DigiCert has been asked if they would extend their CRL lifetime and is currently considering this.
- As a commercial CA provider, DigiCert is a more visible attack target than DOE Grids, but DigiCert is also held to a higher standard of operation (WebTrust[9] and CA/Browser Forum[10] versus IGTF). In 2011 we saw significant compromises of commercial CA providers (DigiNotar, Comodo, etc.). While the DigiCert Grid CA is a private CA not trusted by browsers, it is hosted in the same operational environment as DigiCert's other public CAs. As with any external CA provider (DOE Grids PKI included), there is risk to OSG that the provider will cease operations for a variety of reasons. Using a commercial provider versus a DOE lab provider arguably increases this risk.

Please see Appendix E for a description of specific recommended steps that should be undertaken.

3.8 Negotiate Long-term DigiCert Contract

Goal: Establish a 2-year agreement with DigiCert for providing PKI services to OSG.

3.8.1 Decide which institution will own contract

Indiana University.

---

[8] https://twiki.grid.iu.edu/bin/view/Security/EvaluationOfDigiCertReliability

[9] http://www.webtrust.org/

[10] http://www.cabforum.org/

3.8.2 Draft OSG RA Policies and Practices acceptable to DigiCert

In process. A template Grid Registration Practices Statement is provided in the DigiCert-Grid Repository [4]. As of February 10th, 2012, we have two collaborative round of edits to this document to better match OSG RA policies and practices and believe we are in agreement on all salient points with DigiCert and completion is pending on final wordsmithing.

3.8.3 Negotiate Terms of longer term contract

In process. We have completed negotiations in principle with DigiCert on technical matters and need to capture those in text. We have also negotiated a one-year agreement (as opposed to two year) in order to work better with the federal fiscal cycle. The contract needs to be reviewed by Indiana University purchasing and legal.

3.9 Post-trial Evaluation and Review

Description: Post-trial evaluation and review with OSG-ET to decide go/no-go for next phases.

Goal: Present proposal to OSG-ET on whether DigiCert is suitable service provider for OSG and achieve their agreement. Achieve decision on type of outsourcing.

In process. The distribution of this report to the OSG-ET represents the initiation of this process.

4 Summary of Findings

4.1 Findings Related to DigiCert's Fundamental CA Capabilities

- We have used the DigiCert web UI ("MPKI") to conduct pilot activities and tested it for aspects important to supporting OSG workflows [8]. Outside of bulk host certificate requests, the DigiCert web UI seems to meet expectations for OSG PKI activities and could serve OSG if needed (e.g. if there was a failure of the planned front end services).
- We have discovered a number of assumptions in DigiCert's workflows that customers tie certificate issuance to DNS domains under the assumption that customers represent enterprises that are authoritative for a DNS domain. OSG, being a federation, is not authoritative for DNS domains in general (opensciencegrid.org being the exception). This raises policy issues that need to be worked through with DigiCert.
- DigiCert's Grid CA CP/CPS has passed TAGPMA/IGFTF accreditation and the DigiCert CAs will appear in the January 2012 IGTF v1.44 distribution. Testing with LHC partners is pending the production of this distribution. This has met expectations.
- Testing of DigiCert certificates with OSG workflows in the ITB has shown no problems. This has met with expectations.

- Negotiation of mutually acceptable practices and policies seems to have reached agreement on all major points and is in the process of being documented. A review by Indiana University (IU) a legal and procurement is pending, but not expected to be an issue do to IU's agreement on the Pilot purchase agreement and DigiCert's history of serving a broad range of customers.
- In general DigiCert has been very responsive to queries and requests and seems motivated to meet OSG's needs. It seems clear they are hoping to establish a market in the grid space and see OSG as a key initial customer.

4.2 Findings Related to DigiCert's API to Support a OSG Front-end

- We have tested the DigiCert REST API to evaluate its ability to support an OSG facade in front of the DigiCert PKI service. This API seems to have been developed organically in response to customer request as opposed to designed to provide all the functionality of the web UI. As such we found it initially short of meeting OSG's needs. DigiCert has added significant functionality such that we believe all major OSG needs are now met and we have been convinced of DigiCert ability to make changes as needed to address future needs.
- When OSG goes into production, a separate API test bed would be useful so that changes are not being performed on the live system as they were during the pilot.
- Change management for the API should be implemented so OSG is aware of upcoming changes to the API in advance and can prepare adequately for said changes.

4.3 Findings Related to OSG PKI Usage

- We discovered there are a number (~ten) of mechanism (custom scripts) in use by the OSG Grid Admin community for bulk host certificate request.
- A preliminary evaluation of an OSG identity management contingency plan assuming the use of the DigiCert CA has been accomplished [3]. The main changes identified from the DOE Grids PKI are:
    - DigiCert CRLs only have a one-week lifetime (as compared to one month with DOE Grids PKI), which would necessitate an earlier move to disabling CRL checking in the event of a CRL service disruption. DigiCert has been asked if they would extend their CRL lifetime and is currently considering this.
    - As a commercial CA provider, DigiCert is a more visible attack target than DOE Grids, but DigiCert is also held to a higher standard of operation (WebTrust and CA/Browser Forum versus IGTF). In 2011 we saw significant compromises of commercial CA providers (DigiNotar, Comodo, etc.). While the DigiCert Grid CA is a private CA

not trusted by browsers, it is hosted in the same operational environment as DigiCert's other public CAs. As with any external CA provider (DOE Grids included), there is risk to OSG that the provider will cease operations for a variety of reasons. Using a commercial provider versus a DOE lab provider arguably increases this risk.

- During the pilot, we realized that a shift to DigiCert (or any PKI) from DOE Grids will require users to obtain new distinguished names that will need to be registered in VOMS (and other authorization services). This process should be investigated and suitable assistance provided to the OSG community.
- Outside the pilot, work in OSG is underway to modify GLexec [11] to reduce the need for IGTF accredited host certificates. Since adoption of this work is at the discretion of the OSG sites, it's difficult to judge the impact this will have on OSG's certificate needs and we believe it is too immature to rely on at this time.
- With regards to Requirement #4 in Section 2, we realized during the Pilot that OSG's need for web certificates is both completely commodity and modest (approximately 30-35 [15]). These certificates however work best if they use a CA that is trusted by common web browsers, which the DigiCert Grid CA is not. Using the DigiCert Publicly Trusted CA that is trusted by common web browsers would greatly complicate OSG's RA procedures since that CA must follow commercial CA standards[11]. Hence it is much simpler for OSG to obtain its web certificates from a standard commercial provider outside of its own PKI. It is also the case that Open Science Grid, through Indiana University's InCommon membership and ownership of the opensciencegrid.org domain, can obtain web server certificates from the InCommon Certificate Service[12] at no incremental charge.

5 Recommendation on Path Forward

5.1 CA Selection

We believe it is reasonable for OSG to deploy and operate a PKI based on the DigiCert CA, with OSG-developed services serving as the front-end interfaces to that PKI for OSG RAs, Grid Admins and Users. Given the challenges in operating an IGTF-accredited CA, we recommend this path with the stipulations that follow in this section.

[11] http://www.cabforum.org/

[12] http://www.incommon.org/cert/

The DigiCert Grid CA[13] that would be utilized by OSG for its PKI is not in web browser trust stores. Hence, OSG needs for web server certificates, which seems to be commodity and modest, should continue to be fulfilled via a standard business mechanisms (from DigiCert or other provider) separate from the new OSG PKI.

We recommend that OSG RAs [9] perform identity vetting in compliance with DigiCert policies for issuance of new DigiCert certificates, without relying on existing DOE Grids certificates, to make a fresh start with the new DigiCert PKI rather than carrying forward a dependency on DOE Grids identity vetting. Rather than renewing existing DOE Grids certificates, certificate holders will apply for new certificates from DigiCert. This is expected to approximately double the load on OSG RAs during the one year transition period, given historical statistics that indicate 50-60% of user certificates issued each year by DOE Grids use the self-service renewal option.

5.2 Deployment of Front-end Services

Utilizing the DigiCert CA without front-end services would also be possible for user and low-volume host certificates. Bulk host certificates request methods would need to be modified to use the DigiCert REST API.

We recommend using the DigiCert web UI for administrative tasks that are infrequent and limited to OSG staff; it does not seem to make sense to spend the development effort to create front ends for such functionality.

5.3 Support of Other Current DOE Grids PKI Customers

During the pilot, correspondence was sent out to the DOE Grids PKI user community informing them of planned shut down of the DOE Grids PKI and informing them that interested communities could contact OSG if they were interested in using the planned OSG PKI service [2]. Four DOE Grids communities contacted OSG regarding using its planned PKI service: Fusion, ESG, NERSC and Argonne National Laboratory.

At this time following contact with Argonne is pending, planned for the OSG All Hand Meeting in March.

The other three communities, Fusion, ESG and NERSC, all have similar situations in that they each have a private PKI that they use for the majority of their certificate issuances[14] and rely on the DOE Grids PKI for a small number of certificates (10-20/year for Fusion and ESG, and roughly 100/year for NERSC) when IGTF accreditation is desired for interoperability or some other reason.

---

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

[14] ESNet currently operates the Fusion Grid private PKI. The NERSC PKI is based on a subordinate CA to the ESNet CA. Changes to these relationships are outside the scope of this document.

OSG supporting the IGTF certificates for these communities (not their private PKIs) as VOs does not seem like significant additional effort or cost. We should however continue to evaluate the additional effort as we progress, and if that effort becomes more than a 5% addition to supporting current OSG users, we should reopen discussions relevant to this decision.

5.4 Impact of Proposed Recommendations

5.4.1 Change in Risk Profile

The identified changes to OSG's risk profile by using DigiCert include:

- DigiCert CRLs only have a one-week lifetime (as compared to one month with DOE Grids PKI), which would necessitate an earlier move to disabling CRL checking in the event of a CRL service disruption. DigiCert has been asked if they would extend their CRL lifetime and is currently considering this.
- As a commercial CA provider, DigiCert is a more visible attack target than DOE Grids, but DigiCert is also held to a higher standard of operation (WebTrust and CA/Browser Forum versus IGTF). In 2011 we saw significant compromises of commercial CA providers (DigiNotar, Comodo, etc.). While the DigiCert Grid CA is a private CA not trusted by browsers, it is hosted in the same operational environment as DigiCert's other public CAs. As with any external CA provider (DOE Grids included), there is risk to OSG that the provider will cease operations for a variety of reasons. Using a commercial provider versus a DOE lab provider arguably increases this risk.
- DigiCert is an independent party in that if they lose faith in OSG's ability to live up to its responsibilities as defined in the contracts and agreement between the two parties, DigiCert could reasonably quit serving OSG.

5.4.2 Change in OSG Policies and Practices

For the community: Changes to the OSG Policies and Practices [8] visible to the community that we have identified so far seem to be a matter of specifics and not of fundamental form. In general, the level of formality will increase. E.g.:

- There will be a new UI RA Agents and users use for certificate management.
- The agreements signed by RA Agents will be more formal in terms of language. We should do some education ahead of time to prep the community.
- There will be changes to the details of the API used for bulk host certificate requesting, but the workflow should remain the same.

Per our recommendation, there will be a one-time period when all users will need to request new certificates instead of allowing for re-issuance, which will increase load on the RA Agents.

For the operations staff: There certainly may be times where we need to involve DigiCert in debugging issues. We expect this fundamentally not to be too different that with the DOE Grids PKI, but this certainly needs more exploration.

For OSG management: With the DigiCert contract signed by Indiana University (IU), IU will be put in the position of key participant in any future negotiations and dispute resolutions.

5.5 Contingencies to these recommendations

- We need to reach agreement with DigiCert on the registration authority practice statement and contract. We expect to those agreements to define a SLA for the API that includes availability and change management.
- Indiana University purchasing and legal needs to approve the DigiCert contract.
- Funding for implementation, deployment and operations needs to be identified.

6 Project Management Report

Project Planning was started in early October 2011 and work on the project was officially initiated on November 1, 2011. The project was tracked via weekly conference calls chaired by the technical lead of this project with consistently strong attendance by most project team members. This provided a good mechanism for understanding issues, planning resolution, and addressing priorities of the tasks when they competed for resources.

The project was delayed about one week at the very start due to "initialization" of systems at DigiCert to issue certificates for start of testing; since we had built-in a small schedule buffer (in late-December) during project planning, we were able to keep the impact from propagating to the planned end-date of February 9, 2012.

6.1 Effort

The estimated effort is shown in Appendix A which was 5.86 FTE months; and this project had a well-defined project team early in the planning process which bounded the effort estimate. The actual effort expended on the project is shown in Appendix B; the total expended effort was 7.38 FTE months. This "overage" difference is almost entirely attributable to ITB testing effort; although we knew this work would be needed, we had had not included it in the original effort projections. There were other "localized" variations in effort expended by project team members and those are mainly attributed to helping our newest staff member learn about and become productive in this area of work.

Contingent on the decision to proceed to implementation of this project beyond the pilot phase, it would be beneficial to plan and track separately the effort from within

this funded project as contrasted with effort contributed by OSG and other project partner projects.

6.2 Tasks Completion and Open Items

As of when this report is written, all tasks were completed except for the following:

1. The "Ensure DigiCert is compatible with LHC job submission from EU" (WBS 1.3.3) task was not conducted during the OSG DigiCert Pilot due to delays in IGTF accreditation of the DigiCert Grid CA and unrecognized dependency on the agreement of a Registration Practice Statement between OSG and DigiCert. The IGTF accreditation process for the DigiCert Grid CA is now complete as of January 30, 2012, with the release of IGTF distribution 1.44, and we have reached agreement in principle on the Registration Practice Statement, so EU LHC compatibility testing can proceed in the near future.
2. The "Evaluate DigiCert ability to provide redundant and highly-available services (e.g. CRL)" (WBS 1.5) task was not fully completed due to effort constraint. We believe that the work that was accomplished here did project a positive trajectory on this matter as no important issues were identified.
3. WBS 1.8.2, 1.8.3, and 1.9 pertain to steps needed to negotiate a longer-term contract with DigiCert and procure a go/no-go decision from the OSG Executive Team. These steps are currently in-progress.

We intend to complete items 1 and 3 above before proceeding to the next phase of this project, assuming a decision to implement is reached by OSG management.

7 Lessons Learned

Lessons learned from the pilot, in no particular order, numbered for easy reference, are:

1. The Pilot process was invaluable for establishing an understand of what functionality DigiCert does and does not provide relative to OSG needs, as well as an opportunity to address deficiencies prior to implementation.
2. Our identification of dependencies was imperfect, particularly between technical and policy items. Some of these dependencies would probably have required collaboration from DigiCert in the Pilot planning phase to identify.
3. Changing CAs has a number of potential aspects to it, which could be used to organize the change:
    a. Policy differences in terms of registration and vetting. A real challenge to understanding these policies differences is nomenclature differences between organizations.
    b. Policy changes in terms of certificate and CRL lifetime.

   c. Namespace changes in terms of the distinguished names in the issued certificates. Different CAs normally don't have overlapping namespaces.
   d. Technical changes in the user and other interfaces.
   e. Level of trust in the CAs by collaborators and other relying parties.
   f. Changes in risk profile due to differences of the organization supporting the CA. Objectively analyzing these differences is not easy nor is it clear there is a well-defined process for doing so.
4. DigiCert, in a manner we believe is common for most commercial CAs, thinks of customers are mapping cleanly to DNS domains and being authoritative for those domains (e.g., Indiana University is authoritative for iu.edu, indiana.edu, etc.). OSG, outside of opensciencegrid.org, has users in many domains but is not authoritative for any of them. The assumption of DNS authority effects policies in that there is an assumption that DNS points of contact are aware of all host certificate requests, which is not true for OSG host certificate issuance.
5. OSG, in supporting clusters, requires many more host certificates than would be standard for a typical commercial customer, who would only require certificates for secure web servers.
6. OSG's model of VOs as authoritative for user certificate issuance mapped rather well, nomenclature aside, into DigiCert's notion of business users with in an organization.
7. OSG's requirement for secure web server certificates is better served by a different PKI than its user and grid host certificates. This is because secure web server certificates are best issued by a CA that is in commodity web browsers, and such CAs have policies around issuance that are much more strict that IGTF requirements and hence would require greater changes to OSG's policies and procedures.

8 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.

Appendix A Projected Effort for Project

Name		FTE Level		Start	End		FTE Months
Jim Basney		0.35		10/1/2011	2/1/2012		1.42
Mine Altunay		0.15		10/1/2011	2/1/2012		0.61
TBD-implementer		1		11/1/2011	2/1/2012		3.02
Chander Sehgal		0.1		10/1/2011	2/1/2012		0.40
Von Welch		0.1		10/1/2011	2/1/2012		0.40
Total FTE Months							5.86

Appendix B Actual Effort Expended for Project

	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Total
Jim Basney	0.15	0.15	0.25	0.35	0.10	1.00
Mine Altunay	0.20	0.60	0.30	0.30	0.10	1.50
Jeremy Fischer	0.00	0.50	0.85	0.75	0.10	2.20
Chander Sehgal	0.10	0.05	0.05	0.08	0.05	0.33
Von Welch	0.20	0.20	0.20	0.20	0.05	0.85
ITB Staff for Testing[15]	0.00	0.60	0.90	0.00	0.00	1.50
Actual FTE Months	0.65	2.10	2.55	1.68	0.40	7.38
Planned FTE Months						5.86
FTE Months Overage						1.52
Overage Percent						26%

[15] Effort contributed by existing staff in the OSG Project.

Appendix C Project WBS

ID	WBS	TaskName	Start_Date	Finish_Date	Percent
0	0	OSG IdMgmt using DigiCert	10/25/11	02/09/12	80%
1	1	Trial/Pilot Phase	10/25/11	02/09/12	80%
2	1.1	Initial agreement with DigiCert to gain testing access for Trial	10/25/11	10/31/11	100%
3	1.2	Initialize: Get credentials and issue DigiCert certificates via Web interfaces	11/01/11	11/04/11	100%
4	1.3	Validate suitability of DigiCert certificates	11/07/11	01/19/12	89%
5	1.3.1	Monitor IGTF accreditation process of DigiCert.	12/09/11	01/19/12	100%
6	1.3.2	Demonstrate ability of DigiCert certificates (user, host, service) to function properly with VDT and other OSG software at various sites	11/07/11	12/05/11	100%
7	1.3.3	Ensure DigiCert is compatible with LHC job submission from EU	01/13/12	01/19/12	0%
8	1.4	Validate suitability of DigiCert processes to support OSG workflows	11/07/11	12/14/11	100%
9	1.4.1	Prototype and demonstrate ability for OSG to front DigiCert CA backend with own frontend issuance process (components 2-4) by prototyping those processes (type 3 outsourcing).	11/16/11	12/06/11	100%
10	1.4.2	Demonstrate ability for users and RAs to revoke certificates in a timely manner	11/07/11	11/14/11	100%
11	1.4.3	Demonstrate ability for OSG RAs to gather statistics about certificate issuance and ability to intervene when number of certificate requests exceeds allotted number in the contract	11/15/11	11/21/11	100%
12	1.4.4	Demonstrate ability for OSG RA to monitor Agent and GridAdmin actions for auditing purposes	11/22/11	11/30/11	100%
13	1.4.5	Demonstrate ability for storing and archiving artifacts (auditing) from certificate issuance workflows	12/01/11	12/07/11	100%
14	1.4.6	Evaluate legal and technical issues on whether we can issue new DigiCert certificates based on existing DOE Grids certificates to allow existing certificate holders to have certificates renewed as opposed to new certificates being issued.	12/08/11	12/14/11	100%

15	1.5	Evaluate DigiCert ability to provide redundant and highly-available services (e.g. CRL)	12/15/11	12/22/11	30%
16	1.6	Mid-term Mgmt Meeting between OSG and DigiCert	01/06/12	01/09/12	100%
17	1.7	Update IdM contingency plan based on DigiCert as Platform	12/15/11	01/05/12	100%
18	1.8	Establish longer term contract with DigiCert	01/10/12	02/03/12	56%
19	1.8.1	Decide which institution will own contract	01/10/12	01/16/12	100%
20	1.8.2	Draft OSG RA policies and practices acceptable to DigiCert	01/10/12	01/16/12	60%
21	1.8.3	Negotiate terms of longer term contract	01/16/12	02/03/12	40%
22	1.9	Post-trial evaluation and review with OSG-ET to decide go/no-go for next phases	01/20/12	02/09/12	25%

Appendix D Details on DigiCert API Testing

The initial foray into the DigiCert API was not any easy one. The documentation set forth from DigiCert was limited and had little actual functionality. At the onset of the pilot, only two API functions were available. At the completion there are still just five, but with assurances from DigiCert that more API calls will be forthcoming.

At the start of the pilot, grid_request_host_cert (request host based certificates) and grid_request_email_cert (request and send client certificates) were the only API functions available. Initial attempts to use them resulted in errors stemming from some "security by obscurity" features that were not documented in the GridCertAPI document we received from DigiCert – notably the necessity for a "validity=1" parameter to be passed with the POST and the setting of the USER AGENT to GridAPIClient/0.1 (DigiCert Grid API). The only errors returned were 400 series web server errors with no useful output and not with the detailed error messages shown in the document. Contact with DigiCert helped rectify the malformed POST calls.

An additional error was found in the client cert request in that the email address used to notify the user that a certificate was ready for retrieval may only be one of the DigiCert approved domains. Despite the fact that my registered email address with DigiCert is Jeremy@pobox.com, I had to use my Indiana.edu identity for the API call to actually be successful. This was another "security feature" not noted in the document and has potential issues that will be addressed at the end of this section.

Even though the calls worked, the results were mixed. The client certificate API request emails the user using the email address as part of the request. An email was received with a link to DigiCert. Upon clicking that link, I was taken to their site where it actually installed the new certificate in my browser for me. This is a nice added feature for the user in that they do not have to have knowledge on saving and then importing certificates into their browser manually. This was tested successfully with Firefox and Safari.

The grid host certificate request also worked but does not return an email to the requesting user as the client request does. The certificate is not returned to the output but rather has to be retrieved via the web MKPI interface. This is not necessarily problematic but a future API call to retrieve the certificate would allow more complete automation from the user's perspective. DigiCert lists a Retrieve Grid Host Cert API call in the API functionality matrix we received late in the pilot. However, this function call is not documented in the API. If it exists, it is not documented. This would be the missing link in creating a fully API based grid host certificate request system.

During the course of the API testing, the GridCertAPI document was updated and released. Three new functions were added at this time: grid_request_host_revoke, grid_approve_request (to approve revocations **and** new host certificates), and grid_reject_request (to reject revocations **and** new host certificates). Shortly after the introduction of these new functions, the error handling in the API also changed, matching the documentation, and yielding more useful messages upon failure. No

sample requests for the approve or reject calls were included in the new documentation which made testing a bit more difficult, but some trial and error proved the concepts to be workable.

In addition, one more update was released in late January, as the pilot was winding down. This update included almost all of the items that had been previously missing, including the necessary log retrieval, retrieve grid host certificates, approve and revoke client certificates, view pending certificate requests, and view existing certificates. Also included in this update was a detailed listing of error codes and meanings. To date, I have not found where these newly defined error codes come into play, but the fact that they are now included with the API documentation bodes well for future updates. At the outset, there was no regard to error handling at all.

The DigiCert API and UI model do not currently utilize or recognize any sort of tiered security structure. The API only recognizes privileged or non-privileged where the non-privileged requests are summarily rejected. The Web UI sees User and Administrator. A normal User of UI may still perform certain functions. In order to provide tiered access for Grid Admins, End Users, System Administrators, and SuperUsers, either DigiCert's security model will need to be changed or all functions will need to be controlled via a security hierarchy on an OSG frontend server.

In summary, the DigiCert API as it stands is a good start but is far from robust. Several factors need to be addressed to make this a more usable system for production usage:

1. Error handling needs to be more robust and the ability to retrieve the certificate generation logs is required. At this point, troubleshooting is not just difficult but often impossible without enlisting the help of DigiCert to give specific error messages. It adds an unnecessary layer of difficulty and delay to the process of building and maintaining a system. Update: Post the January 19th update, error handling has indeed improved. It still does need to be more verbose, but now that log retrieval is possible, the capabilities of the API system are much improved.
2. API should be more robust. All of the necessary functions to generate, approve, revoke, generate CRL, etc. should be present in the production model. At this time, there are still portions of the administration that must be done from the MKPI website. To be complete we need calls to: retrieve grid host certificates, approve and revoke client certificates, generate CRLs, retrieve client and host certificates, view pending requests for certificates and revocations, retrieve logging/error information, and request information on existing certificates. One additional call necessary is a renew certificate function that automatically generates a CRL for distribution. Update: Post the January 19th update, the API has calls for all but generating CRLs and certificate renewal.
3. Using DigiCert order numbers instead of serial numbers for certificate approval, revocation, (and when available) retrieval is necessary. Barring that change, an API call to translate the order number to serial number

would be necessary. Update: Post the January 19th update, the API allows for either DigiCert order numbers or serial numbers for most API calls. Approving or rejecting requests obviously does not allow serials since the certificates have not been approved to reach the point of getting a serial number.

A final item for API development would be to provide a separate API test bed so that changes are not being performed on the live system as they were during the pilot. In addition, change management structure should be added so all parties are aware of upcoming changes well in advance and so they might be able to prepare adequately for said changes.

The DigiCert API is a good start and has potential to be a usable service. As further explorations into existing OSG/DOE scripts and tools are completed, I feel that additional work expanding the API will come into focus. The API must meet the current needs of the OSG workflows before it can be used for production services. In addition, the cooperation of DigiCert to create complete documentation and provide useful and complete error handling and logging would be necessary to be able to even create the initial system.

Appendix E Known Contingency Plan Issues to address.

- 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.
- 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?