Options and Recommendation for Replacement of the DOE Grids CA in the OSG PKI

October 5th, 2011

Mine Altunay, James Basney, Von Welch

Executive Summary

The Open Science Grid 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. The goal of this document is to:

> Enumerate and describe requirements and options, and recommend a plan *(including schedule and costs), for replacing the DOE Grids CA in the OSG identity management system such that OSG continues smooth operation in meeting the identity management needs of its user community.*

The authors evaluated the use cases satisfied by the existing CA and determined requirements for the new CA: (1) interoperability with LHC collaborators derived from IGTF accreditation, (2) ability to provide certificates to 1000+ OSG users distributed across the USA, vetted by 36 registration authorities agents, (3) ability to provide host certificates for 300+ gatekeepers plus 8000+ worker nodes to 40 grid administrators at roughly 80 OSG resource provider sites, (4) ability to provide web and other service certificates, and (5) ability to sustain operation into the foreseeable future.

The authors evaluated, based on the use case requirements and other operational factors, eleven options as replacements for the DOE Grids CA: the CILogon Basic CA, the CILogon Silver CA, the InCommon Certificate Service, the NCSA CA, the planned XSEDE CA, a new OSG CA, migrating the current DOE Grids CA to be an OSG service, the CERN CA, the DigiCert commercial CA, the VeriSign commercial CA, a planned Globus Online Identity Provider, and the Fermi National Laboratory KCA. Additionally, the authors considered two options other than a PKI: InCommon and DANE/DNSSec.

Many of the options were found to be viable for serving portions of the OSG user community, but only three options were found to be viable to provide a replacement that would serve the whole OSG user community: contracting with the DigiCert CA, OSG deploying and operating a new CA, and migration of the DOE Grids CA to OSG operations.

The main positive of OSG operating its own CA is control and the avoidance of external dependencies. The main negative of OSG operating its own CA is developing

and maintaining expertise in CA operations. Two OSG sites with expertise, FNAL and NCSA, expressed concern about taking on operating an OSG CA at this time due to other factors.

The main positives of the DigiCert option are that it could be faster and cheaper to deploy, with less effort and skills required by OSG, and probably more reliable in operation. Based on the experience of the authors, deploying an IGTF-accredited CA requires an FTE-year of effort over a year and the estimate is using a commercial CA could reduce that by half or more. Negatives of the DigiCert option are increased risks related to control (unforeseen differences in the interfaces provided by the CA and the current DOE Grids CA), legal/policies issues (signing a contract; assuming DigiCert achieves IGTF accreditation) and an ongoing reliance on an outside party.

Migration of the DOE Grids CA is not as clean as we hoped because the current CA is at end of life and its replacement is not yet in production, adding a number of unknowns to the process. The CA also has entanglements with an ESNet CA hierarchy and other non-OSG users, which complicates the matter. The negatives of OSG operating its own CA apply whether OSG deploys and operates a new CA or migrates the DOE Grids CA to OSG operations.

We estimate that, to first order, ongoing operational costs of all three options are comparable. The DigiCert option offers a possibly cheaper and faster deployment.

Balancing these factors, the authors recommend the DigiCert option. However, to mitigate deployment and contractual risks associated with using DigiCert, we recommend a three month pilot period before fully committing to this path.

If DigiCert were to fail to meet OSG needs, OSG could then choose one of the other two viable options. In choosing a fall back option between OSG establishing a new CA or migrating the new DOE Grids CA, both options are fraught with problems, but the authors would recommend OSG establish its own CA.

The authors recommend that to provide a smooth transition that the DOE Grids CA will need to continue issuing certificates for one year and operate in a limited mode, issuing CRLS, for a second year until all of its certificates have expired.

The authors also recommend that in parallel with any chosen path, OSG should continue to foster options that don't require IGTF accreditation with its collaborators at the DOE Laboratories and LHC in order to give it more options in the future.

1 Introduction and Goal of this document

The Open Science Grid 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. The OSG PKI serves the OSG community by providing X.509 certificates to resource providers (those operating compute and storage elements) as well as end users of the OSG and collaborators such as the LHC distributed across the United States. A more complete description of the OSG PKI can be found in Section 4.1 of the OSG Blue Print [1].

A key component of the OSG's PKI is a certificate authority (CA) operated by ESNET, which we refer to in this document as the DOE Grids CA. The DOE Grids CA has four main functional components: a certificate issuance process that generates user and host certificates, a web interface that allows users to request certificates, a vetting interface that allows designated personnel acting as registration authorities (RAs) to approve user certificate requests, and a command-line interface that allows for the request and issuance of host certificates (potentially in bulk) to authorized grid administrators.

The authors of this document were asked to undertake the following, which is the goal of this document:

> Enumerate and describe requirements and options, and recommend a plan *(including schedule and costs), for replacing the DOE Grids CA in the OSG identity management system such that OSG continues smooth operation in meeting the identity management needs of its user community.*

The highest priority of the recommended plan is the continued smooth use of the OSG by its users as supported by the OSG PKI. Any improvement of the OSG PKI, while desirable if it were to occur as a byproduct of achieving the primary goal, is not itself a goal.

Our scope is limited to OSG users in the United States under the premise that other OSG users could be served by their respective national CAs or project CAs such as the CERN CA.

Supporting other users of the DOE Grids CA besides OSG is out of scope of this document.

2 Technical Background

We briefly introduce some background, terminology and concepts used throughout the remainder of the document.

2.1 The DOE Grids CA

The DOE Grids CA[1] is part of a CA hierarchy. It is subordinate to the ESNet Root CA and has peers (i.e. other CAs subordinate to the ESNet root) that serve NERSC, the Fusion community and ESNet itself.

The DOE Grids CA is currently on the brink of transition with an "Old CA" that is currently providing service and a "New CA" that is close to being production ready.

The Old CA is being retired as it is utilizing CA software, an operating system (Solaris) and an HSM that are no longer supported by their respective vendors.

The New CA is operational at Berkeley with a 2nd instance in process of deployment at BNL (but operated by ESNet staff at BNL). The main hurdle of making the New CA production ready for OSG is in the interfaces for certificate issuance (both user and host) and for the RAs [4]. ESNet is spending approximately $70k/year on licensing for the New CA (~$15k for 3 HSMs and ~$55k for CA software[2]).

A two-FTE team operates the DOE Grids CA, with roughly a third of an FTE spent on administration, a large fraction of an FTE on user support, and the remainder on R&D.

2.2 Outsourcing Taxonomy

Various options discussed in this document involve outsourcing of the OSG PKI, that is having parts of the PKI operated by a third party who has some sort of relationship with OSG (e.g., formal contract, shared desire to serve the scientific community). In these discussions the authors found defining, albeit simplistic, levels of outsourcing to be useful for clarity of discussions:

1. Complete outsourcing: OSG would direct users to the PKI provider and have no direct involvement in the process except to mediate problems. For example, this describes the relationship that InCommon has with Comodo.
2. Exposed outsourcing: OSG would direct users to a third party but OSG is in the loop and has visibility to workflows. For example, this describes the current relationship between OSG and the DOE Grids CA, where ESNet operates the CA, but OSG has influence over the process and has visibility into open tickets.
3. Hidden outsourcing: OSG would completely hide the outsourcing such that user never directly interacts with the outsourcing party and wouldn't know if the outsourcing provider changed. For example, a commercial provider of a network-based CA service where OSG would operate the user and RA interfaces.
4. No outsourcing: OSG would handle every aspect of the PKI service.

[1] https://pki1.doegrids.org/

[2] 15k certificates at $3.74/certificate. This is an acknowledged overprovisioning to avoid running up against a licensing limit.

2.3 gLexec

gLexec[3] is a process run on compute nodes. It authenticates an end-user certificate and does a setuid() call so that processes run under an account configured by the local administrator for the submitter of the process. The use of gLexec has two ramifications for the OSG PKI:

1. It requires an end user certificate be used to authenticate the job submission.
2. It requires the compute node have a host certificate to authenticate to GUMS for user authorization. On large clusters, this creates a demand for a large number of host certificates and it is believed this accounts for the majority of OSG's host certificate usage.

2.4 International Grid Trust Federation (IGTF)

The International Grid Trust Federation (IGTF) [2] provides accreditation of CAs. IGTF provides for a standard set of security controls and, perhaps more importantly, it provides for interoperability. An analogy is that IGTF provides for the international Grid PKI community what InCommon is in process of doing for the U.S. higher education Shibboleth/SAML community. The IGTF has made PKI interoperability much more tangible for many VOs by defining a set of CAs that conform to a set of defined profiles. This has allowed VOs to forgo doing their own vetting of these CAs and instead accept the set of IGTF accredited CAs as both a security and interoperability measure.

This use of IGTF to vet CAs is a significant saver of work for many VOs, but does mean a significant hurdle for introducing a new CA to support those VOs. IGTF accreditation requires complying with one of the IGTF profiles. Simply put, those profiles require the use of hardware security modules (HSMs) that are difficult to work with, and a user vetting procedure that requires either in-person vetting or a reliance on a professionally maintained user database. Since OSG does not have a central user database, its only current option for an IGTF CA (besides introducing a new profile to IGTF) is the in-person vetting process OSG has in place today.

In OSG, interoperability with the LHC is the primary driver for IGTF accreditation. DOE laboratories also contribute to this need, however it is unclear how much this requirement is driven indirectly by LHC VOs, as large users of the laboratory resources, or by the laboratories themselves.

3 OSG PKI Use Cases and Requirements

In this section we review the use cases that the OSG PKI supports and the requirements placed on it, and in turn the CA, by those use cases. These requirements are used subsequently in the document for evaluating alternatives to the DOE Grids CA.

[3] https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/GlexecInstall

3.1 End Users Use Cases

Some of the use cases for end user certificate can be classified based on virtual organizations (VOs):

- *LHC Users*: Includes users from CMS, ATLAS[4] and Alice who use certificates issued by the OSG PKI to access LHC resources. LHC has a policy [3] of requiring certificates to be issued by a CA accredited by the IGTF (the DOE Grids CA is so accredited). This requirement extends to both user certificates and host certificates used to authenticate compute and storage resources.
- Engage and OSG VOs: VOs that grant access to OSG to users who do not belong to other VOs. These VOs currently use OSG PKI certificates, but do so because it was the default method when they formed and have no unusual OSG PKI requirements of their own.
- GLOW, nanoHUB, NEES: These VOs do not issue end user certificates, but instead use a single certificate (pilot or community) to issue jobs on behalf of users who are authenticated via other means. These VOs place no unusual requirements on the OSG PKI.

Other use cases spanning or not particular to VOs are:

- Various glide-in users on systems not using gLexec: Similar to GLOW, nanoHUB and NEES, users are not issued end user certificates; they are authenticated by other means and then submit jobs via a pilot certificate. These VOs place no unusual requirements on the OSG PKI.
- OSG Build System: The OSG Build system uses PKI certificate for authentication[5]. It places no unusual requirements on the OSG PKI.
- *Access to OSG web-based information systems:* As part of the OSG PKI certificate issuance process, users receive a copy of their certificate in their web browser. This copy is then used to authenticate user access to the OSG Information Management System (OIM), TWiki, DocDB, MyOSG, etc.

3.2 Host Certificate Use Cases

The OSG PKI maintains a list of grid administrators who are authorized to request host certificates through a set of command-line scripts[6]. Three categories of host certificates were identified:

- *End-user visible host certificates*: These certificates are used in services that are accessed directly by clients running on end user systems. Some users of

[4] We note there is some debate currently in ATLAS about requiring the use of gLexec [5]. The removal of this requirement would relax the ATLAS VO requirement on end user certificates.
[5] Personal correspondence with Brian Bockelman 8/29/2011.
[6] https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/GetGridCertificates

these services are users from the broader LHC community, who by LHC policy [3] expect certificates to be issued by IGTF-accredited CAs.

- *Worker node certificates*: These certificates are running on cluster worker nodes and are not directly accessed by end user clients, but instead by processes running on cluster head nodes. There was some discussion by the authors that IGTF accreditation may not be required for these certificates even in the context of VOs who require such accreditation, since interactions could be entirely in the scope of OSG control, but we felt this fact needs to be verified, which there is not time to accomplish in the timeframe of authoring this document.
- *Service (aka Community, Pilot, Robot) certificates*: Certificates used by processes acting as clients, either automated or on behalf of a user. Similar to worker node certificates, the authors felt there was potential of using certificates from a CA that was not IGTF accredited, but more research is needed to verify this.

3.3 Requirements from Use Cases

Requirement #0: Certificates Must Work with VDT

Any issued certificates need to work with the VDT Software stack. 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)[7]. Hence, while 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 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). 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 1000+ OSG users distributed across the USA, vetted by 36 registration authorities agents.

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

Requirement #3: Ability to provide host certificates for 300+ gatekeepers plus 8000+ worker nodes to 40 grid administrators at roughly 80 OSG sites.

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

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

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. OSG also uses "service" certificates in a manner unique to the computational grid community, e.g. with Glide-in systems.

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

As discussed below, 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.

4 Examined Options

As we evaluated options for replacing the DOE Grids CA, we found they split into two groups. The first group represents options operated by external parties that could serve a portion of the OSG user community. The second group represents options operated by OSG (or under contract with OSG) that could serve as a "catch-all," that is, they could handle all OSG users, including those that could not be handled by any of the first group. In the third subsection we discussion non-PKI alternatives we considered.

Table 1, on the following page, provides an overview of the examined replacement options. Details are contained in the subsequent text.

CA Option	Requirement				
	(1) LHC Compatibility	(2) User Certificates	(3) Host Certificates	(4) Web and Service Certificates	(5) Allow for sustained operations
CILogon Basic CA	No	For some portion of OSG users	No	No	Future funding in question.
CILogon Silver CA	Yes	For a very small portion of OSG users.	No	No	Future funding in question.
InCommon Certificate Service	No	For some portion of OSG users	For some portion of OSG institutions.	For some portion of OSG institutions.	Yes
NCSA CA	Yes	Would require major changes to support non-NCSA users and institutions.			Some concerns.
Planned XSEDE CA	Probably	Uncertain	Uncertain	Uncertain	Uncertain
CERN CA	Yes	For about 50% of OSG users.	No	No	Yes
Planned Globus Online IdP	Doubtful	Uncertain	No	No	Uncertain
FNAL KCA	Yes	Only for FNAL users	No	No	Yes
New OSG CA	Yes	Yes	Yes	Yes	Yes, assuming sufficient DOE Grids lifetime
Migrate DOE Grids CA to OSG	Yes	Yes	Yes	Yes	With coordination with ESNet
DigiCert Commercial CA	Yes (if DigiCert IGTF accreditation succeeds)	Yes	Yes	Yes	Yes, assuming successful pilot and sufficient DOE Grids lifetime
VeriSign	No	Yes	Yes	Yes	Yes
InCommon	No	N/A			No
DANE/DNSSec	Uncertain	No	Yes	No	No

Table 1: Comparison of Replacement CA Options.

4.1 Third Party CA Options

4.1.1 CILogon Basic CA

The CILogon Basic CA[8] is a CA that issues user certificates based on authentication of users via the InCommon identity federation. Because there is no defined standard for the level of identity vetting done by InCommon members, the CILogon Basic CA is not IGTF accredited. It issues only user certificates and not host certificates. OSG could outsource users to the CILogon Basic CA as either a type 2 or type 3 outsourcing, depending on the level of effort OSG wanted to expend on developing a front end service. A concern here is CILogon's NSF funding expiring in Fall of 2012.

Conclusion: The CILogon Basic CA would suffice for some OSG users, but cannot replace the DOE Grids CA by itself because of a lack of IGTF accreditation and support for host certificates. Long-term funding issues would need to be addressed.

4.1.2 CILogon Silver CA

The CILogon Silver CA[9] is an IGTF accredited CA that issues user certificates based on InCommon Silver authentication. OSG could outsource to the InCommmon Silver CA in the same manner as discussed for the InCommon Basic CA. No InCommon identity providers are yet accredited at InCommon Silver, so this CA is not yet operational. It is extremely unlikely that a critical mass of InCommon Silver identity providers will be available in the timeframe of an OSG CA transition.

Conclusion: The CILogon Silver CA is not yet a viable option.

4.1.3 InCommon Certificate Service

Comodo operates a CA for the InCommon Certificate Service[10] that issues user and host certificates to subscribers of the service. Subscription fees are $2,000-$20,000 for each institution in addition to InCommon membership fees. The CA is not IGTF accredited. There are two options for how OSG could use the InCommon Certificate Service:

- OSG could direct users to use their home institution's subscription to the InCommon Certificate Service to request user and host certificates (a type 1 outsourcing). A challenge here is that only 50 out of 92 OSG member institutions currently subscribe to the InCommon certificate service.
- OSG could subscribe to the InCommon Certificate Service and request certificates on behalf of its users. The challenge here is that it is not clear how OSG as a multi-organizational institution would function in the context of a service that assumes it is serving individual organizations.

Conclusion: It seems possible, with some negotiation and risk, that the InCommon Certificate Service could serve at least some of OSG's non-IGTF certificate needs. One

[8] http://ca.cilogon.org/
[9] http://ca.cilogon.org/news/cilogonsilvercaaccreditedbyigtf
[10] http://www.incommon.org/cert/

author has noted that the subscriber experience with Comodo through the InCommon Certificate Service is not without problems, with InCommon acting as a middleman between the users and Comodo with limited influence and visibility into what happens at Comodo.

4.1.4 NCSA CA

The NCSA CA[11] issues user and host certificates to NCSA/XSEDE users and administrators. It depends on the NCSA/XSEDE user database as part of the issuance process. This CA is funded by the XSEDE project, but there are concerns about the stability of this CA in the future due to recent changes in how its funding is being routed within NCSA.

Conclusion: Given the dependency on the NCSA user database and the funding concern, the NCSA CA does not seem like a viable option.

4.1.5 Planned XSEDE CA

An XSEDE CA is planned for operation by June 2012 but the project plan is not yet in place.

Conclusion: Given unknowns in both how and when it will be instantiated, relying on the XSEDE CA in the near future is a high risk.

4.1.6 CERN CA

The IGTF accredited CERN CA[12] issues user certificates to people in the LHC user database, which covers about 50% of OSG users. It also issues host certificates, but only to hosts in the cern.ch domain.

Conclusion: The CERN CA would be a viable option for OSG to direct its LHC users to (as a type 1 outsourcing).

4.1.7 Planned Globus Online Identity Provider

The Globus project is planning on providing identity management solutions, including a MyProxy CA, as part of its Globus Online service [6]. No specifics in terms of features or timeline are available

Conclusion: This CA is unlikely to be IGTF accredited and is high risk given uncertainties in features and timeline.

4.1.8 Fermi National Laboratory KCA

The FNAL KCA[13] is IGTF accredited to issue short-lived user certificates based on FNAL accounts. It includes software for using certificates easily with web browsers.

Conclusion: The Fermi KCA is dependent on the Fermi National Laboratory HR database, meaning it can only serve a small portion of the OSG user community.

---

[11] http://security.ncsa.illinois.edu/CA/
[12] https://ca.cern.ch/ca/
[13] http://computing.fnal.gov/xms/Services/Getting_Services/Certificates

4.2 OSG "Catch All" CA Options

The options in the previous section would serve portions of the OSG community. However the authors do not feel that even in combination they could serve all of the OSG community. Host certificate would be a clear problem. The coverage for user certificates includes some large fraction of the OSG user base, but is not complete.

Hence it seems at a minimum for the near-term future, OSG would need some form of "catch all" CA that would serve users that could not be served by the above options. Options for this catch all CA follow.

4.2.1 From Scratch CA

A new CA deployed at an appropriate OSG site (Fermi National Laboratory, Indiana University's GOC, or NCSA Cybersecurity group are potentially viable[14] options and there may be others), funded and staffed by OSG and under OSG control.

Conclusion: A viable option, though costly to develop all four CA components, both in terms of personnel time and expertise.

4.2.2 Migrating the current DOE Grids CA to be an OSG service

ESNet would transfer control and operations of the doegrids.org domain, the CA hardware and all associated data (keys, records, etc.) to OSG, who would assume responsibility for its continued operations. This would involve hardware at Berkeley moving to an OSG site (such as one of the sites considered in the previous option). An unexplored question is whether the second CA at BNL could remain there, which would be beneficial in terms of providing redundancy.

Conclusion: The Old CA is at end of life and is not worth migrating because it would be hard-to-impossible to maintain. The New CA bears some risk because it is not yet in operation, it is part of a CA hierarchy and would need to be untangled, it serves other customers, we would be reliant on the availability of ESNet staff to effect its transition, and we would have bureaucratic risk and red tape of transferring hardware to another organization. The high annual cost for software and hardware support at $70k seems quite steep.

4.2.3 DigiCert Commercial CA

The DigiCert CA[15] is pursuing IGTF accreditation for issuing user and host certificates and we believe that barring an unexpected problem, they will be successful in the coming months. The DigiCert CA could represent an outsourcing of type 2 or type 3, depending on the level of effort OSG wanted to put into developing front ends. We focused our consideration on a type 3 outsourcing with OSG acting as

[14] No formal discussions with any of these organizations has taken place regarding their willingness, particularly with regards to the estimated effort levels given later in this document. Author affiliations should not be construed as organizational endorsement.

[15] http://www.digicert.com/

a front end and being the sole interface for the user. Type 2 could be done with less effort and more quickly at the cost of OSG control and user experience. Estimates from DigiCert for OSG's current issuance numbers are approximately $86k/year.

Conclusion: DigiCert has some risk in terms of how OSG would interface with them and the effort required to establish user interfaces, but is a viable option. Ideally we would conduct a pilot with DigiCert before committing to ensure they could meet OSG needs and deliver a user-friendly experience.

4.2.4 VeriSign Commercial CA

Similar to DigiCert, VeriSign[16] represents a commercial outsourcing. However, DigiCert is the only known commercial CA seeking IGTF accreditation. A verbal quote from VeriSign is approximately $150k/year. There is some concern with how their host certificate service will work for OSG given its multi-institutional nature (will they require every organization to work through their DNS administrators?).

Conclusion: Given lack of IGTF accreditation, risks of host certificates and costs, there seems no reason to consider VeriSign as a preferable option to DigiCert.

4.3 Non-PKI Alternatives

4.3.1 InCommon Federation

InCommon[17] offers SAML-based identity federation to the U.S. Higher Education community. It is used by the CILogon CA, described previously, to authenticate certificate requesters. OSG could look to replace its PKI with SAML, but it's not clear in the near term how interoperability with LHC would be accomplished (international federations[18] are still a field of study). It is also not clear how all the workflows (particularly command line activities) would operate without a PKI. Adding SAML support to VDT would be a substantial software development task.

Conclusion: OSG should continue to explore InCommon/SAML, but it is not a viable solution in the near term.

4.3.2 DNS-based Host Authentication (DANE)

DANE[19] is a proposed standard to leverage secure DNS (DNSSec)[20] to replace the functionality currently supplied by host certificates. The use of DANE in OSG would be predicated on its support in VDT, which will be a substantial software development task, and a broad support for DNSSec among OSG sites.

---

[16] http://www.verisign.com/
[17] http://www.incommonfederation.org/
[18] https://refeds.terena.org/index.php/Main_Page
[19] https://datatracker.ietf.org/doc/draft-ietf-dane-protocol/
[20] http://www.dnssec.net/

Conclusion: The software development changes alone make this a non-viable solution in the near future. The requirement for DNSSec would need to be researched as adoption is far from ubiquitous.

5 Comparison of Viable Options

Three options in the previous section were considered viable replacements for the DOE Grids CA for the OSG PKI: using the DigiCert commercial CA, deploying and operating a new OSG CA, and migrating the DOE Grids CA to OSG operations.

The following table compares the choices. Note that operational costs are not complete. There is some uncertainly in those figures as the two options where OSG operates the CA do not include tier 2 user support currently provided by ESNet, and it is unclear without experience how much support OSG would need to provide in the DigiCert case.

Attribute	DigiCert Commercial CA	Deploying a new OSG CA	Migrating DOE Grids CA to OSG[21]
Time to deploy	12 months, including a 3 month pilot.	11 months	6 months
Deployment Cost	1 FTE TBD, .35 FTE Basney, .1 FTE Altunay, .1 FTE Sehgal, .1 FTE Welch,; $10k for commodity servers to run interfaces; $10k for DigiCert contract for Pilot; $86k/year for DigiCert contract starts with deployment	1 FTE TBD, .35 FTE Basney, .1 FTE Altunay, .1 FTE Sehgal, .1 FTE Welch, $15k for HSM hardware, $55k for software licensing, $10k for commodity servers to run interfaces	6 FTE-months TBD, .35 FTE Basney, .1 FTE Altunay, .1 FTE Sehgal, .1 FTE Welch,; $10k for commodity servers to run interfaces
Operational Cost (for operation of CA, does not cover tier 2 user support currently handled	.75 FTE/yr TBD, .1 FTE Altunay or Basney, $86k/year estimated based on DigiCert quote	1.25 FTE/yr TBD, .1 FTE Altunay or Basney, $5k/year for HSM support, $55k for software	$70k for software licensing and hardware support plus .5

[21] Note that the migration option was not explored as fully as the other two options and estimated effort and costs should be considered preliminary.

by ESNet staff)		licensing,	FTE/year
Risk	Legal/contractual and technical inflexibility. IGTF accreditation looks likely but is still not certain.	Complexity, staff continuity, organizational commitment	Bureaucratic risks with getting equipment transferred. Reliance on ESNet personnel availability. Disentangling from CA hierarchy and other DOE Grids customers.
Reliability	Dependency on single external supplier	Dual site redundancy possible (not budgeted)	Dual site possible (not budgeted)
Improvements	Host certificates would be accepted by browsers without pop-ups.	No major improvements planned.	No major improvements planned.

6 Recommendation

Balancing all factors the authors recommend the DigiCert option. Two reasons we consider outsourcing appealing are:

- Pragmatically, running an IGTF-accredited CA is difficult because of a number of reasons, a big one being the operation of the HSM and coupled software. This operation is a steep learning curve and requires specialized expertise. We don't have a known site in OSG right now that is eager to take this on. NCSA and FNAL both have experience and potential to leverage other efforts, but have organizational issues in taking this on right now. IU has operational experience with the GRNOC, but no particular relevant experience or related effort.
- Longer-term, we'd like to see OSG become broader in terms of serving the identity management needs of its VOs. The IGTF PKI serves a portion of OSG's audience (LHC collaborators), but there doesn't seem to be a demand for that type of identity management outside of those VOs (i.e., most use it because it was the default choice when they started). We think there is a great deal to

be gained by exploring and adopting (and perhaps ultimately transitioning entirely to) other models of identity management that better fit VO desires, particularly for end users. Minimizing the investment into the IGTF PKI would allow OSG to more quickly move forward on other fronts.

However we acknowledge there are significant risks, both technical and contractual, with this approach. To address those risks, we recommend a three-month pilot period before fully committing to this path.

If DigiCert were to fail to meet OSG needs, OSG could then choose one of the other two viable options. In choosing a fall back option between OSG establishing a new CA or migrating the new DOE Grids CA, both options are fraught with problems, but the authors would recommend OSG establish a new CA due to the complications involved with migrating the DOE Grids CA, namely: (1) the untested nature of the New CA, (2) complications with untangling it from the ESNet CA hierarchy, (3) complications of its existing non-OSG users, (3) a reliance on ESNet staff outside of OSG's control, (4) unknown procedural issues with equipment transfer, and (5) the ongoing software licensing fees.

The authors recommend that to provide a smooth transition that the DOE Grids CA will need to continue issuing certificates for one year and then for a second year operate in a limited mode, issuing CRLs, until all of its certificates have expired.

The authors also recommend that in parallel with any chosen path, OSG should continue to foster options that don't require IGTF accreditation with its collaborators at the DOE Laboratories and LHC in order to give it more options in the future.

7 References

1. OSG Document 18-v12: A Blueprint for the Open Science Grid. http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=18
2. The International Grid Trust Federation. http://www.igtf.net/
3. Joint Security Policy Group. Approval of Certification Authorities. Version 3.0, August 2008. https://edms.cern.ch/document/428038
4. DOEGrids CA transition to New RHCS8 software. March, 2011. https://twiki.grid.iu.edu/bin/view/Security/NewRASoftware
5. ATLAS gLexec memo. Undated. https://indico.cern.ch/getFile.py/access?contribId=8&resId=0&materialId=0&confId=115406
6. Tuecke, S. Globus Online Future. April, 2011. http://globusworld.org/files/2011/04/Futures.pdf
7. Contingency Planning for the dependencies of OSG on the DOEGrids CA service. https://twiki.grid.iu.edu/bin/view/Security/IdMContingencyPlanning (Page access may be restricted.)