Open Science Grid

OSG PKI Transition: Status and Next Steps (and Lessons Learned)

Von Welch
OSG PKI Transition Lead
Indiana University Center for Applied Cybersecurity Research

Key Message

DOE Grids CA stops issuing new certificates March 23rd, 2013.

(in 10 days)

VOs should already have:

1) Enrolled with new OSG PKI

2) Be ready to handle new user identities

3) Updated documentation and processes

Project Overview and Goals

DOE/ESnet has announced shutdown of DOE Grids CA.

OSG is transitioning that CA functionality to an OSG service.

In coordination with ESnet, project goal is to manage a smooth transition of PKI functionality to the new OSG service.

Community-wide Responsibilities

Previously ESnet and now OSG, will set policy and process, and provide mechanism to issue certificates.

VO and RPs continue to vet their user communities and authorize based on certificates.

What VOs need to do…

- Enroll RAs with OSG PKI
  - https://oim.grid.iu.edu/oim/vo
- Be prepared to handle changing user identities (DNs)
- Update documentation and internal processes

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

Resources

- OSG PKI Service: idmanager.opensciencegrid.org

- Manuals, how-tos, experiences:
  https://www.opensciencegrid.org/bin/view/Security/PKIDocumentationIndex

- Tomorrow:
  - 9:45am: Security for administrators, RA, GA *IT-159*
    - *Also: https://twiki.grid.iu.edu/bin/view/Security/OSGPKITraining*
  - 11:00am: Ask the Experts IT-152

Open Science Grid

Status

PKI is in operations –

- 39 VOs registered
- Issued 300+ user certificates
- Handled 350+ host requests (some for up to 50 certificates)

Web and command-line clients

We are listening and learning what's missing/wrong in new PKI.

Next Steps

Expect more missing features exposed as 23rd approaches and passes.

OSG PKI works at strong level (IGTF) to enable collaboration with EU and others. There is room for other solutions (e.g. CILogon) for those with lower security needs.

Lessons Learned

Not going to cover today, will include in slides.

Contributors to the Transition

Mine Altunay, Jim Basney, Tim Cartwright, Alain Deximo, Jeremy Fischer, Soichi Hayashi, John Hover, Viplav Khadke, Christiane A. Ludescher-Furth, Ruth Pordes, Rohan Mathure, Robert Quick, Alain Roy, Chander Sehgal, Mátyás Selmeci, Anthony Tiradani, and John Volmer

Also thanks to Dhiva Muruganantham and Lauren Rotman of ESnet

Conclusion

DOE Grids CA stops issuing new certificates March 23rd, 2013.

(in 10 days)

VOs should already have:

1) Enrolled with new OSG PKI

2) Be ready to handle new user identities

3) Updated documentation and processes

Lessons Learned

Project Phases

- Project was divided into Pilot, Planning, Development, Deployment and Transition Phases
- Allowed for good checkpoints on project
- Perhaps a couple phases too many?
  - Hard to get management engaged to review five times.
- One phase too short at one month

Underestimated VO role in transition

- VO is responsible for both for vetting when users enroll in PKI and consuming certificates when used.
- We should have had focused effort on VO impact and communication of that from the project start.
- In particular, FNAL was central to many VOs.

VO Engagement Critical

- Communication via twiki, weekly calls, email list.
- Worked well with those that engaged.
- Needed more effort to engage with those that didn't engage.
  - Both VOs and other OSG project teams.
  - Not enough budgeted effort to communication.

Collaboration with ESnet was Critical

- Coordinated communications between two organizations.
- Access to historical data about PKI usage.
- Deep insights as to how the PKI was used.

We don't know how OSG uses PKI...

- DOE Grids CA was around for 10+ years with web and HTTP/REST interfaces
- Plethora of usage patterns, client tools
- We still don't know how PKI is used by all parties.

Use of Browser PKI Functionality

- DOE Grids PKI used the browser heavily to generate/renew keys.
- This caused lots of browser version dependencies and issues
- Following CILogon, OSG PKI implemented key generation in OIM. Seems to have worked out well.

Everything is a VO?

- Treating sites (Argonne, ORNL, etc.) as VOs seems to be working well.

- We initially thought of host certificates requests as being an issue of domain (e.g. uiuc.edu) and not VO. This was probably wrong, and these requests should have been VO-centric.

DigiCert (Commercial vendor) Relationship

- Nomenclature was different and took time to work through.
- Policy agreements were time consuming.
- Contract was complicated.
- Should have budgeted more time for all the above.

Separation of Web (HTTPS) and Grid Certificates

- By focusing our relationship with DigiCert on Grid certificates and using a separate CA that doesn't issue certificates trusted by browser, we made life much easier for all.
  - Only have to meet IGTF policies and not CAB Forum policies – much lower bar.

- Downside is OSG PKI certificates are not good web server certificates.

Bulk Request is a very special case

- Bulk request of host certificates is not something PKIs outside of the Grid support.
- Was a source of a lot of interaction issues with DigiCert.
- Lots of tricky details.
- Should have scheduled more time and effort for this specific case.

Audit

- We are now undergoing our first self-audit with DigiCert.
  - This is a normal annual event.
- Audit is based on policy.
- Questions indicate some different interpretations of policy.
  - Will be worked out.
- Having a test audit prior to implementation would have been useful.

If I could budget over…

I would add effort for:

- Use case documentation & requirements
- QA/Testing
- Documentation
- Communication/VO engagement
- Policy/legal/contracts

CLI Client Development

- During development of CLI clients, a release often and early approach would have been nice.
  - Community wants RPMs not head-of-SVN.
- OSG doesn't do software development, they do integration. Have limited release, testing, etc.
- Should have established own SW processes as independent team.
  - And then wound down after transition.

Panda/Gridsite issue

- When ATLAS started testing, discovered show-stopping problem with Panda.
- Turns out Panda is not represented in the OSG test bed (ITB)
- Gridsite (a Panda component) is known to be picky about PKI implementation.
- Should have been hit early and often with new PKI.

Using a Commercial CA

- Use of a commercial CA for a backend is a new model and was somewhat controversial.

- I still have no doubt it was the right choice. OSG deploying and operating a CA with all the IGTF requirements would easily have been more expensive.

Lessons Learned Caveat

It's not over yet, we certainly have more lessons to learn.

OSG PKI Reports

- Pilot Phase
  - https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1097
- Planning Phase
  - https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1120
- Development and Deployment Phases
  - http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1145
- Transition Phase
  - https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1148