OSG PKI Transition

John Hover

US ATLAS T2/3 Workshop

Indianapolis, Indiana

Outline

Rationale and Background

Important Facts and Dates

- March 23: DOEgrids -> OSG CA

Digicert Testing

- OSG Software
- ATLAS Software

Potential Problems/Special Cases

- Non-VOMS services.
- Site admin accounts

Documentation

Questions and Discussion

Rationale

DOEGrids

- Funded and managed by DOE

OSG/Digicert

- OSG CA outsourced to commercial certificate provider Digicert.
- Digicert has established a sub-CA specifically for OSG.
- OSG pays for all service. User and host certs still free.
- Cheaper and (arguably) better service.
- In theory, OSG could move to another CA if there are problems.

CERN Note:

- If you have a CERN computing account, you can get a personal cert there via the SSO system.

Important Facts and Dates

March 23rd: No more DOEgrids certificates being issued.

- Existing certs still good. CRLs still updated. etc. until April 2014.
- HINT: Good idea to renew critical service host certs now.

Digicert user and host certificates available now.

- End users can request certs when DOEgrids cert is expiring.
- Admins should get them ASAP so that they understand any issues.
- OSG client tools have changed. Different web interface. But gridadmin concept stays the same.

User and admin interface via OSG OIM:

- https://oim.grid.iu.edu/oim/certificate
- Cert and gridadmin requests handled as tickets.

Procedure Overview

In general, same procedure as we have now when a user gets a new DN from DOEgrids...

Get new Digicert certificate:

- Go to OIM | Certificate
- Choose ATLAS VO. Sign agreement.
- (Sponsor selection via drop-down coming soon.)

Add it to your existing ATLAS VOMS registration:

- Connect using current DOEgrids cert
- Go to Members | Certificates | Add certificate
- Enter new DN and CA
- Await VO Admin approval. Email if urgent.

Add it to your GUMS administrator group

Add it to your CERN SSO

IMPORTANT: Do such mappings *before* your DOEgrids cert expires.

Digicert Testing

OSG has tested all service packages that it packages/provides:

- OSG CE
- dCache
- Bestman
- GUMS
- etc. etc. ...

Earlier this year we ran the full ATLAS end-to-end using Digicert user cert

- VOMRS/VOMS registration
- proxy generation
- Pilot submission (which entails data stage-out to SE).
- Panda submission

Problems: Found a severe bug in mod_gridsite, now fixed.

- Issue with pathlen: 0 parameter in Digicert CA cert
- Prevented job dispatch from Panda over HTTPS.

Special Cases

Non-VOMS based external services

- GGUS
- CERN SSO: map new DN to existing account.
- OSG web interfaces: OIM, MyOSG, Ticketing
- Cert-secured Twikis
- Cert-secured Subversion repositories
- DQ2/DDM??

Local facility web-based services

- GUMS
- RSV certificates
- others? Monitoring? Ticketing?

Gotchas

Ensure CA distribution up-to-date:

- Shouldn't be an issue on heavily-managed systems
- *yum update osg-ca-certs* for standard systems.

FYI: DOEgrids CA cert is new as of January 23rd.

- Also solvable by *yum update osg-ca-certs*

Documentation

OSG Documentation:

- https://www.opensciencegrid.org/bin/view/Security/PKIDocumentationIndex
- https://www.opensciencegrid.org/bin/view/Security/OSGCATransition2012
- https://twiki.grid.iu.edu/bin/view/Documentation/CertificateGetWeb

OSG FAQ:

- https://www.opensciencegrid.org/bin/view/Security/OSGPKIFrequentlyAskedQuestio

ATLAS administrator documentation

- http://www.usatlas.bnl.gov/twiki/bin/view/Admins/DigiCerts.html

ATLAS end-user documentation

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

Questions? Discussion.

How many of you already have Digicert certs?

How many of you are gridadmins and request host certificates for your site?

How many host certs do you have?