OSG PKI Grid Admin (GA) Training

Mine Altunay, Jim Basney

OSG PKI Team

October 8, 2012

The OSG PKI

- Transition from DOEGrids CA to OSG PKI.
  - Registration Authority Agents (RA Agent)/Grid Admins (GA) will interface directly with OSG and OSG Information Management System (OIM).
  - The back end CA, DigiCert CA, is invisible to RA Agents and GAs for their work.
  - Most of the RA Agent/GA functions remain the same. New user interface at OSG OIM, but basic functionalities are the same
    - Using GOC ticketing system instead of mailing lists
  - Separation of RA Agent and GA duties:
    - RA Agents only approve User certs, does not approve host certs anymore.
    - GAs only approve host certs.

The OSG PKI

- An RA Agent can be assigned to one or more Vos
- A GA can be assigned to one or more network domains (e.g. fnal.gov) and a domain can be approved by one or more GAs
- A person can be an RA Agent and GA simultaneously

Training Goals and Outline

- Perform the GA duties in OSG PKI.
  - Everything we perform in training is in **ITB** instance. No **Production** certs will be issued.
  - Two goals: how to approve host certificate requests via OIM and do bulk requests via the command line.

1. Request to become a GA
2. First, demonstrate the OIM interface
   - Request host certificates for your domain
   - Approve the cert
   - Retrieve the cert
   - Revoke the cert
   - Approve another person’s host cert request as a GA

Training Goals and Outline

3. Demonstrate the command line interface
   - Request and retrieve host certs
   - Approve another sys admin's host cert request (in OIM interface)

- Go over the policies and requirements of the new PKI
- After the training, request to become a GA in the Production system.

Request to Become a GA

- Check if you already done this:
  - Go to https://oim-itb.grid.iu.edu/oim/gridadmin
  - If you do not see your name listed, then you should request to become a GA.
- To request GA privileges: Go to https://oim-itb.grid.iu.edu/oim/gridadmin
- And click on “Request for GridAdmin Enrollment”
- In the form, fill in your name and the domain name(s) as directed, read the form carefully and Submit the request.
- Please tell us what you think about the form.

OIM Interface: Request a Test Service Cert

- Go to Open https://oim-itb.grid.iu.edu/oim/certificaterequesthost.
- Create your certificate request:
  - **umask 077;**
  - **openssl req -new -newkey rsa:2048 -nodes -keyout hostkey.pem -subj "/CN=osg-ce.example.edu"**
  - Replace osg-ce.example.edu with your own domain
- Paste CSR on the web form.
- Check the "I AGREE" box and click Submit.

OIM Interface: Approve the Test Service Cert

- Check your email for a message from OSG containing: "Please determine this request's authenticity, and approve / disapprove at URL
- Open the URL from the email message. (Your browser might already be on the right page.)
- Verify the certificate request is legitimate. Review NewOSGPKI now.
- Enter an "Action Note" ("OSG Grid Admin Training") and click the "Approve" button.

OIM Interface: Retrieve the Test Service Cert

- Check your email for a message from OSG containing: "Your host certificate request has been approved. To retrieve your certificate please visit URL and click on Issue Certificate button."
- Open the URL from the email message. (Your browser might already be on the right page.)
- Click the "Issue Certificate" button.
- Click the "Download PEM" link to download the certificate.

OIM Interface: Revoke the Test Service Cert

- Review circumstances under which Grid Admins should revoke certificates. https://twiki.grid.iu.edu/bin/view/Security/NewOSGPKI
- Open https://oim-itb.grid.iu.edu/oim/certificatesearchhost.
- Click the "Others" tab.
- Enter the hostname in "CN Contains" and click the "Search" button.
- Click on the line for your certificate.
- Enter an "Action Note" ("OSG Grid Admin Training") and click the "Revoke" button.
- For a normal revocation, briefly explain why you need to revoke the cert in the “Action Note” field.

OIM Interface

- Completed the GA functionalities in OIM interface.
- Will move onto the command line interface (cli) for the same functionalities.
- If you do not plan to use CLI, you can skip the rest!

Command Line Interface (CLI): Request and retrieve certs

- Has three scripts:
  - osg-gridadmin-cert-request
  - osg-cert-request
  - osg-cert-retrieve
- osg-gridadmin-cert-request will be most useful for GAs.
  - Request, approve, issue and retrieve multiple host certs for your domains

Command Line Interface (CLI): Installing the scripts

- Need a Linux machine
- osg-pki-tools is currently not compatible with python-json distributed by epel for RHEL5
  - Run **python -c "import json; json.dumps('x')”**
  - If you have the following error:
    AttributeError: 'module' object has no attribute 'dumps’
  - Execute **yum remove python-json**
- yum install --enablerepo=osg-testing osg-pki-tools

Command Line Interface (CLI):osg-gridadmin-cert-request

- osg-gridadmin-cert-request -help to see the options
- Requires your user certificate registered as Grid Admin in OIM. Looks in $HOME/.globus/usercert.pem and $HOME/.globus/userkey.pem by default. Use -c and -k options for alternate user cert/key locations
- Create a hostname file containing Fully Qualified Domain Name (FQDN) for each host certificate
- Create a hostnames file
- **vi hostnames**

```
pepperjack-itb.fnal.gov
cheddar.fnal.gov
gruyere.fnal.gov
```

- 50 cert requests/day at most

Command Line Interface (CLI): Request and retrieve certs

- **osg-gridadmin-cert-request -T -f /root/hostnames**
  - **-T is important.** It signifies a test request; goes to the OIM-ITB. You do not need it once you complete the training and move to production OIM.
  - Will request, approve, issue and retrieve the certs automatically.
  - Patience! May take a few seconds to complete.
- In the same directory, find the certificate and key files. For example, gruyere.fnal.gov.pem and gruyere.fnal.gov-key.pem
- If you have a single certificate to request
- **osg-gridadmin-cert-request –T --hostname=cheddar.fnal.gov**

Command Line Interface (CLI):osg-cert-request

- osg-cert-request --help to see the options
- Will be used by regular users without GA privileges.
- The GA will approve/reject the request
- **osg-cert-request -T --hostname=cheddar.fnal.gov --name="Mine Altunay" --email=maltunay@fnal.gov --phone=6308406490**
  - **Note the -T option.**
- The GAs will receive an email from GOC. "Dear GridAdmin, Host certificate request has been submitted. Please determine this request's authenticity, and approve / disapprove at URL"
  - Click on the ticket URL and update the ticket that you will work on this request
  - Go to https://oim-itb.grid.iu.edu/oim/certificatehost
  - Click on "My Request". Under the Section "Host Certificate Requests that I Approve" find the request, and click on it
  - In "Action Note" field, explain why you grant the request briefly.
  - For training, just type "GA Training"
  - Click Approve
- Your job as a GA is complete!

Command Line Interface (CLI):osg-cert-retrieve

- osg-cert-retrieve -help to see the options
- Will be used by non-GAs, not useful for GAs.
- The user will receive an email from GOC when GA approves the request and will run the osg-cert-retrieve to download the cert
- **osg-cert-retrieve -T -i 1289**
  - -i is the request ID.
  - Included in the ticket email as well.
- Certificate will be written to ./hostcert.pem file automatically unless --certfile option is chosen

After the training

- Note the difference between **OIM-ITB** and **OIM**
- Apply to become an OSG GA. Go to https://oim.grid.iu.edu/oim/gridadmin and click on “Request for GA Enrollment”, and complete the form.

New Distinguished Names: Will NOT Affect the GAs, but affect your VOs

- Certificates from new OSG PKI will have new Distinguished Names
  - Users will need to register new certificate DNs in VOMS
- Current DOEGrids DNs:
  - Issuer: /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1
  - Subject: /DC=org/DC=doegrids/OU=People/CN=*full name DOEGRIDS-ID#*
- New OSG PKI DNs:
  - Issuer: /DC=com/DC=DigiCert-Grid/O=DigiCert Grid/CN=DigiCert Grid CA-1
  - Subject: /DC=com/DC=DigiCert-Grid/O=Open Science Grid/OU=People/CN=*full name OSG-OIM-ID#*
- More details at: https://twiki.grid.iu.edu/bin/view/Security/DOEGrids2DigiCertDNTransition
- Testing so far has found no issues related to this DN change

End of the Training

- You are now Ready to handle production requests
- DOEGrids CA will shut down in mid-March and transition will start slowly after that
  - As users certs expire, they will start using OSG PKI
- Useful URLs:
  - https://twiki.grid.iu.edu/bin/view/Security/OSGPKITraining
  - https://twiki.grid.iu.edu/bin/view/Security/NewOSGPKI
  - https://twiki.grid.iu.edu/bin/view/Operations/OSGPKITrustedAgent