OSG PKI RA Training

Mine Altunay, Jim Basney
OSG PKI Team
October 1, 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.
  - 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

The OSG PKI

- 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
- Quotas for the number of certificates:
- There is no quota for RA agent
- Each user can request up to 25 per year
- For GridAdmin, it's 50 per day, 1000 per year.

Training Goals and Outline

- Perform the RA Agent duties in OSG PKI. You will also act as an non-privileged user briefly.
  - Everything we perform in training is in **ITB** instance. No **Production** certs will be issued.
  - Request to become an RA Agent
  - Request a test cert for yourself, acting as a non-privileged user.
  - Approve the cert as an RA Agent
  - Revoke the cert as an RA Agent.
- Go over the policies and requirements of the new PKI
- After the training, request to become an RA Agent in the Production system.

Request to Become a RA Agent

- Check if you already done this:
  - Go to https://oim-itb.grid.iu.edu/oim/home
  - Under your VOs, you should be listed as an RA Agent
- If you are not an RA Agent yet, request it now
  - Visit https://oim-itb.grid.iu.edu/oim/vo, select your VO, then click the "Request for RA Enrollment" button in the upper right hand corner, and complete the form.
- Read the Agreement before you click yes. Tell us what you think about it. Agreement can be found at https://twiki.grid.iu.edu/bin/view/Operations/OSGPKITrustedAgent

Request a Test User Cert

- Request a user certificate: Go to https://oim-itb.grid.iu.edu/oim/certificaterequestuser.
- You will do this as a normal non-privileged user.
- In the CN field, add “RA Training” next to your name.
- Select your VO.
- Check the "I AGREE" box and click Submit.

Approve the Test User Cert

- You are acting as an RA Agent.
- Check your email for a message from OSG containing: "An OIM Authenticated user ... has requested a user certificate. Please determine this request's authenticity, and approve / disapprove at URL." Look for a email from "FootPrints"
- Open the URL from the email message. (Your browser might already be on the right page.)
- For Training, we will NOT email sponsors, but normally, you will:
- Select a Sponsor who is best suited to perform the identity vetting.
- You can find sponsors at https://oim-itb.grid.iu.edu/oim/vo. Click on your VO and capture the list of Sponsors. All sponsors are cc'ed on the ticket, you should clarify which sponsor is responsible for vetting

Approve the Test User Cert

- When sponsor responds with a signed email about their decision, go to https://oim-itb.grid.iu.edu/oim/certificateuser
- Under "**User Certificate Requests that I Approve"**, click on the request.
- In the Action Note Field, write down the sponsors name and his/her response.
- For training, we do not use the sponsors. Just type "OSG RA Training" in the Action Note Field and click the Approve button.
- No need to send a separate email to GOC ticketing system (or update GOC ticket) or to osg-ra@opensciencegrid.org. Action note will be added to the corresponding GOC ticket automatically.
- Email osg-ra email list if you have questions & need help.

Retrieve the Test Cert

- Back to being a regular non-privileged user.
- Check your email for a message from OSG containing: "To retrieve your certificate please visit the URL”
- Open the URL from the email message. (Your browser might already be on the right page.)
- Enter a 12 character or longer password / pass phrase.
- Click the "Issue Certificate" button.
- Click the "Download Certificate & Private Key" button.

Revoke the Test Cert

- Revoke the cert with your RA Agent privileges.
- Review circumstances under which RA Agents should revoke certificates. https://twiki.grid.iu.edu/bin/view/Security/NewOSGPKI
- Open https://oim-itb.grid.iu.edu/oim/certificatesearchuser.
- Click the "Others" tab.
- Enter your name in "DN Contains" and click the "Search" button.
- Click on the line for your certificate.
- Enter an "Action Note" ("OSG RA Training") and click the "Revoke" button.
- Do not forget to remove the test certificate from your browser. It is only good for testing environment

After the training: Request a User cert in Production System

- Obtain a real user certificate from https://oim.grid.iu.edu/oim/certificaterequestuser.
- Note the difference between **OIM-ITB** and **OIM**
- Apply to become an OSG RA Agent. Go to https://oim.grid.iu.edu/oim/vo Select your VO and then click “Request for RA Enrollment" button in the upper right hand corner, and complete the form.

New Distinguished Names: Will NOT Affect the RAs, 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