OSG PKI Transition

Update

OSG All Hands Meeting

March 19, 2012

Von Welch

vwelch@indiana.edu

Open Science Grid

Background

- OSG has since its inception has operated a public key infrastructure to provide certificates to users, hosts, and services

- Key to this a public key infrastructure provided by ESnet: the DOE Grids PKI

  https://pki1.doegrids.org/ca/

Open Science Grid

Background

- In 2011, the decision was made to transition the CA from ESnet to OSG

  http://www.es.net/services/doe-grids-service-transition/

  https://twiki.grid.iu.edu/bin/view/Security/OSGCATransition2012

- Since then, OSG and ESnet have been working together to transition responsibility for the CA to OSG

Open Science Grid

Goals of Transition

- Provide all functionality of DOE Grids PKI
- Serve all of OSG U.S. user community
- High-quality, usable service
- Smooth transition

Open Science Grid

Chosen path

- DigiCert is a commercial PKI company based in Utah
  - IGTF-accredited, so provide interoperability with other Grids
- OSG will contract with DigiCert for back-end CA
- OSG will establish own “front end” web service

Open Science Grid

What does this mean to me?

- RA Agents, Grid-admins: there will be replacement agreements similar to DOE Grids PKI agreements

- Grid-admins: New bulk host certificate request script, using new API, will be provided.

What does this mean to me? (2)

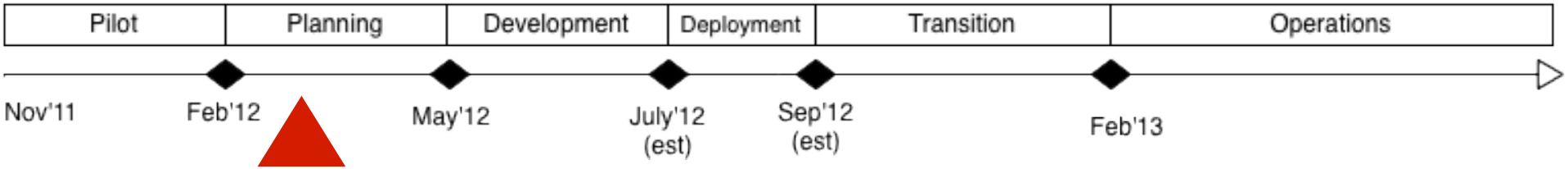
- Getting certificates will be similar workflows.

- Users will need to be re-vetted for their first certificate from new OSG PKI
  - No automated re-issuance (first time).
  - Will cause higher load for RA Agents

What does this mean to me? (3)

- Users will need to register new DNs in VOMS
  - Documentation coming…
- Will I have to pay for certificates?
  - No, OSG will contract for enough certificates to meet needs of users.

Where we are…



- Planning phase until May'12

  https://twiki.grid.iu.edu/bin/view/Operations/DigiCertPlanningDevAndImplementation

Open Science Grid

Next Steps

- Development (~May'12)
  - Create front-end, connect to DigiCert
  - Processes, backups, contingency plans, etc.
- Deployment (~July'12)
  - Stand up PKI, testing, acceptance

Open Science Grid

Next Steps (2)

- Transition (~Sep'12)
  - Users start seeing changes
  - Will start directing subset of community to new OSG PKI.
    - Start with OSG staff, most tolerant users.
- Operations (~Feb'13)
  - OSG PKI fully operational, all users using it
  - DOE Grids PKI stops issuing certificates
    - Continues to issue CRLs for ~one year.

For more information

- Public web page:

  https://twiki.grid.iu.edu/bin/view/Security/OSGCATransition2012

- Planning page (details):

  https://twiki.grid.iu.edu/bin/view/Operations/DigiCertPlanningDevAndImplementation

- Planning email list (weekly emails):

  OSG-PKI-TRANSITION@OPENSCIENCEGRID.ORG

  - To subscribe, send email to listserv@fnal.gov with contents:

    SUBSCRIBE OSG-PKI-TRANSITION@opensciencegrid.org FIRSTNAME LASTNAME

Open Science Grid

Conclusion

- In summary:
  - OSG will establish own PKI by early 2013
  - Transition will begin in September'12, moving users over slowly by Feb'13.
  - Will be extra work during transition (e.g., registering new DNs), but general process won't change substantially.

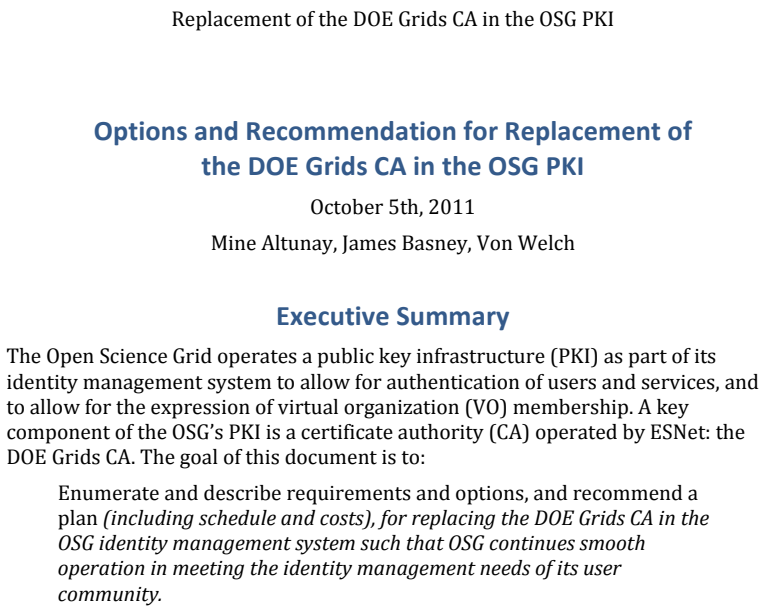
- Questions, comments, etc. to:

Von Welch (vwelch@indiana.edu)

Old, detailed slides

OSG Analysis of Options

- OSG analyzed their options for a new CA
- Document OSG requirements
- Examined 14 options
- Published Nov'2011
  OSG Doc 1077-v2



Replacement of the DOE Grids CA in the OSG PKI

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.*

http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=1077

Open Science Grid

Outcome of Analysis

- No combination of existing CAs meets OSG needs in the near future
  - ~1-2 years
- OSG needs its own CA

Open Science Grid

Traditional Route for own CA

- Purchase and configure secure hardware
- Write or integrate software
- Obtain IGTF accreditation for interoperability

- Summary: Lot of specialized work

Alternate Route for Own CA

- DigiCert is a commercial PKI company based in Utah
- Independent of OSG, they were deploying an IGTF-accredited CA
- OSG could contract with DigiCert for CA services
- OSG could establish own “front end” web service

Open Science Grid

Why DigiCert?

- DigiCert takes on difficult, specialized tasks of operating CA
- IGTF accreditation gives OSG interoperability with LHC and other international collaborators.

Concerns with commercial CA approach…

- How would OSG's VO structure map well onto a typical customer?
- Would DigiCert's policies work for OSG?
- If OSG wanted to run its own front-end, would DigiCert's API's suffice.

Pilot Phase

- Decision was to run a 3-month pilot to evaluate DigiCert services in the context of OSG needs.
- Pilot ran from Nov'11 to Feb'12
- Short version: Everything OK.
- Pilot report (draft):

https://twiki.grid.iu.edu/twiki/pub/Operations/DigiCertPlanningDevAndImplementation/OSG_Pilot_Report_11.pdf