Identity Management in Open Science Grid
Challenges, Needs, and Future Directions

Mine Altunay*, James Basney**, Von Welch*
*Fermilab, **NCSA, *Univ. Of Indiana

Presented by Keith Chadwick*
*Fermilab
Identity Management in OSG

- All services use X509 PKI certificates for identity and trust.
- OSG participates in the U.S. TAGPMA and International Grid Trust Federation (IGTF) as a Relying Party.
- OSG accepts IGTF accredited Certificate Authorities (CAs) and two TeraGrid CAs
- OSG has a long history of dependence on and collaboration with the ESnet DOEGrids CA for issuing personal and service (host) certificates
- OSG Runs a Registration Authority for handling requests for certificates issued by DOEGrids.
- In 2011 OSG became a member of InCommon and started looking into supporting Shibboleth/SAML based identities for the future.
## DOE Grids Certificates Issued/Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Cert type</th>
<th>2009</th>
<th>2010</th>
<th>2011*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>User</td>
<td>Host/Service</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>HEP</td>
<td>785</td>
<td>6790</td>
<td>7575</td>
</tr>
<tr>
<td></td>
<td>NP</td>
<td>26</td>
<td>67</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>Other DOE</td>
<td>185</td>
<td>469</td>
<td>654</td>
</tr>
<tr>
<td></td>
<td>NSF (non-LHC)</td>
<td>184</td>
<td>298</td>
<td>482</td>
</tr>
<tr>
<td></td>
<td>other</td>
<td>121</td>
<td>308</td>
<td>429</td>
</tr>
</tbody>
</table>

*Data collected as of June 8, 2011*
OSG Trust Model: Current Identity Vetting Workflow

- OSG has no central user database
- Distributed certificate management
2011-2012: Transition of Esnet DOEGrids CA services to OSG

• In 2011, ESNet announced that it will transition services offered by DOEGrids to the OSG to operate.

• OSG started an 18 month project to plan and implement this transition.
  – Led by Von Welch from Univ. of Indiana, Jim Basney from NCSA, and Mine Altunay from Fermilab
OSG ID Requirements

• We developed, and will talk about, a “Replacement” document [1]:
  • Requirements
  • Evaluated Options
  • Decision
  • Current Status

• Requirements:
  • Must work with OSG software; Sustainable within OSG efforts
  • LHC interoperability/IGTF Accreditation
  • Certificates for 3000+ users across the USA, vetted by 36 Registration Authorities agents.
  • Certificates for 300+ gatekeepers plus 8000+ worker nodes at 80+ OSG sites
  • Implement an evolving infrastructure that can incorporate new ID mgmt technologies.

Options Considered:

<table>
<thead>
<tr>
<th>CA</th>
<th>CA Description</th>
<th>IGTF Accredited</th>
<th>Host Certs</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCSA CILogon Basic</td>
<td>User certificates based on authentication of users via the InCommon identity federation.</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>NCSA CILogon Silver</td>
<td>User certificates based on authentication of users via the InCommon identity federation.</td>
<td>Yes</td>
<td></td>
<td>No Silver-level Incommon IdPs</td>
</tr>
<tr>
<td>InCommon CA</td>
<td>Provides user and host certificates to InCommon subscribers.</td>
<td>No</td>
<td></td>
<td>Only 52 of 92 OSG institutions members.</td>
</tr>
<tr>
<td>NCSA CA, XSEDE CA, Globus Online CA</td>
<td></td>
<td></td>
<td></td>
<td>Too many unknowns about the future plans.</td>
</tr>
<tr>
<td>CERN CA</td>
<td>Provides user certificates to LHC members.</td>
<td>Yes</td>
<td>Only for CERN hosts</td>
<td>Only LHC.</td>
</tr>
<tr>
<td>Fermilab Kerberos CA</td>
<td>Serves users registered at Fermilab</td>
<td>Yes</td>
<td>No</td>
<td>Only Fermilab users.</td>
</tr>
</tbody>
</table>
Other Options Considered

• Build an OSG CA:
  - Would be a new CA deployed funded and staffed by OSG and under OSG control.
  - Viable, but costly. Specialized hardware and skills to operate (HSM), no economy of scale

• Migrating existing DOEGrids CA h/w and s/w to OSG control
  - DOEGrids CA software is End of Life and costly to maintain.
  - Upgrading to new CA software has more unknowns.
  - Determined to be more risky than building from scratch.

• Outsource to Commercial CA
The Pilot Project

- For the past 3 months we have been doing a pilot using the DigiCert commercial CA and investigating how to build an OSG registration front end:
- New venture for us; a commercial/research collaboration
- Activities in the pilot:
  - Tested against VDT; Tested user interface and programmable (Rest) API for OSG workflows and use cases.
  - Risk assessment and contingency planning started
  - No major problems identified.
  - Currently moving towards a decision in conjunction with DOE and OSG management based on the results.
Next Steps

Implement OSG CA services in production:

- Feb-Mar: Develop the plan and timeline
- Apr-Oct: Develop software, integrate and train RAs and users
- Oct-Dec: Deploy services and transition users.

Services included:
- Front end services (registration and logging).
- Digicert will provide back end CA services
- Maintain local database of requests in case back end is unavailable for a length of time.
- Plan implementation of contingencies.
2013 and beyond

Once we have OSG based CA services in production we will consider what new technologies and methods for federated identity can be integrated to ease the users burden of multiple identities across web, grid and local campus interfaces and services.

We are participating in the Federated Identity workshops in Europe and elsewhere.
2013 and Beyond

• Goal is to
  - Make certificates transparent to the users
  - Use campus IDs wherever possible; sites that accept Campus IDs
  - Use CILogon or likes to convert Campus IDs into certificates to submit grid jobs
  - Heterogeneous environment
    - Some sites want IGTF-accredited certificates
    - Some sites will not – use Campus IDs