Evolution of the Open Science Grid Authentication Model

Kevin Hill
Fermilab
OSG Security Team

Highlights

- Introduction
- OSG PKI transition to OSG CA
- SHA2
- CILogon CA certificates
- Certificate-Free Job Submissions
- Future Goals

Introduction

- OSG Security Team
  - Mine Altunay – OSG Security Officer
  - Kevin Hill
  - Anand Padmanabhan
- The Open Science Grid is funded by National Science Foundation and Department of Energy

Open Science Grid

OSG PKI Transition

- OSG historically has used x509 certificates (proxies) for authentication.
- The security team is responsible for the OSG root CA bundles.
  - IGTF bundle + a few additions.
- DOEGrids CA shut down, and OSG started its own CA.

PKI Transition – DOEGrids CA

- DOEGrids CA stopped issuing new certs March 2013. All existing DOEGrids certs will expire early 2014.
- When announced (well ahead of time) OSG started planning to create its own CA.
- Some concerns:
  - DOEGrids CA had its own web site for user cert requests, as well as command line tools for getting certificates.
  - DOEGrids CA had its own concept of Sites and Virtual Organizations.
  - Served wider audience than OSG.
  - Slightly different mapping of virtual organizations.

OSG CA

- OSG now has its own certificate portal with DigiCert CA signing certificates in the background.
- Digicert created a separate OSG Grid root CA.
- New web interface and command line tools.
- Web interface part of existing OIM system.
- Integrated with OSG GOC ticket system.
- Some growing pains with getting old DOEGrids Virtual Organizations mapped to OSG Vos.

Certificate Approval Process

- Certificate is requested.
  - Requester specifies a VO, as well as a sponsor.
- The sponsor verifies the requester comes from a real person.
- The RA approves the certificate based on sponsor's ok.
- Certificate is signed and downloaded by the requestor.

Open Science Grid

SHA2 Transition

- SHA1 certificates are nearing the point where processing power to generate collisions won't be unreachable
- Current recommendation is to start issuing SHA2 certs December 1st. OSG will recommend January 15th, to avoid changes during the holidays.
- All OSG provided software is working with SHA2.
- Other software may still need testing.

CILogon Basic Certificates

- Alternative source of x509 certificates for users.
- Uses federated authentication to issue certificates authorized by requesters' home institution, acting as a Identity Provider (IdP) .
- CILogon Basic CA certs not IGTF approved currently. Unfortunately includes most sites.
- CILogon Silver CA currently in IGTF Root CA bundle.

CILogon Basic CA Advantages

- Quick for users to get certificates
- Replaces the RA->Sponsor manual verification step in the OSG CA workflow a federated authentication check via InCommon federation.

Future CILogon Basic usage

- Currently looking for more sites to accept certs, so more users can use them.
- Not currently issuing service certs.
- Some sites have issue with certain IdPs, which effectively lets everyone with a valid email account sign up.
  - Can be limited via modified signing_policy file.
  - Care needed in case of updates to cilogon ca cert package.
- Really not that different than regional CA or large university.
- VO registration is an added authentication step.

Certificate-free Job Submission

- Certificate management can be a headache, especially for new users who may not need individual certificates for any other use.
- Manual approval process in the case of traditional CAs could result in delays of several days in issuing certificates.
- Glidein WMS allows users to submit jobs with local account on a submission system, without their own certificate.

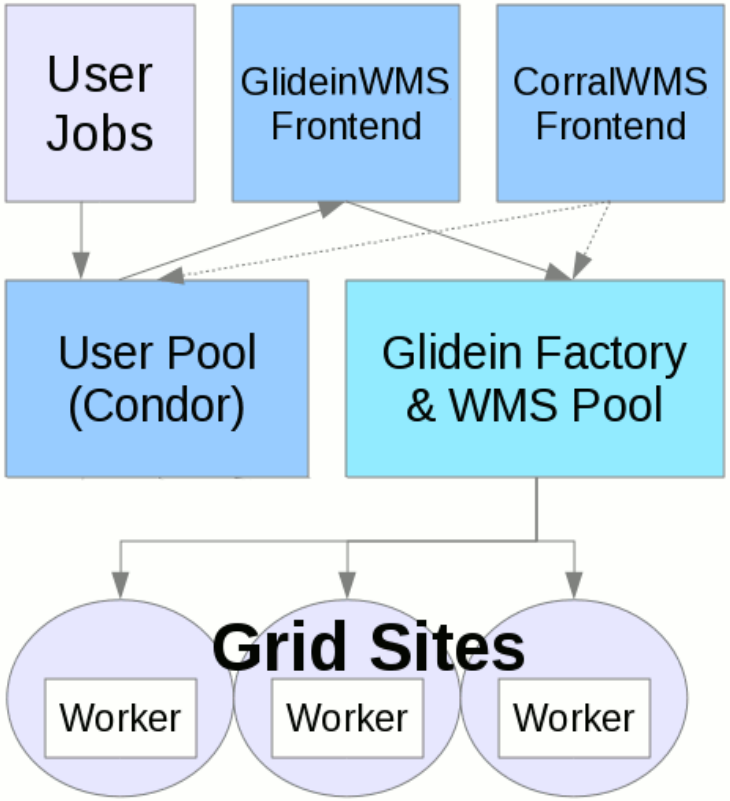
Certificate-Free Job Submission

- Why do we use certificates?
  - Identify users running jobs (traceability)
    - Identify who is running a particular job.
    - Identify where a particular user has jobs running.
  - Control access
    - Block a compromised account from running new jobs.
  - Block unwanted access
    - Limit access to jobs from certain VOs, or other criteria.

Certificate-Free Job Submission

- Can we do these functions without certificates?
- Yes, if we move job submission from end user systems to VO managed portals.
- Only reliable if user management policies of submission portal is trusted.
- Certificates allow jobs to be submitted from any computer with appropriate tools installed.
- Account management needs to be trusted.

Glidein WMS Overview



* Blatantly stolen from http://www.uscms.org/SoftwareComputing/Grid/WMS/glideinWMS/doc.prd/index.html

Certificate-Free Job Submission Project

- Evaluate if traceability is possible, to determine individual running job submitted via Glidein without end user x509 cert.
- Requires coordination of admins at worker node, factory and frontend systems.
- All information was preserved in logs. Not a single stop for the information needed.

Traceability concerns

- VOs can have multiple independent submission systems.
- Access control limited to blocking dn of the VO submission system instead of individual dn.
- Flocking produces additional complications.
- Should all VOs be trusted?
- If not, what changes should we make?

OSG Connect

- OSG Connect project provides a web portal for users to sign up and submit jobs
- Uses CILogon/InCommon federated authentication so there is only minimal delays in creating accounts for users of existing experiments
- Uses Globus Online to transfer data via web browser
- Submitted jobs are flocked to existing OSG VOs frontend

Future Plans

- Continue with Digicert CA signed certificates for the time being.
- Recommend CILogon CA signed certs for InCommon member sites.
- Pursue federated login support via InCommon federation (CILogon).
- Eliminate end user certificate requirements for normal usage from known submission nodes.
- Move job submission from end user systems to VO managed portals.

Links

- https://twiki.grid.iu.edu/bin/view/Security/
  - OSG Security Page
- http://cilogon.org/osg
- http://incommon.org/
- http://osgconnect.net/
- http://home.fnal.gov/~kevinh/
- https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1149
  - Traceability Requirements for end user jobs without certificates
- https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=1175
  - An Assessment of User Job Traceability in GlideinWMS framework

Questions?

- Hopefully everyone is still awake…