OSG Security: Identity Management

Anand Padmanabhan
Mine Altunay
Kevin Hill

OSG Security Team

Open Science Grid

Agenda

- Quick Security team overview
- Certificate changes
- Traceability project
- Future directions for Identity Management

Our Mission

- Protecting OSG users and resources from security breaches
- Preventing loss of effort and resources due to security problems
- Making OSG resources easily accessible to users without compromising their security
- Being a security hub; disseminate security knowledge, best practices, and education

Team Members

Staff	Institution	Effort FTE
Anand Padmanabhan	NCSA	0.5
Kevin Hill	Fermilab	0.8
Igor Sfiligoi	UCSD	0.1
Mine Altunay	Fermilab	0.7
Total		**2.1**

Identity Management

- Transition of Certificate Service from DOEGrids CA to OSG CA.
  - Now complete! Last certificates expired.
  - 5855 Host certificates
  - 1596 User certificates
  - OSG-Wide effort, drawn from operations, software, security teams, and more.
  - Big success!
  - OSG CA is in operation for almost a year now.

SHA-2 Transition

- SHA-1 certificates are nearing the point where processing power to generate collisions won't be unreachable
- SHA-2 certs now being issued by default
- Only a few issues.
- Digicert will be switching to a SHA-2 signed signing cert shortly.

Impact

- The biggest benefit of transitioning to OSG CA:

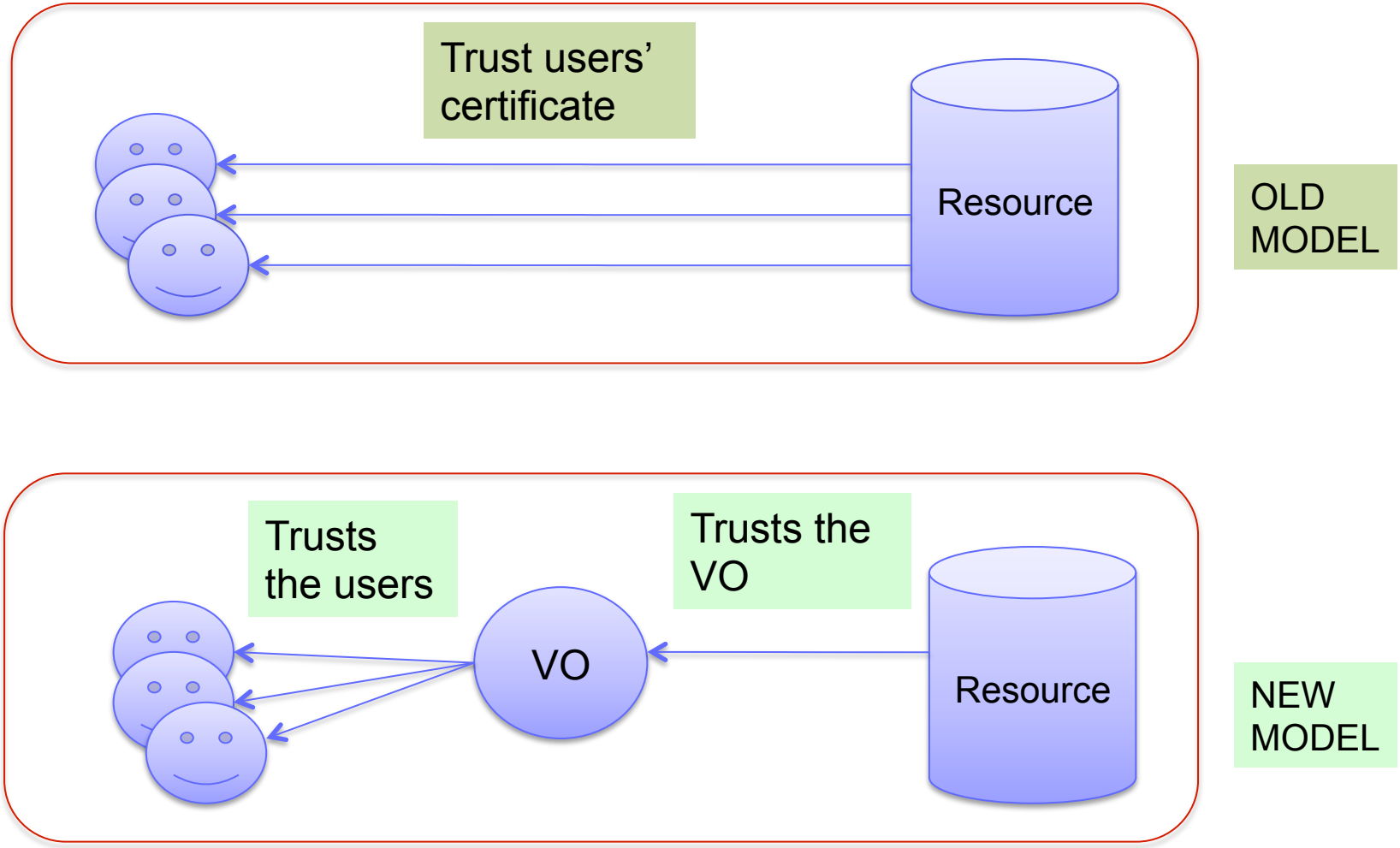
A thorough analysis of OSG infrastructure's access control needs and options.

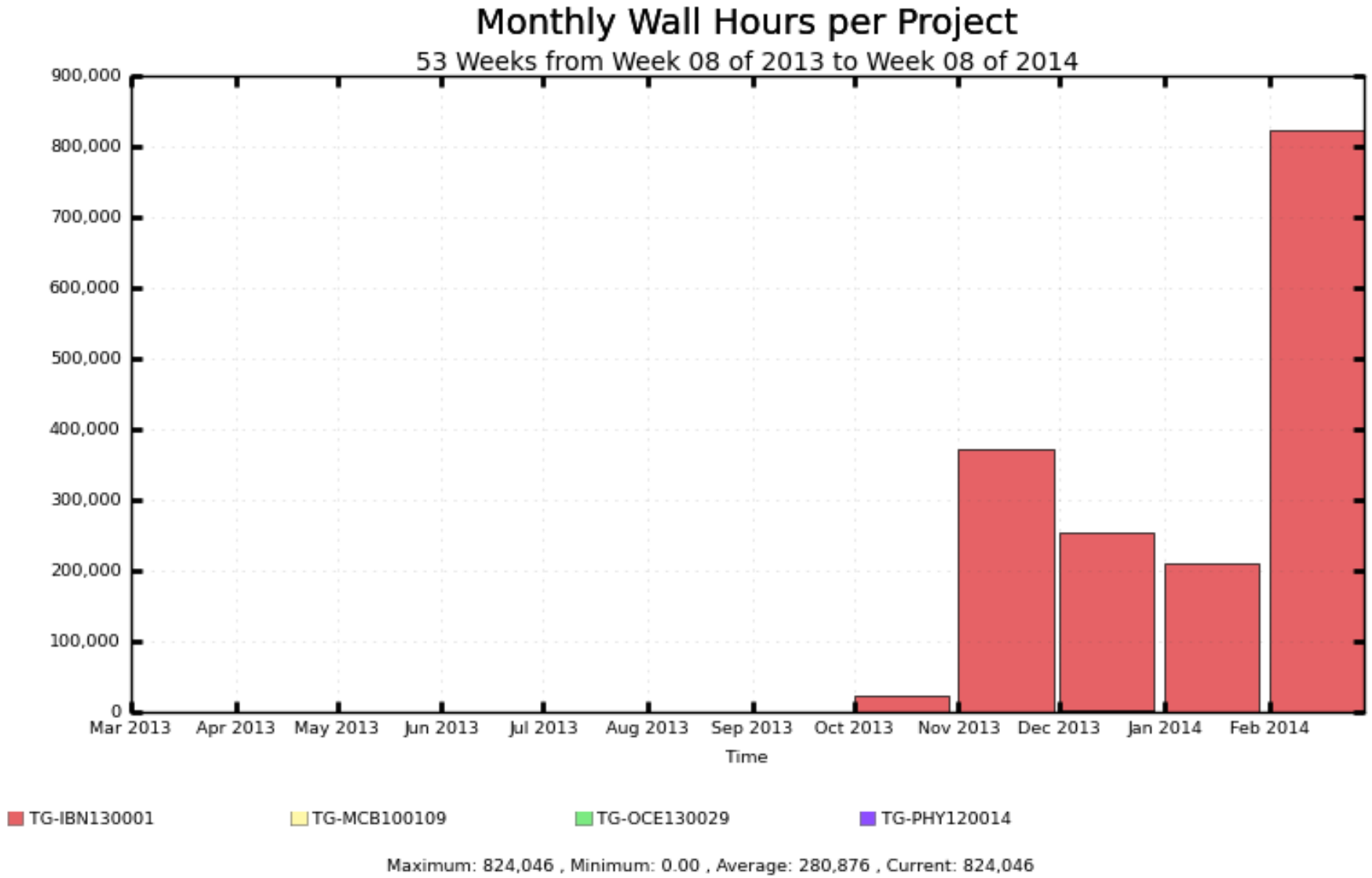
  - Why do we need this many certificates?
  - Can we use a different, more user-friendly technology instead of certificates?
- Started two key projects:
  - Traceability of user jobs
  - Federated Identities

Traceability

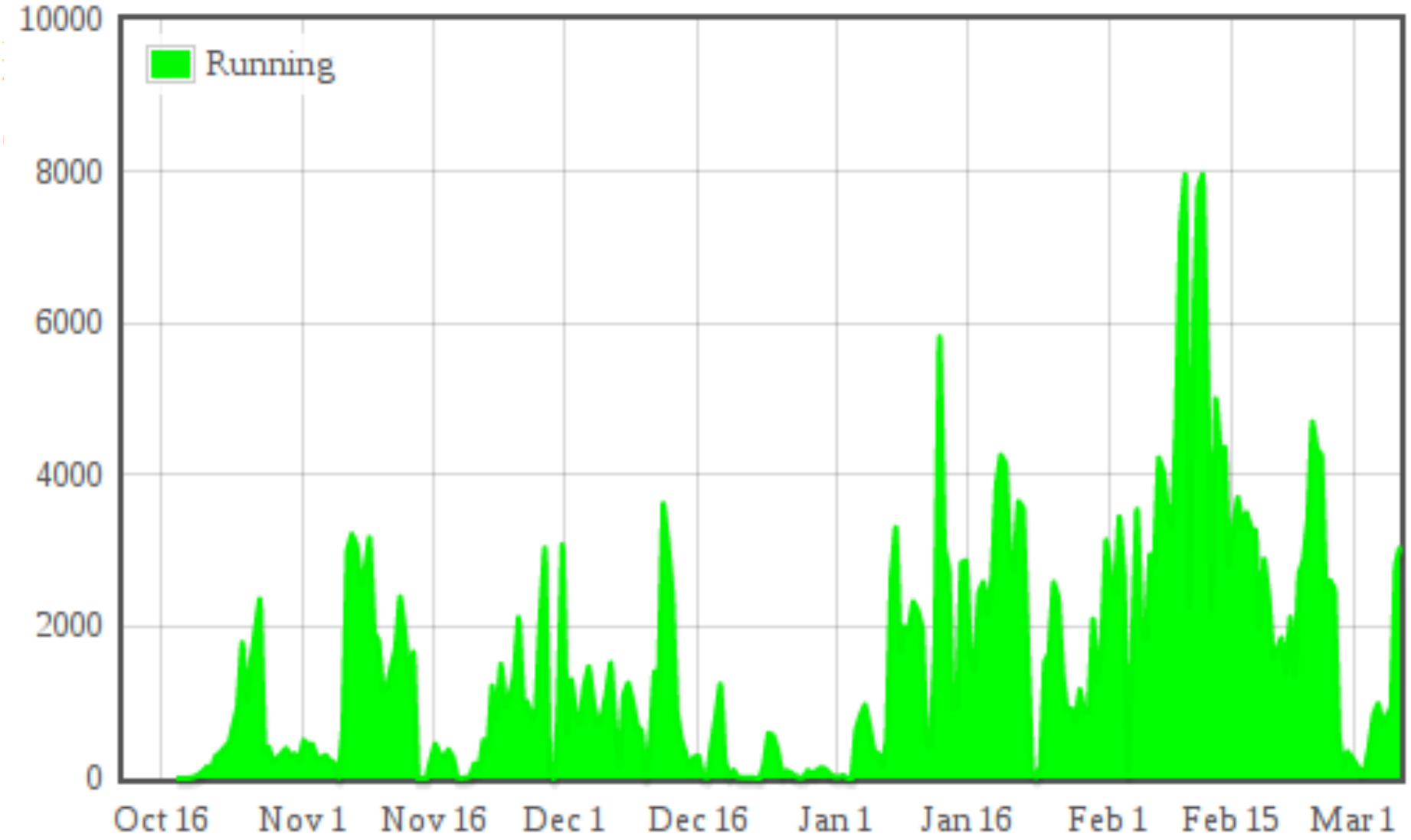
- Goal is eliminating certificates for end users
  - Traceability = associating users with their jobs
  - Who owns this job? Can we answer this question without certificates?
  - Proved that GlideinWMS system can trace user jobs even without certificates.
  - OSG-XSEDE VO and GLOW VO are the first beneficiaries. Evaluated their user management practices and job submission systems

Traceability Project: Changing Trust Relationships





Traceability project took effect in October for OSG-XSEDE
Sharp increase in computing usage after October 2013.



- Number of jobs from OSG VO including XSEDE project.
- Spike in # of jobs after Traceability project took effect.

Traceability Project

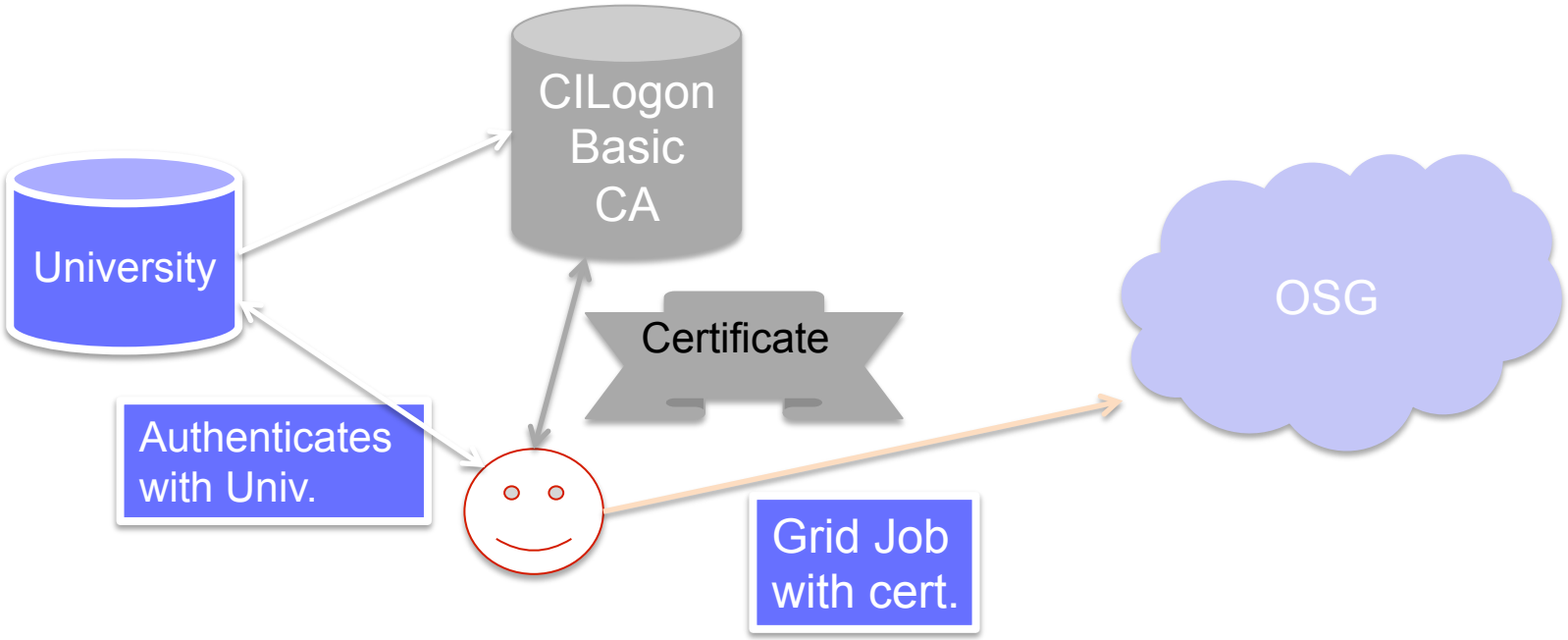
- GLOW VO will start submitting jobs without certificates to OSG, too.
- 607 users will start getting access to resources they could not get to before.
- Significant increase in computing availability.

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.

Federated Identities

- Federated Identities for access
  - For those users, who still need certificates
  - Providing certificates via their home organization
  - No need to get vetted by OSG to get a cert, users utilize their university accounts



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.
- 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.

Federated Identities

- CILogon Basic CA is accepted at 6 OSG sites, Fermilab, Nebraska, UCSD and more, representing 40% of total wall clock hours available in OSG.
- Goal is to reach out to more sites.
- The challenges are that
  - CILogon Basic CA is not an accredited CA (yet)
  - It has a slightly different risk model
- So, sites are slower to adopt this CA and the federated identities represented by that.
- Helping sites by explaining the new risk model behind CILogon Basic CA.

Next Challenge: Storage

- Can we provide access to storage without certificates?
- We've gotten requests to provide individual user access to storage, vs. group accounts normally used for job execution
- Will need some sort of session token for authentication/authorization
- Perhaps we can hide certs/proxies in the background?

Storage

- Possible solution – hide certificates
  - Upon login to submission system, generate short term cert or proxy to be used with job submission as part of login process
  - DN for cert will be in VOMS, no need for user to register, or otherwise handle it.
  - Storage systems can map DN to individual user, as now.
  - Jobs can run Glexec, giving even more traceability.

Challenges/ What Lies Ahead

- Goal is to shield users from certificates and offer more user friendly access control technologies.
- Certificate-free jobs was a big success, we want to repeat it for accessing storage
- Get more VOs to submit jobs without certificates
- Campus grid and federated identities. Utilize campus identities seamlessly in OSG.
- Further reducing the number of host certificates. Optimizations on osg software stack.
  - Can we completely get rid of them?

Questions?