Open Science Grid

OSG PKI Transition

Experiences and Lessons Learned

Von Welch, Mine Altunay, Jim Basney, Alain Deximo, Soichi Hayashi, Viplav D. Khadke, Rohan Mathure, Robert Quick, Chander Sehgal, Anthony Tiradani

International Symposium on Grids and Clouds 2014
25 March 2014, Academia Sinica, Taipei, Taiwan

Background

OSG has used an identity management system for the past 10 years based on a public key infrastructure (PKI).

Allows authentication of users and services.

ESnet provided the core (certificate authority) of this system until 2013. This presentation about OSG's transition to a new PKI system and the lessons learned.

Transition Overview

Transition took approximately 16 months.

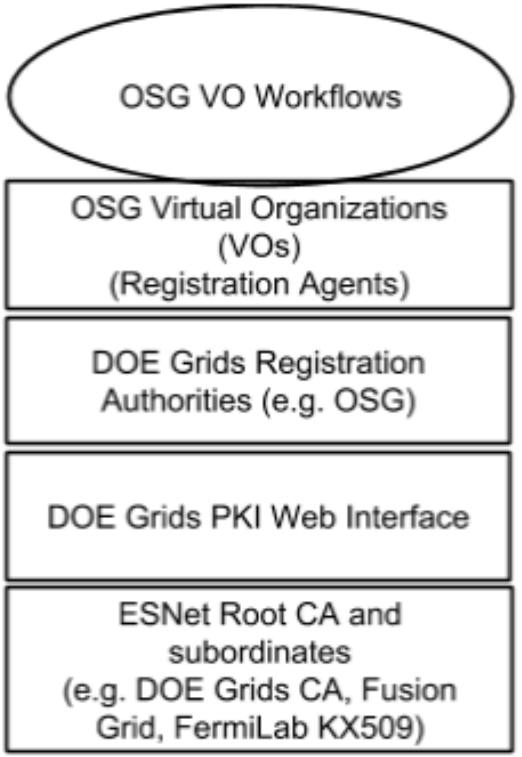
Without service interruption to OSG's 50+ virtual organizations relying on the PKI.

Approximately 2 FTE*years of effort in OSG itself, plus significant effort in virtual organizations and ESNet.

DOE Grids PKI

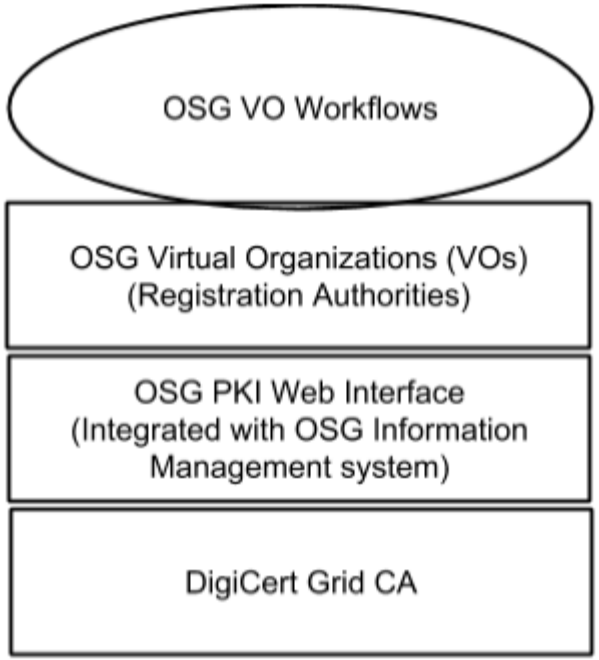
Handled over 2k user and 9k host certificates for OSG.

Served OSG and larger DOE community (Argonne, NFC, ESGF, etc.)



New OSG PKI

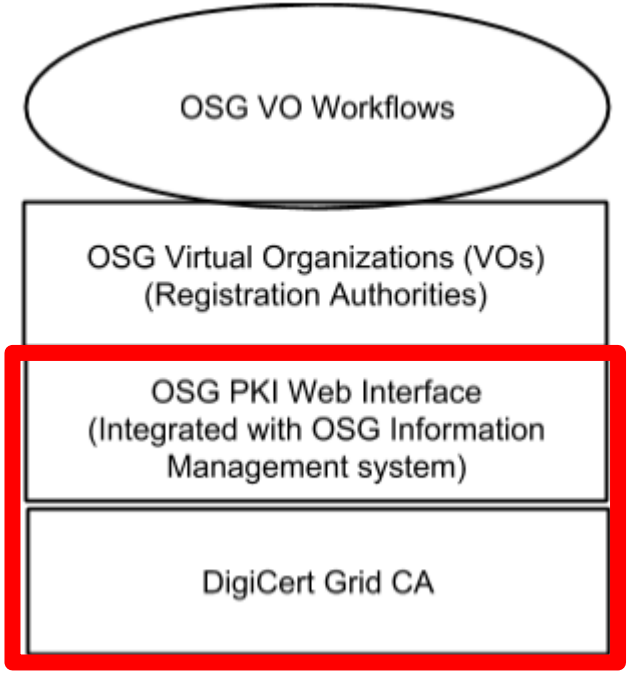
Same basic structure as DOE Grids PKI.



New OSG PKI (2)

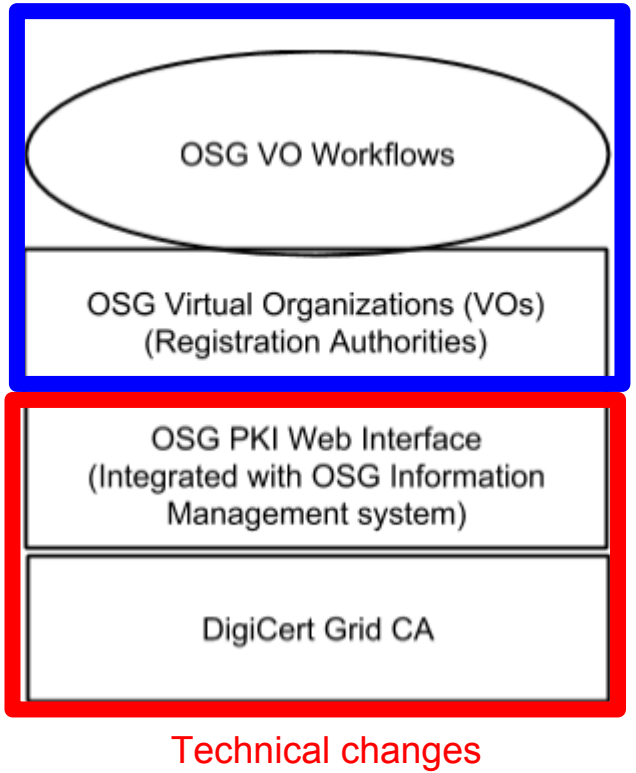
OSG Project implemented Web Interface to DigiCert CA.

OSG interfaces holds all metadata, designed to work with other CAs and IdM systems in the future.



New OSG PKI (3)

Significant work had to be undertaken by the OSG community in changing configuration and learning new workflows.



Lessons learned...

Applicability of Lessons

While this particular transition was from one PKI to another, most lessons are generally applicable for any transition of an identity management system.

Or good advice to anyone developing an identity management systems.

Support multiple User Identities

It is extremely useful for services to allow users to have multiple identities treated as equivalent.

Saves having a “flag day” in transition when user changes identity and service configuration must change at the same time.

Understand Use Cases, Test Early and Often

Identity management systems exist to support workflows.

Knowing workflows critical to testing a new identity system.

This is hard - flexible identity management systems lead to lots of innovative usages.

- Especially in decentralized grids.

Community Effort and Coordination

Changes to the identity system are only part of transition.

Configuration and procedure changes in supported community just as important.

And perhaps more effort.

Key to determine needed community changes early, communicate early and often, and provide help and guidance.

Especially important to involve them in testing of new system.

Bulk Certificate Request is Challenge

Common use case is certificates for clusters - 100's of certificates.

Use case involves obtaining these certificates in bulk instead of individually.

This case is unique to Grids. Not supported by commercial CAs.

Also has many challenge corner cases.

Avoid PKI Browser Functionality

Web browsers have functionality built in for PKI.

Was used in DOE Grids PKI, avoided in OSG PKI to good effect.

Double-edge sword, use of functionality limits workflows.

Dealing with different browser quirks also very challenging.

In the OSG, everything is a VO

Initially we treated users a part of VOs and hosts as part of domains.

Assumption was each domain would be administered centrally at domain.

Turns out in OSG each domain is managed by one or VOs.

Separation of Web and Grid

Initially we explored contracting for both Grid and secure web (http) certificates.

Web certificates are governed by CAB forum.

CAB forum requirement are much stricter.

Separating these concerned allowed for more usable Grid certificates processes.

Use of Commercial CA is viable

Use of DigiCert as commercial CA has worked well operationally.

Differences in nomenclature were a challenge in set up.

Contracting process complicated by OSG not being legal entity and its distributed management structure.

Did undertake a contingency plan.

Thank yous

We thank the Department of Energy, the ATLAS and CMS projects, Indiana University Center for Applied Cybersecurity Research and ESnet for supporting this work.

We thank Tim Cartwright, Jeremy Fischer, John Hover, Christiane A. Ludescher-Furth, Dhiva Muruganantham, Ruth Pordes, Alain Roy, Lauren Rotman, Mátyás Selmeci, and John Volmer for contributions to this work.

We also thank all the OSG virtual organizations who worked to make the transition a success for their user communities.