Open Science Grid

OSG CA Transition:

Issues, challenges and lessons learned

Jeny Teheran

OSG Security Team

OSG AHM 2016

March 15th, 2016

Preliminaries

- OSG has collaborated with various Certificate Authority (CA) operators such as DOEGrids CA and DigiCert CA.
  - Over the course of 2012-2013, OSG transitioned from DOEGrids CA to DigiCert CA.
  - DigiCert CA has been providing the certificate signing service since then.
- OSG's contract with DigiCert CA expires mid 2016.

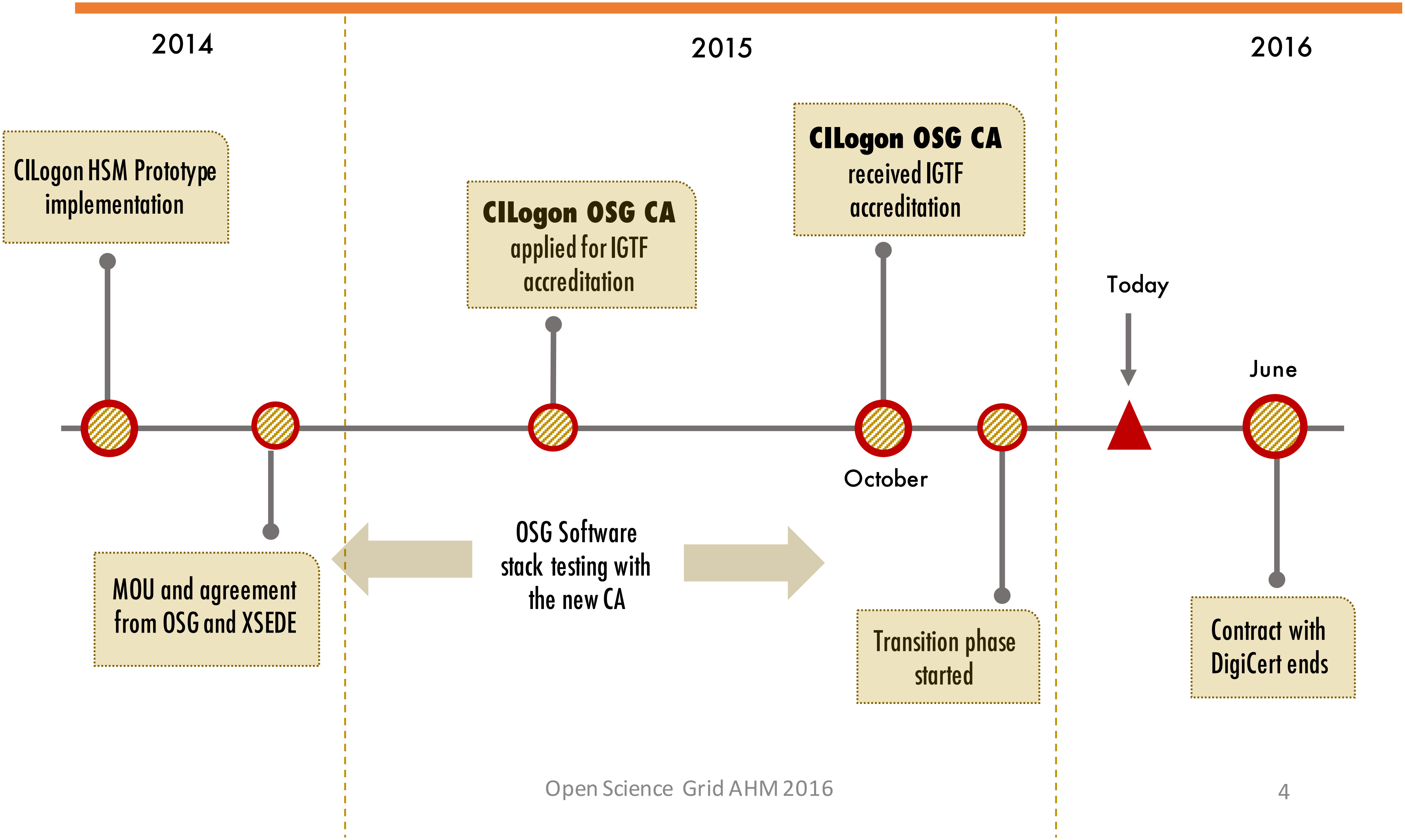
Open Science Grid

CILogon Hardware Security Module

- OSG OIM interface was integrated with CILogon Hardware Security Module (CILogon HSM) resulting in the new CILogon OSG CA.
- CILogon OSG CA is operated by XSEDE in collaboration with OSG.

Open Science Grid

Timeline



2014

2015

2016

CILogon HSM Prototype implementation

MOU and agreement from OSG and XSEDE

CILogon OSG CA applied for IGTF accreditation

OSG Software stack testing with the new CA

CILogon OSG CA received IGTF accreditation

October

Transition phase started

Today

June

Contract with DigiCert ends

Open Science Grid

CILogon OSG CA

- During the testing phase, OSG Software stack was thoroughly tested using the new CA.
- Some Virtual Organizations (VOs) actively participated in the testing phase.
- CMS and Atlas started to test their software stack in November 2015.
  - CMS and Atlas are only allowed to use IGTF-accredited certificates in their infrastructure.

Open Science Grid

CILogon OSG CA

- A new capability of transitioning every VO individually to the new CA was implemented.
- Certificate Distinguished Name (DN) namespace was modified:

```
"/DC=com/DC=DigiCert-Grid/O=Open Science
Grid/OU=People/CN=Jeny Teheran 3194”

"/DC=org/DC=opensciencegrid/O=Open Science
Grid/OU=People/CN=Jeny Teheran 3194"
```

Open Science Grid

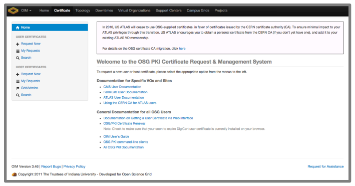
Transition Project

- The transition project started in December 2015 by moving a set of VOs every month to CILogon OSG CA:
  - VO Managers were contacted 4-5 months in advance to agree on the schedule.
  - 10-15 VOs each month.
  - VOs grouped according to the amount of certificates issued to the VO members and the complexity of each VO infrastructure.

Open Science Grid

Backend transition

Frontend CA



OIM ▾ Home Certificate Topology Downtimes Virtual Organizations Support Centers Campus Grids Projects

Home

USER CERTIFICATES
- Request New
- My Requests
- Search

HOST CERTIFICATES
- Request New
- My Requests
- GridAdmins
- Search

In 2016, US ATLAS will cease to use OSG-supplied certificates, in favor of certificates issued by the CERN certificate authority (CA). To ensure minimal impact to your ATLAS privileges through this transition, US ATLAS encourages you to obtain a personal certificate from the CERN CA (if you don't yet have one), and add it to your existing ATLAS VO membership.

For details on the OSG certificate CA migration, click here

Welcome to the OSG PKI Certificate Request & Management System

To request a new user or host certificate, please select the appropriate option from the menus to the left.

Documentation for Specific VOs and Sites

- CMS User Documentation
- FermiLab User Documentation
- ATLAS User Documentation
- Using the CERN CA for ATLAS users

General Documentation for all OSG Users

- Documentation on Getting a User Certificate via Web interface
- OSG/PKI Certificate Renewal
  Note: Check to make sure that your soon to expire DigiCert user certificate is currently installed on your browser.
- OIM User's Guide
- OSG PKI command-line clients
- All OSG PKI Documentation

OIM Version 3.46 | Report Bugs | Privacy Policy Request for Assistance

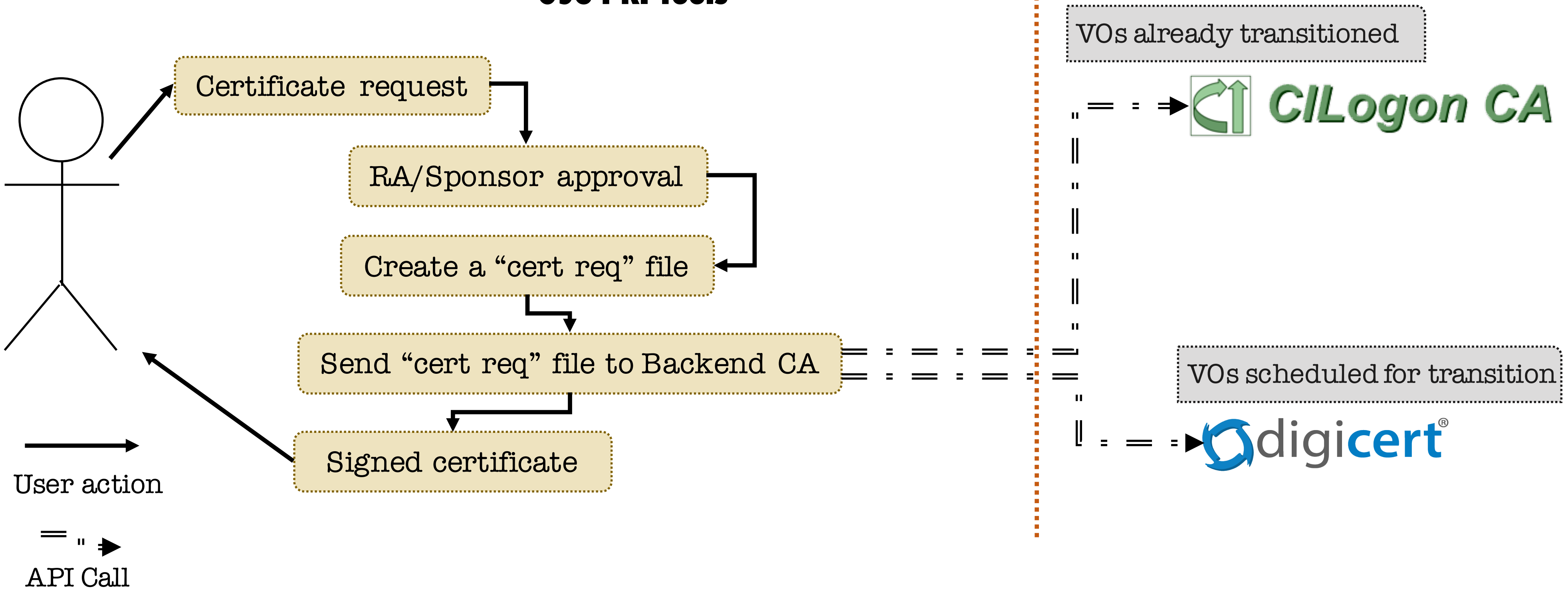
Copyright 2011 The Trustees of Indiana University - Developed for Open Science Grid

OIM

```
osg-cert-request
osg-cert-retrieve
osg-gridadmin-cert-request
osg-user-cert-renew
osg-user-cert-revoke
osg-cert-revoke
```

OSG-PKI-Tools

Backend CA



VOs already transitioned

CILogon CA

Certificate request

RA/Sponsor approval

Create a “cert req” file

Send “cert req” file to Backend CA

Signed certificate

VOs scheduled for transition

digicert®

User action

API Call

Open Science Grid

Transitioning a VO

- Scheduled month, agreed with VO manager when the certificate signer for the VO is changed:
  - After that date in the month, all the certificates issued to the VO members will be signed by CILogon OSG CA.
  - Some users/host/services still hold DigiCert certificates.
- VO should communicate transition to VO members.
- VO should test the production workflow and infrastructure involved.

Open Science Grid

Transitioning a VO

- VOMS administrators are asked to register new DNs in services to guarantee continuous access: VOMS (VO membership), DocDB, etc.
- Transition team coordinate the update of the VOMS server(s) certificate(s) and the vomses file in VO package.

Open Science Grid

Issues

- Intermittent issue with Certificate Signing Request (CSR) format
  - `CertificateProviderException:: From CILogon: Unknown status code from cilogon: 500`
  - The CSR received by server (CILogon endpoint) was broken (had zero length version number).
- Revocation requests for DigiCert certificates were being routed to CILogon
  - If a certificate was issued prior to a VO switching signers, and that certificate must be revoked, the revocation request was sent to CILogon instead of DigiCert.

Open Science Grid

Issues

- Globus announced changes in the name matching mode from Hybrid to Strict mode.
  - All hostnames and aliases must be included in the certificate (X.509v3 Subject Alternative Names field).
  - OIM, OSG-PKI-tools and CILogon did not support host certificate requests with alternate hostnames/aliases.
  - Host certificates with alternate names used to be requested manually through the DigiCert account portal.
- Host certificate requests with alternate FQDNs in different domains were rejected.
  - OIM added support for this use case as long as the domains share at least one common Grid Admin.

Lessons learned

- Pay attention to all error messages:
  - OIM expanded the error messages received from CILogon API.
- Keep monitoring the VO for possible problems.
- Keep testing!

Open Science Grid

Issues

- Understanding the technical process needed in OIM to switch the backend of a VO.
  - Transition dates were initially agreed for the first day of every month.
  - GOC and OSG Software cycle releases are established for Tuesdays.
- Communication to all the VO members
  - Atlas decided to move their users to CERN CA. Still use host and service certificates at OSG.
  - Atlas users needed to be warned about the transition and directed to CERN CA
  - Preventing Atlas users to renew OSG certificates

Open Science Grid

Lessons learned

- We adjusted the VOs transition dates accordingly to GOC and OSG Software Team cycle releases.
- Confirm action items and deadlines repeatedly.

> Speak up how you understand things, clarify/confirm with parties involved – repeat as necessary, until everyone is on same page! KEEP REPEATING!
>
> Neha Sharma, OSG CA Transition, Fermilab

Challenges

- For VOs managing their VOMS servers
  - New certificate need to be installed right after the VO had the Certificate Signer switched in OIM.
  - Also, the VO Package needed to be installed ASAP in the nodes where `voms-proxy-init` calls were expected.

Open Science Grid

Summary

- Transition project has been successful so far
  - None of the 26 transitioned VOs have reported any negative impact to their workflows production.
  - Collaboration between GOC, Software, Security and transition team has been crucial for this outcome.
- There are still 19 VOs scheduled to be transitioned until the end of May.
  - Remaining VOs have fewer users and less complex infrastructures/workflows

Open Science Grid

Summary

- DigiCert contract ends on May 31st, 2016.
    - Certificates will remain valid until their expiration date.
    - Revocations can be submitted anytime.