Open Science Grid

OSG Security: Updates on OSG CA & Federated Identities

Mine Altunay, PhD
OSG Security Team

OSG AHM

March 24, 2015

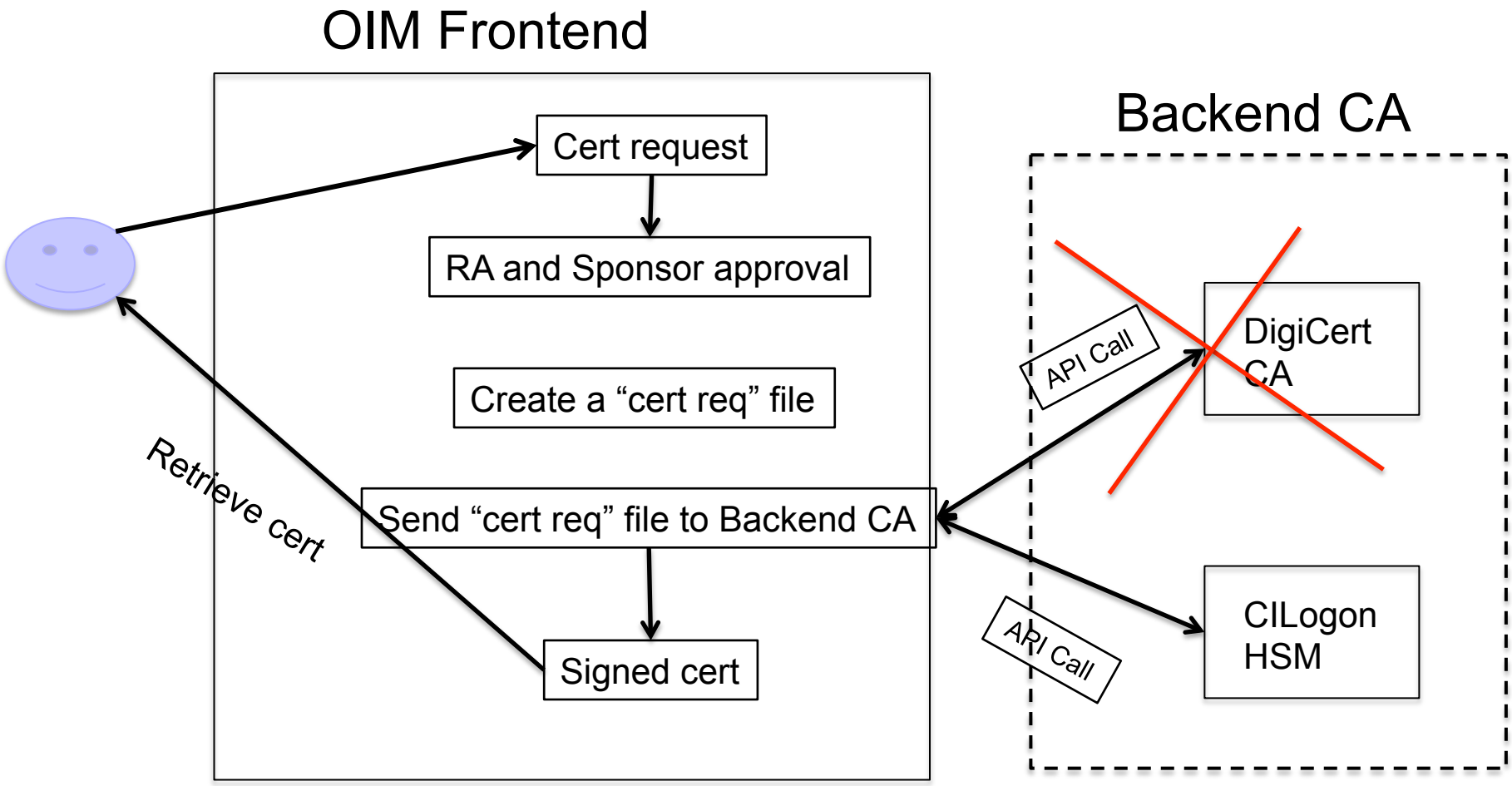
Updates On OSG CA

- OSG CA functions and serves our community well.
- In last year, we have issued
  - 1067 user certificates to 44 different VOs.
  - 6261 host certificates to 28 VOs.
- There will be some changes to OSG CA
  - Impact on end users will be minimal to zero.
  - Some impact on Site admins who manage host certs
- **OSG will continue the OSG CA service. No disruption to the service**
- **All users will continue to obtain their certificates in the same manner as before.**

OSG CA Change

- OSG CA has two main components:
  - The OIM Frontend that handles all the user interface and certificate workflows
  - The Backend that cryptographically signs the certificate requests. This is currently DigiCert CA. OIM Frontend invokes DigiCert API and sends the requests.
- We are changing the Backend only
  - From DigiCert to CILogon HSM service.
- We are not making any changes to the OIM Frontend. Users will still see the same interface and they will do the same actions to obtain certificates

Open Science Grid



Open Science Grid

Scope of the Change

- User interface, certificate workflows (steps taken to obtain a certificate), and OSG policies will remain the same
- The OIM makes some API calls to the Backend Provider. These calls will be changed.
- The user will have a new certificate DN. This will be the only apparent difference to the user that we changed the backend provider.

Open Science Grid

Motivation For the Change

- CILogon HSM is offered by XSEDE. Allows us to collaborate with a major peer grid and share resources.
- In return XSEDE asked OSG to function as a backup CA for XSEDE resources, which we agreed.

Impact on End Users

- The only visible change to the user is his/her new certificate Distinguished Name. The new DN will be:
  - /DC=org/DC=opensciencegrid/O=Open Science Grid/ OU=People/CN=Mine Altunay.
- The users will have to register the new DN with VOMS servers. BUT:
- **To ease the pain, we plan to automate this process and register the new DNs ahead of time. So the end users will NOT have to take any action.**
- In other words, when certificates expire, users will renew their certs just like in the past and continue with their work.

Open Science Grid

Impact on Site Admins

- They will receive new host certs as their existing certs expire. The mechanism to obtain the certs remain the SAME
- If they are an ITB site, we will ask them to help us test the certs before we switch to production
- If the service DN is registered by another service, then the site admin must notify the corresponding service owners. E.g. GUMS service registers the DN of VOMS servers.

Open Science Grid

Impact of the Change

- The impact of this change on our users will be smaller than our transition from DOEGrids CA to OSG CA.
- In the former transition, we also build the OIM frontend and defined the user workflows. Changed the way the end users receives certificates.
- In this transition, the frontend remains the same. The users will use the same process and mechanisms to obtain certificates

Open Science Grid

Timeline

- Our current contract with DigiCert CA will end June 2016.
- We will start transitioning our users starting January 2016.
- Our ITB sites and VO services should test the new certificates starting April 2015 through July 2015.
- All OSG software will be tested during the ITB stack
- VOs should test any VO specific software that is not included in the OSG Stack.

Updates on Federated Identities

- What do Federated Identities mean?
  - Similar to how passports work. You have one passport from your country, but when you travel, all other countries recognizes your passport. You do not have to get a new passport from each country you visited.
  - Federated Identities work the same way.
  - When you have an identity token from your home organization, you can use this token to access other institutions.
    - For example, you logged into Fermilab services domain. It will issue an access token (cookie, cert, or etc). You can use this token to access CERN

Open Science Grid

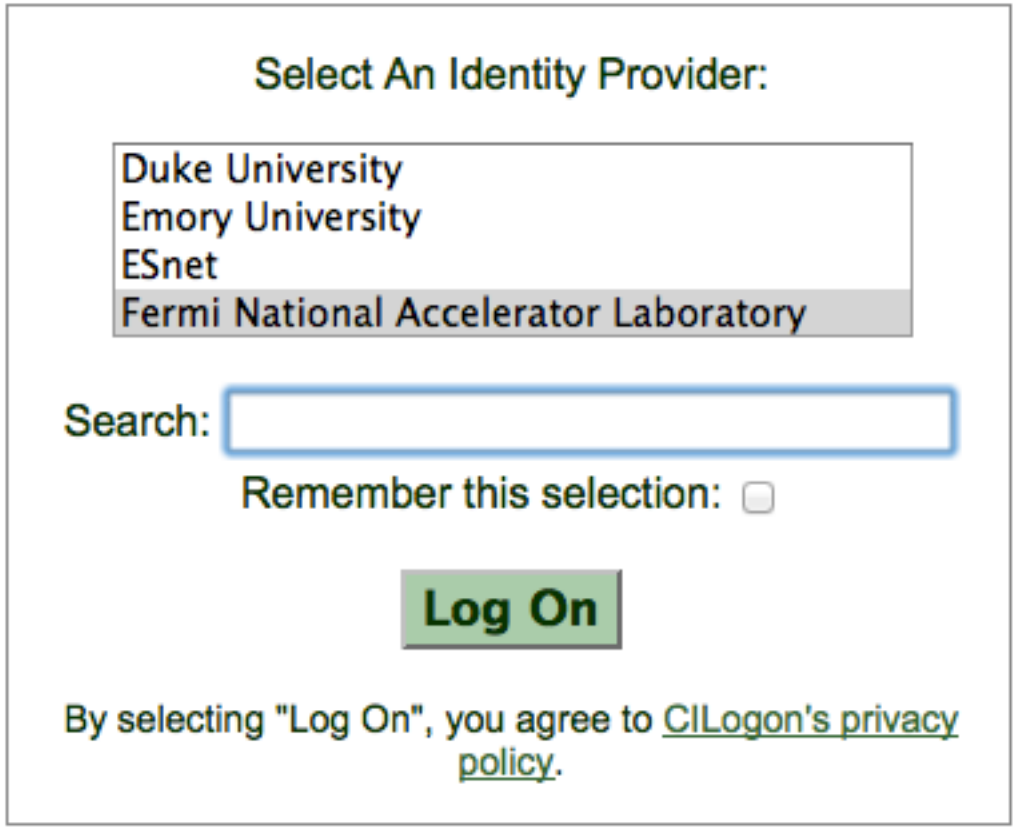
Federated Identities

- How does Federated Identities help the end user
  - You do not have to create a new account with every single institution that you need access to.
  - You have a single account with your home organization. And, your home org sends this info to other organizations if you need to access them.
- Requires a coordination between the organizations, they need to know who they trust and which access tokens they will get from them

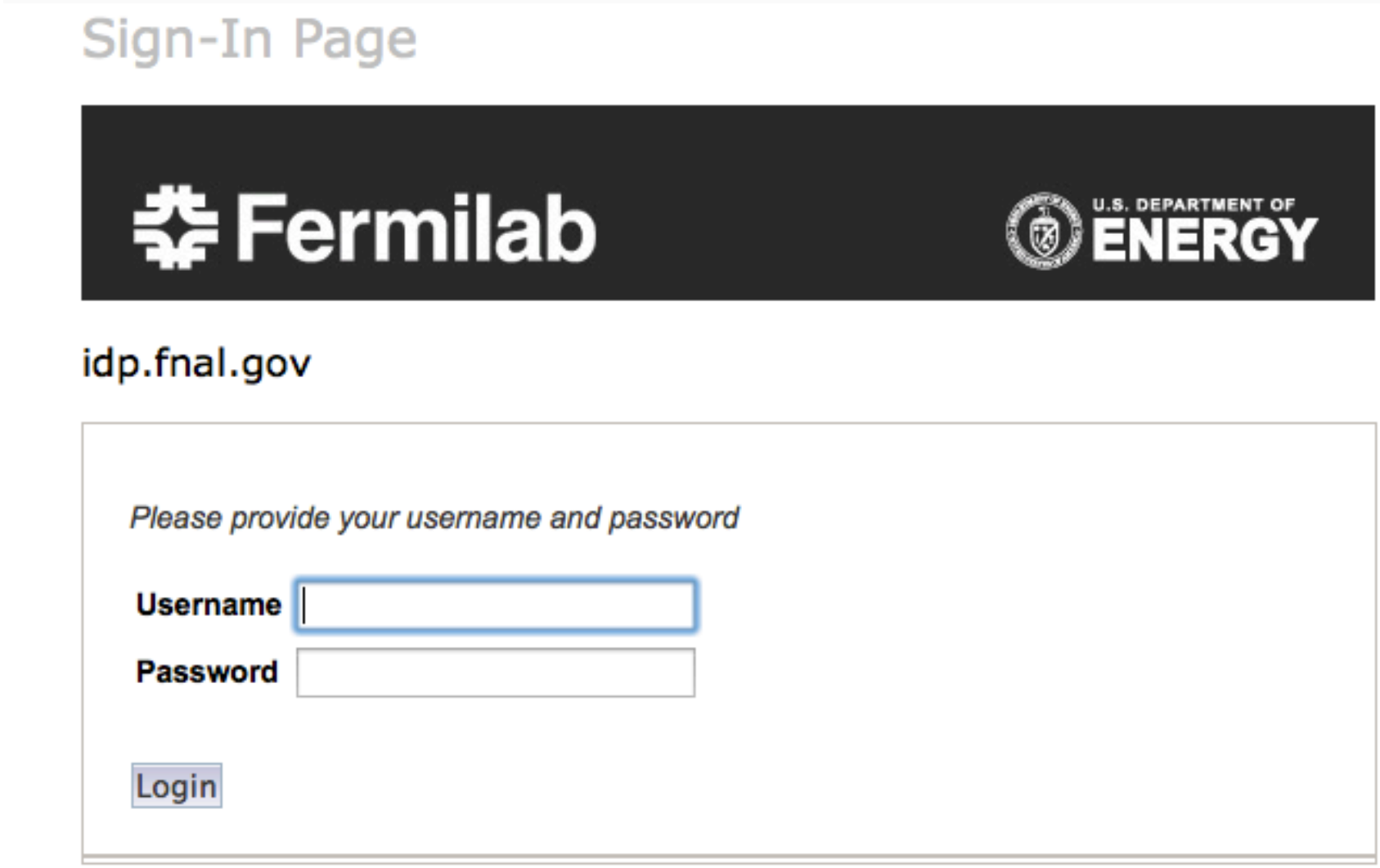
Benefits of Federated Identities

- OSG infrastructure is mainly built on certificates.
- CILogon Basic CA is a Certificate Provider who works with Federated Identities
  - CILogon Basic CA can issue fully-automated certificates
  - User goes to CILogon Basic website, selects his home organization. CILogon forwards the user to its home to authenticate itself. Once the user authenticates, his browser is redirected to CILogon website and the user obtains a certificate.

CILogon Basic CA



CILogon Basic CA



Open Science Grid

CILogon Basic CA

Certificate Subject:	/DC=org/DC=cilogon/C=US/O=Fermi National Accelerator Laboratory/CN=Mine Altunay A18111
Identity Provider:	Fermi National Accelerator Laboratory
Level of Assurance:	Basic

Password Protect Your New Certificate:

Enter A Password:

Confirm Password:

Get New Certificate

Log Off

Open Science Grid

CILogon Basic CA

- Fully IGTF accredited. You can obtain certificates from this CA and use it on OSG
- Can access to grid sites and OSG twiki, docdb, etc
- Over 130 organizations directly collaborate with CILogon, so their users can get automated certificates
- Fermilab is one of the strong collaborators, allowing all users to get these certs.

Open Science Grid

CILogon Basic CA

- How is that different than OSG CA
  - Much faster, fully automated CA
  - Identity vetting is fully automated. User is authenticated by his home org.
  - With OSG CA identity vetting is a manual step; create a ticket, route this to a sponsor who knows the requestor, check the user's identity, approve the request, then issue the cert. Can take a few days.
  - We encourage all our users to try the new CILogon Basic CA
- One Final point: CILogon project has multiple services. Basic CA is different than the HSM service we talked about before.