Grid Access with Federated Identity

Dave Dykstra

OSG All Hands Meeting

March 15, 2016

Ordinary grid access and Federated Identity

- Ordinarily, in order to submit jobs to OSG, users need to (in addition to other things):
  - annually get an X.509 certificate for themselves
  - register the Distinguished Name (DN) of the cert in VOMS
  - store the certificate and encrypted key in ~/.globus
  - daily run grid-proxy-init or voms-proxy-init, type in their passphrase
- The first step above can be done with cilogon.org web interface and federated identities
  - cilogon contacts home institution Identity Provider
  - more convenient for managing identity
  - still has same user hassles for managing certs, however

Fermilab's current job submission

- Fermilab's current job submission system (Jobsub) bypasses user hassle of certificates:
  - "jobsub_submit" automatically invokes "kx509" to create a cert using Fermilab Kerberos credentials when needed in order to contact Jobsub server
  - DNs automatically registered in VOMS for Fermilab users
- The system has a few issues, however:
  - setting up Fermilab Kerberos is painful for remote users
  - Jobsub server has to manage duplicate kerberos credentials for every user for long-lived jobs
  - the Kerberos Certificate Authority (KCA) server is getting shut down in October

Distributed Computing Access with Federated Identities (DCAFI) project

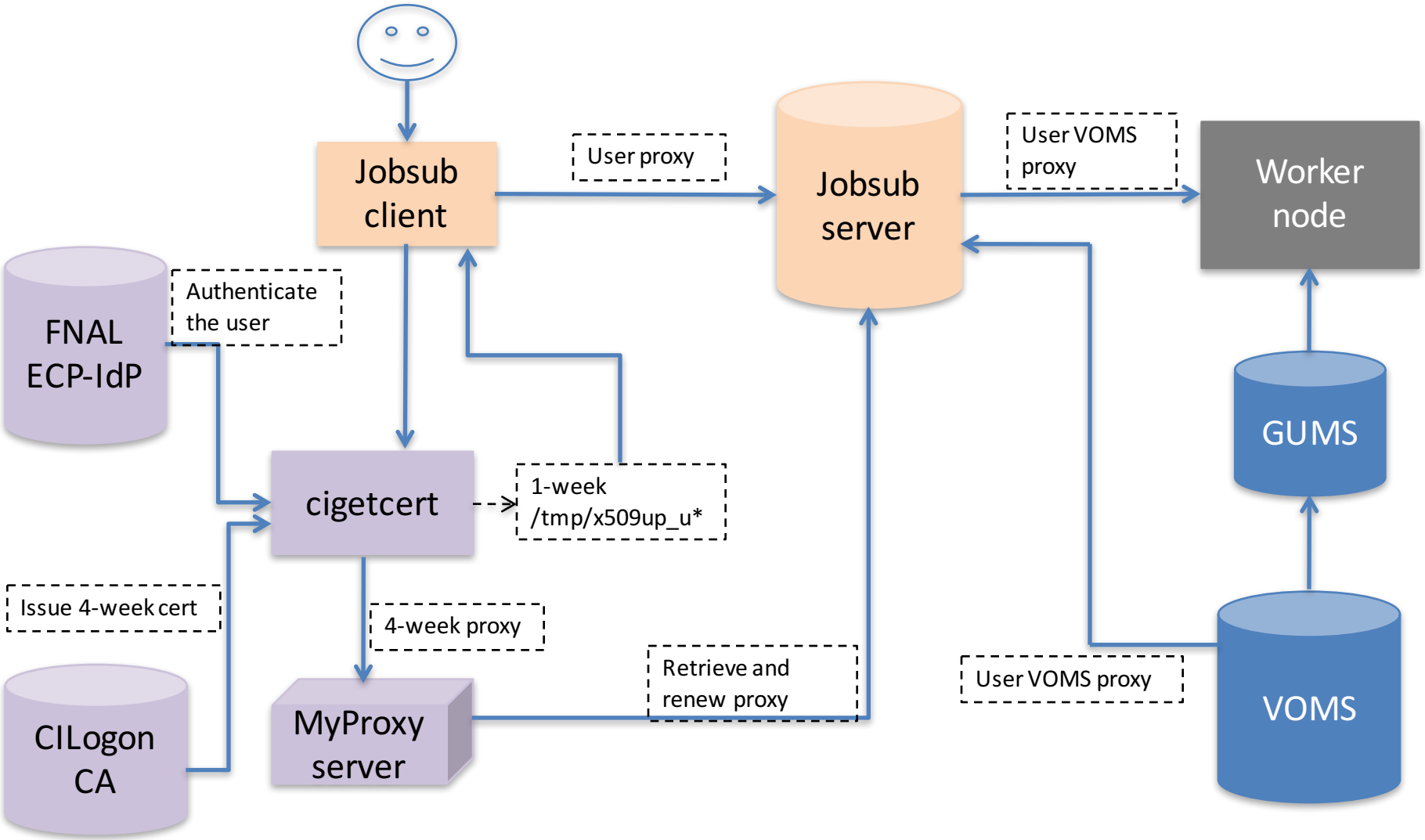
- Motivation for the DCAFI project:
  - Dependency on Kerberos makes it difficult for non-Fermilab scientists to access our grid resources remotely, obstructing our lab's goal of being an international laboratory
  - The KCA server is losing its support starting this October, forcing us to find a replacement Certificate Authority (CA) for grid access
  - Asking users to manage their own certificates is a burden on them we avoided with KCA grid access, and we want to continue to avoid it

- Project Goals
  - Remove our dependency on Kerberos and KCA certificates
  - Shield the users from the complexities of X.509 certificates
  - Integrate our authentication infrastructure with federated identities
  - In phase 1 we will use only Fermilab identities, but in phase 2 we will support other institutions. Phase 1 users need a Fermilab account but don't need to login to a Fermilab machine or set up Fermilab kerberos

Basic DCAFI plan

- Make use of existing InCommon CILogon CA and existing federated identity service
  - change format of certificate DN to be similar to old KCA/kx509
- Write cigetcert command line tool to get new certificate
  - authenticate with Fermilab Kerberos or Services password
  - get 4 week certificate from CILogon, store 1 week proxy on local disk and 4 week proxy in MyProxy
- Change jobsub_submit to attempt to use cigetcert with kerberos, and if that fails, tell user to run it to enter Services password
- Change Jobsub server to renew proxies out of MyProxy
- Add new compatibility kx509 wrapper command for other tools that just get a certificate with kerberos (no MyProxy, no password)
- Automatically register all new user DNs in VOMS (as old ones are)
- Transition VOs separately based on Jobsub server config

Jobsub infrastructure with CILogon



Enhanced Client or Proxy

- Standard federated identity protocol using SAML expects full web browser
  - usually used for single-signon
  - assumes javascript, cookies, etc.
- SAML 2.0 includes a profile called Enhanced Client or Proxy (ECP) for use by non-browser applications such as command line tools
- Requires no cookies or formatted displays
- Not many sites have yet enabled it, but it is supported by Shibboleth software
- Fermilab has enabled it
  - our IdP supports both kerberos over https (SPNEGO) and basic authentication (for Services username/password)
- http://www.cilogon.org/ecp

cigetcert

- New command line tool that implements ECP, kerberos or password with IdP, and pushes proxy to MyProxy
  - intended to be generic, usable by many projects
  - written in python
  - https://github.com/fermitools/cigetcert
  - man page: https://git.io/vgcZm
- Lots of optional parameters
  - "-s" specifies server to read file of parameters, including MyProxy specifications and default institution; we host on Jobsub server
- Reads file from cilogon translating institution names to IdP URLs
- Available in cvmfs (currently el5 & el6) and being made available as Scientific Linux-Fermi rpms (el6 & el7)

```
$ . /cvmfs/fermilab.opensciencegrid.org/products/common/etc/setup
$ setup cigetcert
```

Status

- DN format produced by CILogon for Fermilab updated
  /DC=org/DC=cilogon/C=US/O=Fermi National Accelerator Laboratory/OU=People/CN=Dave Dykstra/CN=UID:dwd
- cigetcert done
- kx509 done
- rpms made, waiting on integration into SLF
- Jobsub server change developed, in production soon
- jobsub_submit change to be developed and deployed in March
- Production MyProxy server to be deployed in March
- DN auto-VOMS registration developed, working on mismatch found with people who have middle initials
- Testing and integration planned for April
- Transition VOs planned for May through August