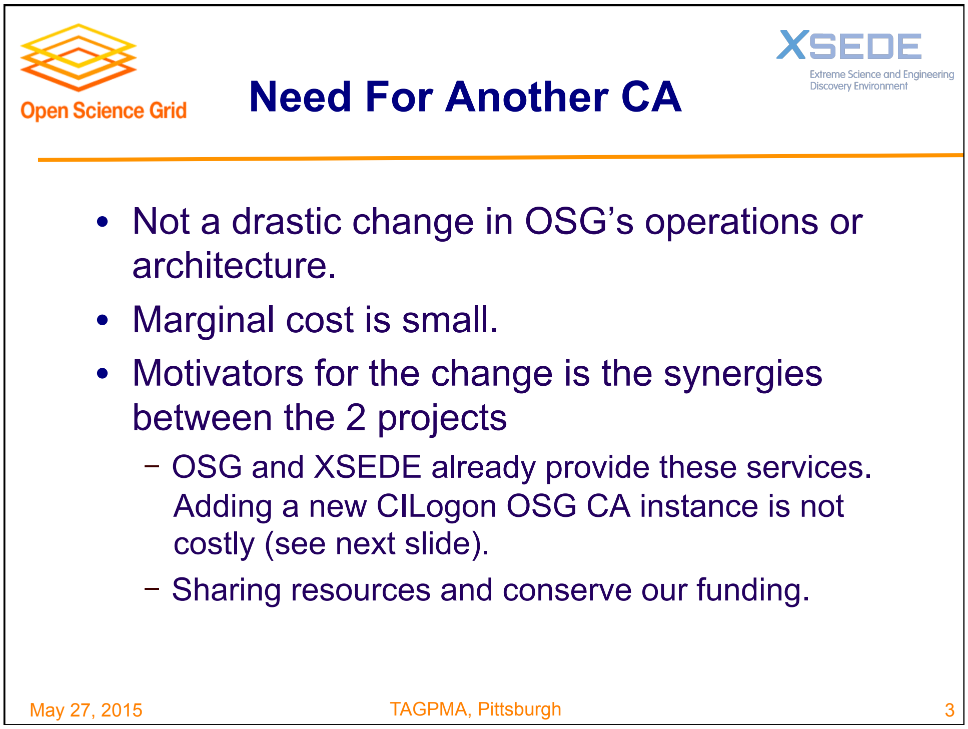
CILogon OSG CA

Mine Altunay (maltunay@fnal.gov),
Jim Basney (jbasney@illinois.edu)

TAGPMA Meeting
Pittsburgh
May 27, 2015

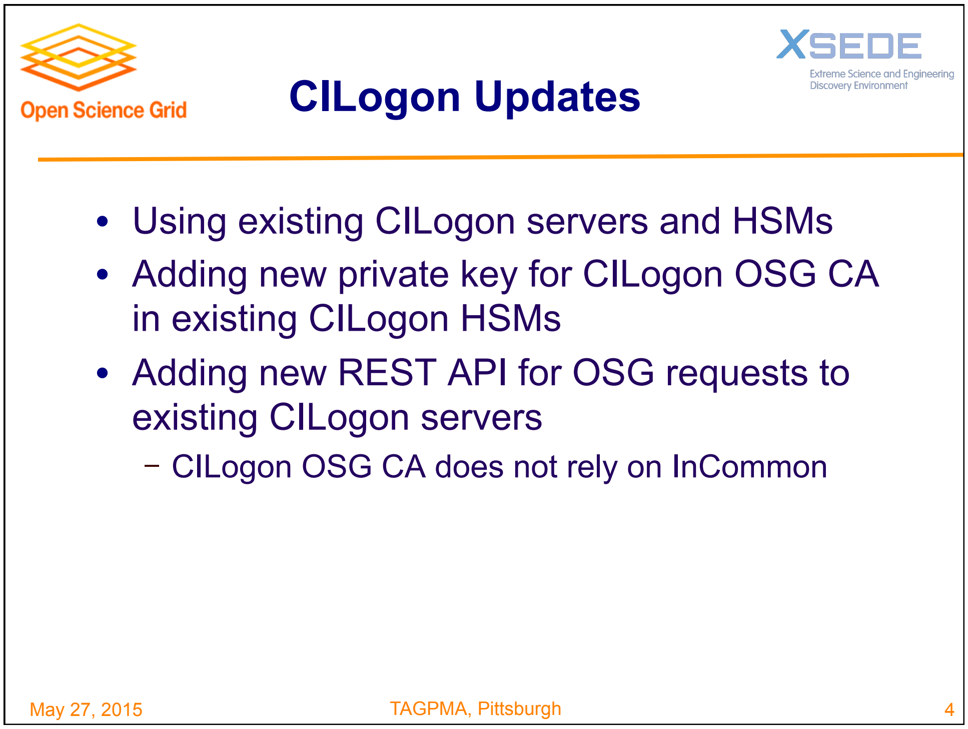
Need for Another CA

- OSG has always been running its Registration Authority. Has collaborated with various CA operators such as DOEGrids CA and DigiCert CA.
- OSG now forms a new collaboration with XSEDE
  - CILogon is now an XSEDE service. CILogon team will provide CA services to OSG. CILogon already provides CA services for various communities.
  - OSG will continue to run its RA service
-



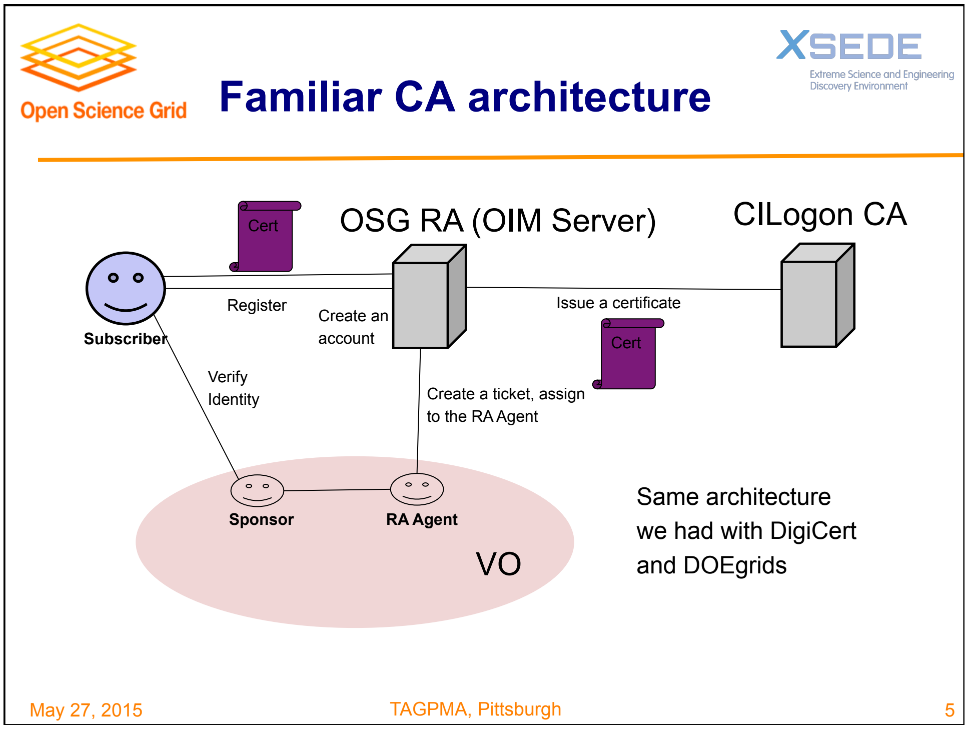
Need For Another CA

- Not a drastic change in OSG’s operations or architecture.
- Marginal cost is small.
- Motivators for the change is the synergies between the 2 projects
  - OSG and XSEDE already provide these services. Adding a new CILogon OSG CA instance is not costly (see next slide).
  - Sharing resources and conserve our funding.



CILogon Updates

- Using existing CILogon servers and HSMs
- Adding new private key for CILogon OSG CA in existing CILogon HSMs
- Adding new REST API for OSG requests to existing CILogon servers
  - CILogon OSG CA does not rely on InCommon

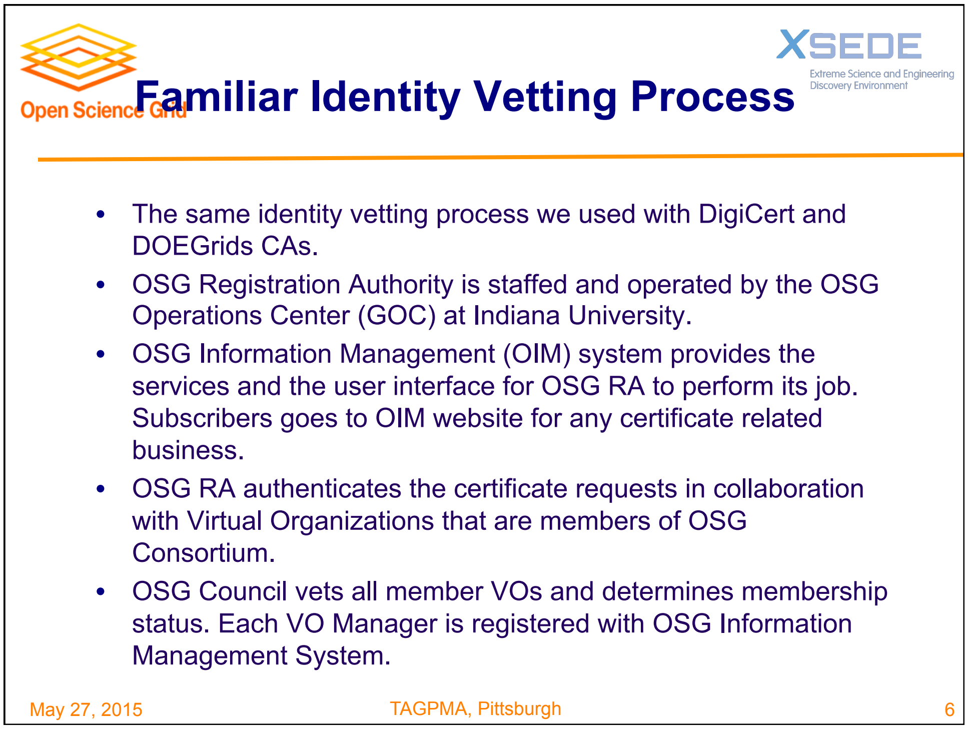


Open Science Grid

XSEDE Extreme Science and Engineering Discovery Environment

Familiar CA architecture

Same architecture we had with DigiCert and DOEgrids

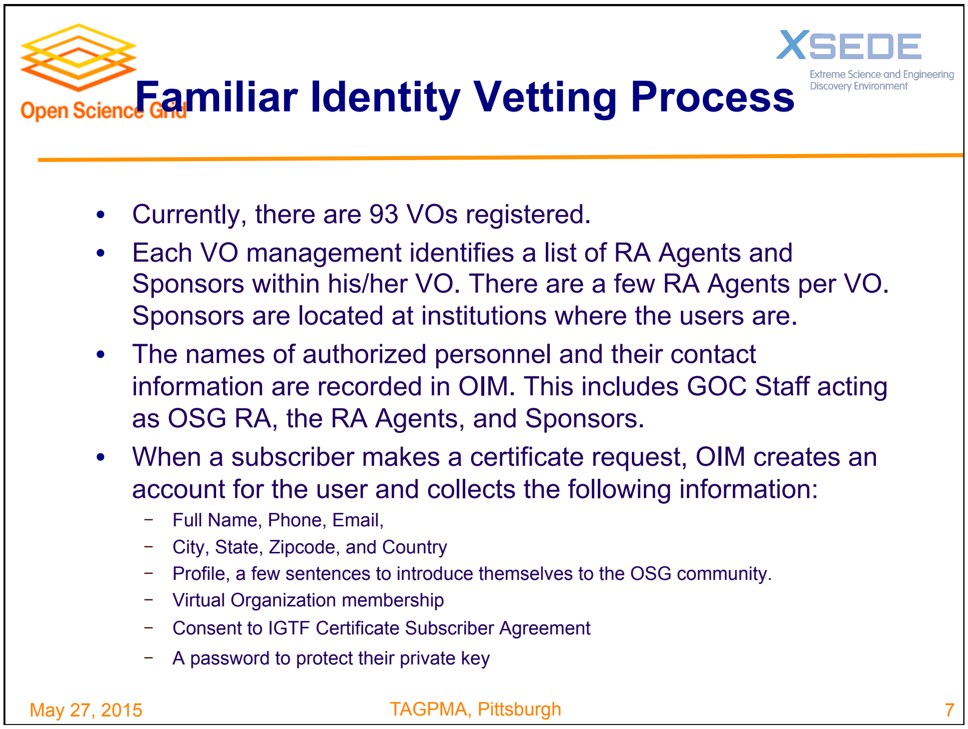


Open Science Grid

XSEDE Extreme Science and Engineering Discovery Environment

Familiar Identity Vetting Process

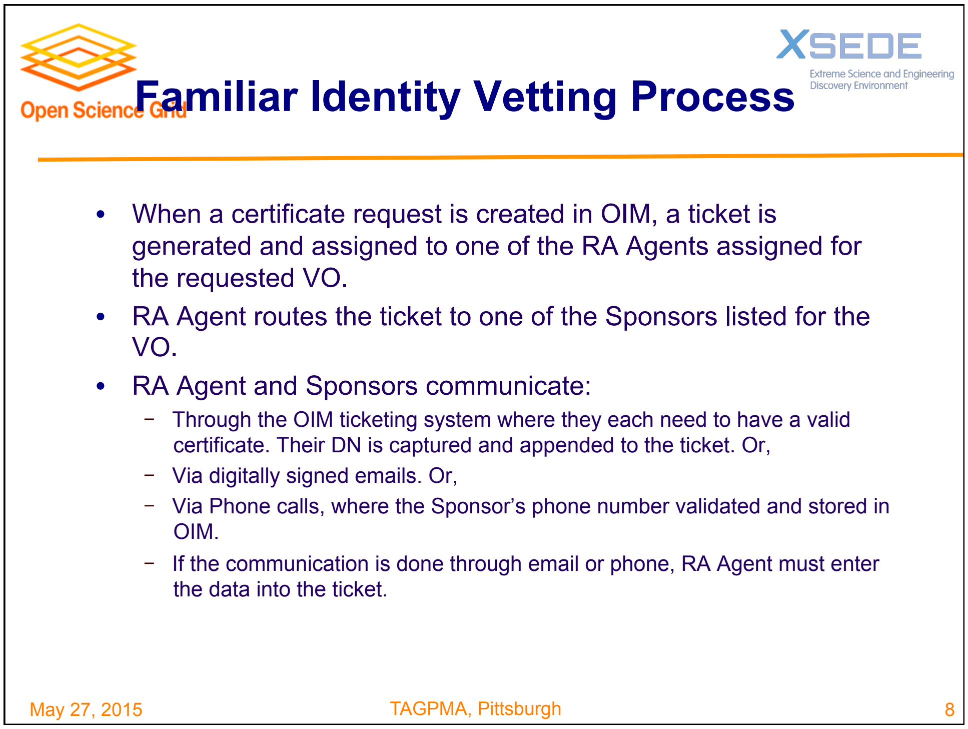
- The same identity vetting process we used with DigiCert and DOEGrids CAs.
- OSG Registration Authority is staffed and operated by the OSG Operations Center (GOC) at Indiana University.
- OSG Information Management (OIM) system provides the services and the user interface for OSG RA to perform its job. Subscribers goes to OIM website for any certificate related business.
- OSG RA authenticates the certificate requests in collaboration with Virtual Organizations that are members of OSG Consortium.
- OSG Council vets all member VOs and determines membership status. Each VO Manager is registered with OSG Information Management System.



Familiar Identity Vetting Process

- Currently, there are 93 VOs registered.
- Each VO management identifies a list of RA Agents and Sponsors within his/her VO. There are a few RA Agents per VO. Sponsors are located at institutions where the users are.
- The names of authorized personnel and their contact information are recorded in OIM. This includes GOC Staff acting as OSG RA, the RA Agents, and Sponsors.
- When a subscriber makes a certificate request, OIM creates an account for the user and collects the following information:
  - Full Name, Phone, Email,
  - City, State, Zipcode, and Country
  - Profile, a few sentences to introduce themselves to the OSG community.
  - Virtual Organization membership
  - Consent to IGTF Certificate Subscriber Agreement
  - A password to protect their private key

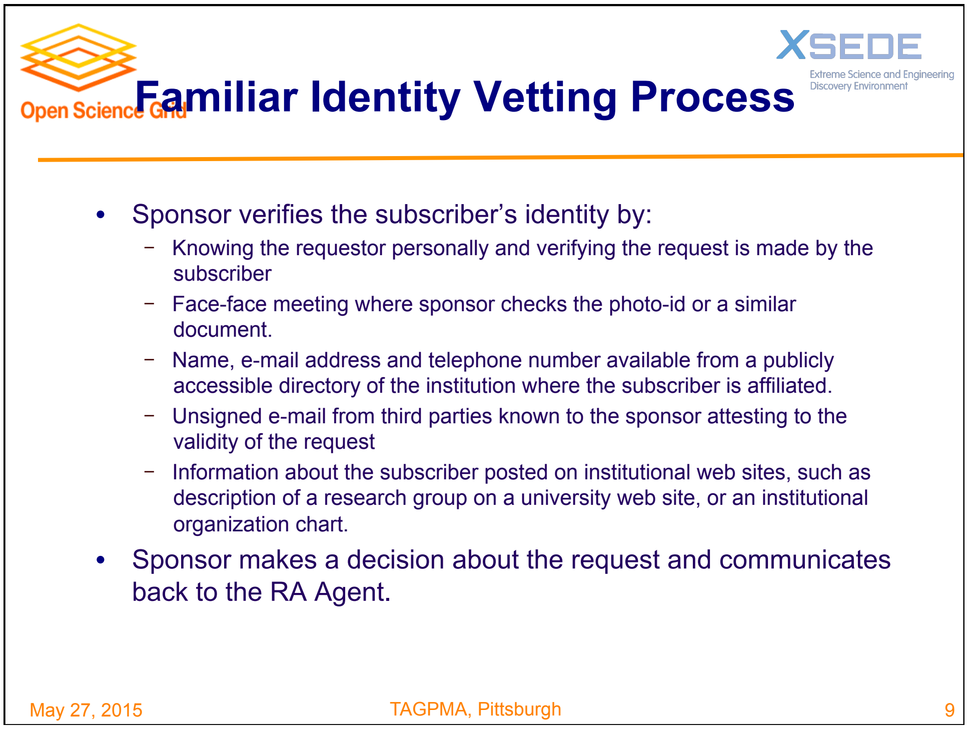
May 27, 2015 TAGPMA, Pittsburgh 7



Familiar Identity Vetting Process

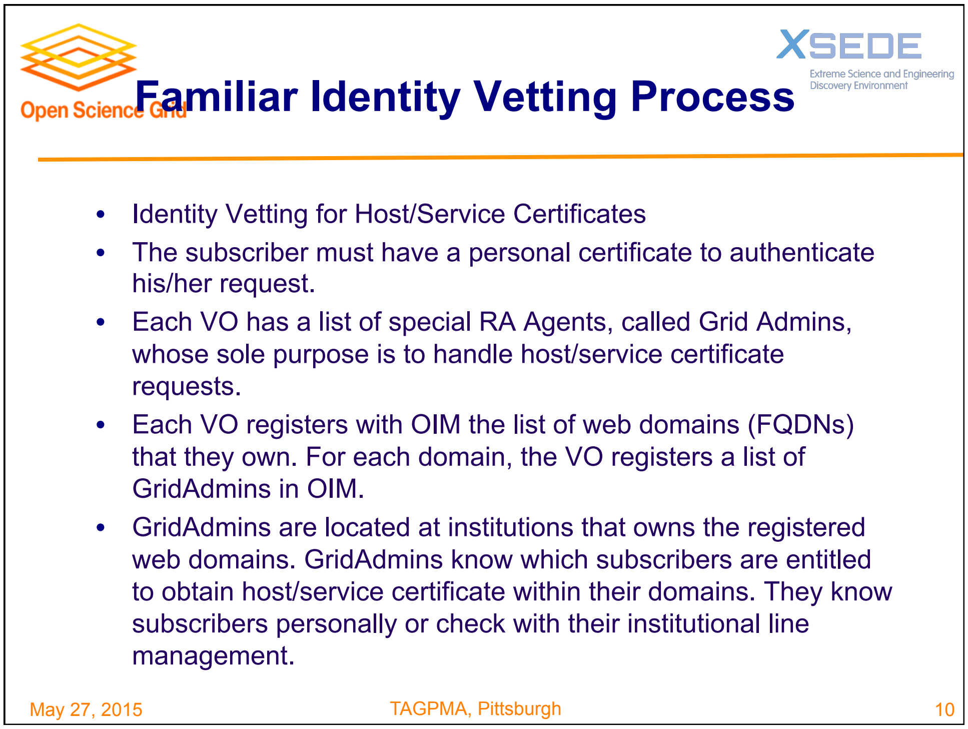
- When a certificate request is created in OIM, a ticket is generated and assigned to one of the RA Agents assigned for the requested VO.
- RA Agent routes the ticket to one of the Sponsors listed for the VO.
- RA Agent and Sponsors communicate:
  - Through the OIM ticketing system where they each need to have a valid certificate. Their DN is captured and appended to the ticket. Or,
  - Via digitally signed emails. Or,
  - Via Phone calls, where the Sponsor's phone number validated and stored in OIM.
  - If the communication is done through email or phone, RA Agent must enter the data into the ticket.

May 27, 2015 TAGPMA, Pittsburgh 8



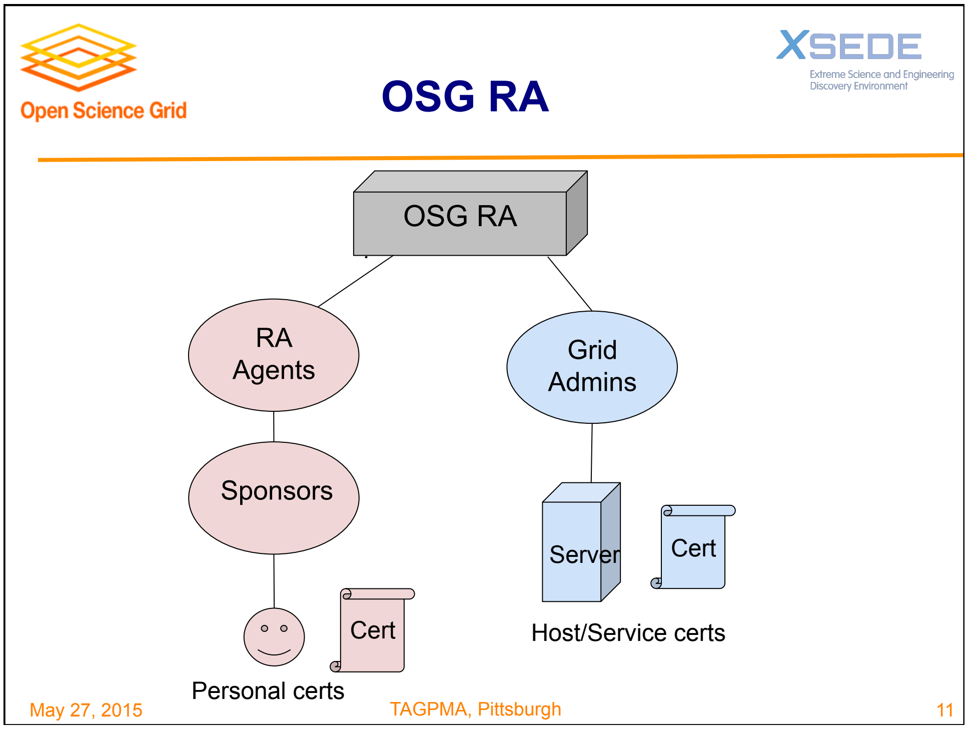
Familiar Identity Vetting Process

- Sponsor verifies the subscriber’s identity by:
  - Knowing the requestor personally and verifying the request is made by the subscriber
  - Face-face meeting where sponsor checks the photo-id or a similar document.
  - Name, e-mail address and telephone number available from a publicly accessible directory of the institution where the subscriber is affiliated.
  - Unsigned e-mail from third parties known to the sponsor attesting to the validity of the request
  - Information about the subscriber posted on institutional web sites, such as description of a research group on a university web site, or an institutional organization chart.
- Sponsor makes a decision about the request and communicates back to the RA Agent.



Familiar Identity Vetting Process

- Identity Vetting for Host/Service Certificates
- The subscriber must have a personal certificate to authenticate his/her request.
- Each VO has a list of special RA Agents, called Grid Admins, whose sole purpose is to handle host/service certificate requests.
- Each VO registers with OIM the list of web domains (FQDNs) that they own. For each domain, the VO registers a list of GridAdmins in OIM.
- GridAdmins are located at institutions that owns the registered web domains. GridAdmins know which subscribers are entitled to obtain host/service certificate within their domains. They know subscribers personally or check with their institutional line management.



Open Science Grid

OSG RA

XSEDE Extreme Science and Engineering Discovery Environment

OSG RA

RA Agents

Grid Admins

Sponsors

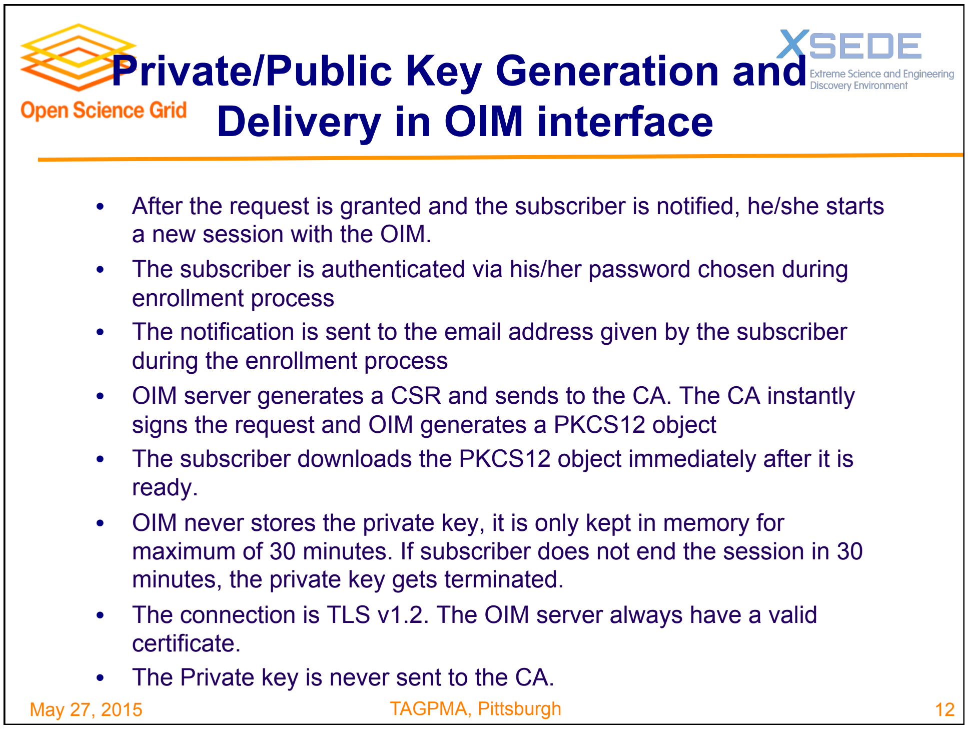
Server

Cert

Cert

Host/Service certs

Personal certs

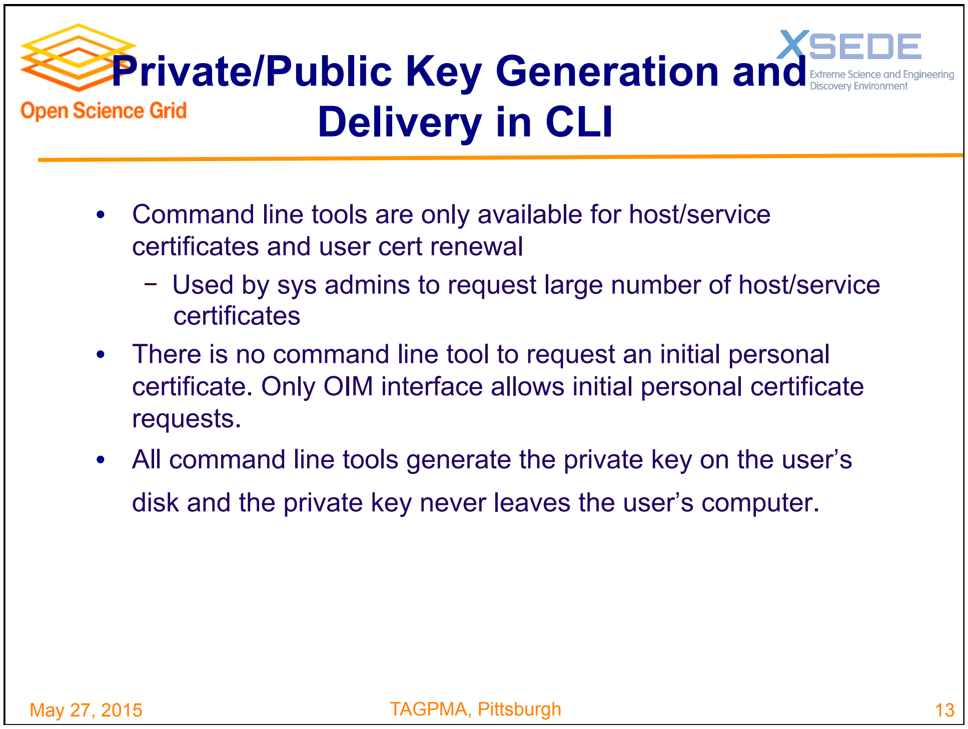


Open Science Grid

Private/Public Key Generation and Delivery in OIM interface

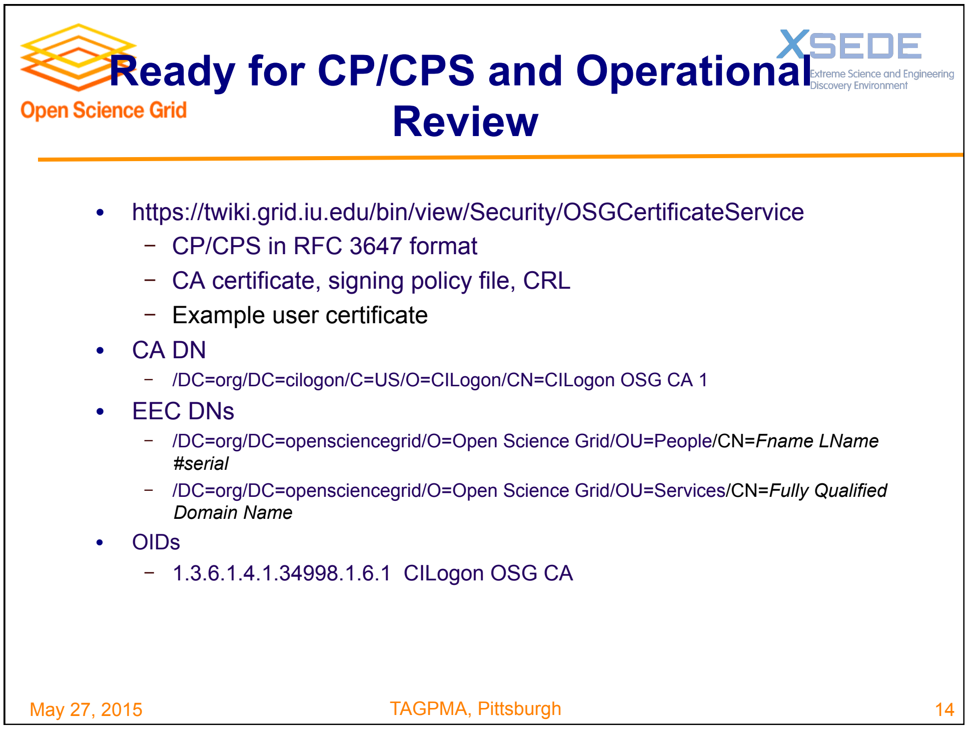
XSEDE Extreme Science and Engineering Discovery Environment

- After the request is granted and the subscriber is notified, he/she starts a new session with the OIM.
- The subscriber is authenticated via his/her password chosen during enrollment process
- The notification is sent to the email address given by the subscriber during the enrollment process
- OIM server generates a CSR and sends to the CA. The CA instantly signs the request and OIM generates a PKCS12 object
- The subscriber downloads the PKCS12 object immediately after it is ready.
- OIM never stores the private key, it is only kept in memory for maximum of 30 minutes. If subscriber does not end the session in 30 minutes, the private key gets terminated.
- The connection is TLS v1.2. The OIM server always have a valid certificate.
- The Private key is never sent to the CA.



Private/Public Key Generation and Delivery in CLI

- Command line tools are only available for host/service certificates and user cert renewal
  - Used by sys admins to request large number of host/service certificates
- There is no command line tool to request an initial personal certificate. Only OIM interface allows initial personal certificate requests.
- All command line tools generate the private key on the user’s disk and the private key never leaves the user’s computer.



Ready for CP/CPS and Operational Review

- https://twiki.grid.iu.edu/bin/view/Security/OSGCertificateService
  - CP/CPS in RFC 3647 format
  - CA certificate, signing policy file, CRL
  - Example user certificate
- CA DN
  - /DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon OSG CA 1
- EEC DNs
  - /DC=org/DC=opensciencegrid/O=Open Science Grid/OU=People/CN=*Fname LName #serial*
  - /DC=org/DC=opensciencegrid/O=Open Science Grid/OU=Services/CN=*Fully Qualified Domain Name*
- OIDs
  - 1.3.6.1.4.1.34998.1.6.1 CILogon OSG CA