MyProxy and GSISSH Update

Von Welch
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign
vwelch@ncsa.uiuc.edu

MyProxy Logon

- **Authenticate to retrieve PKI credentials**
  - End Entity or Proxy Certificate
  - CA Certificates and Certificate Revocation Lists (CRLs) (http://myproxy.ncsa.uiuc.edu/trustroots)
- **Maintains the user's PKI context**
  - Users don't need to manage long-lived credentials
  - Enables server-side monitoring and policy enforcement (ex. passphrase quality checks)
  - CA certificates and CRLs updated automatically at login
- **Integrates with existing authentication systems**
  - Providing a gateway to grid authentication

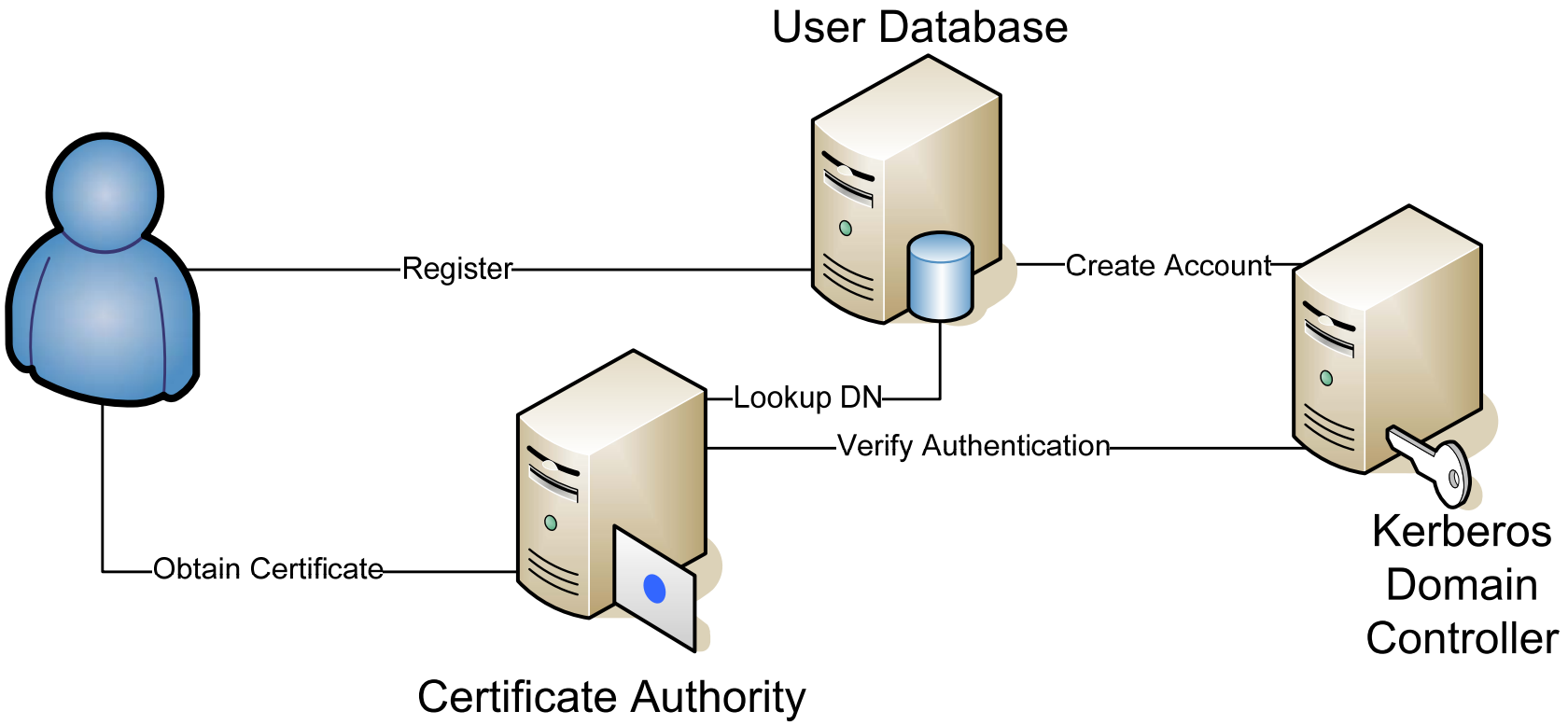
MyProxy CA

- **Issues short-lived X.509 EECs**
- **Authentication via certificate, PAM, SASL/Kerberos, Pubcookie, VOMS**
  - Including “renewal authentication” where trusted service authenticates and proves possession of user credential to get a new user credential
- **Name mapping via mapfile, callout, and LDAP**
- **Certificate extensions specified by OpenSSL configuration file or callout**
- **http://myproxy.ncsa.uiuc.edu/ca**

MyProxy and IGTF SLCS Profile

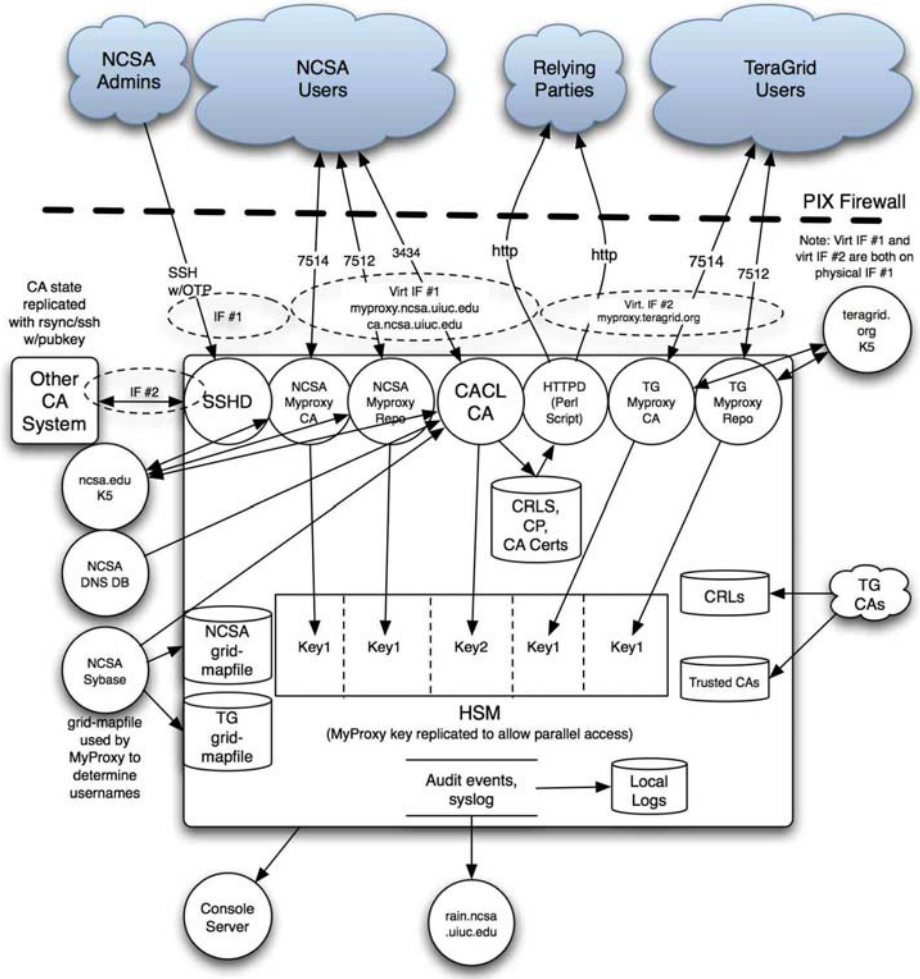
- **Recent modifications to MyProxy CA based on IGTF SLCS Profile recommendations:**
  - Log all certificate requests
  - Archive all issued certificates
  - Use 1024 bit keys
  - Use SHA1 instead of MD5
  - Set recommended certificate extensions
- **NCSA SLCS undergoing TAGPMA review**

NCSA SLCS Architecture



- **http://security.ncsa.uiuc.edu/CA/**

NCSA CA Architecture



NCSA

MyProxy OCSP Support

- **Server checks certificate validity before performing delegation**
  - Includes CRL and OCSP checks
  - Removes invalid credentials from repository
- **Follows recommendations in OGF CAOPS "OCSP Requirements for Grids"**
- **Server can be configured to use:**
  - OCSP responder in AIA extension
  - Trusted OCSP responder
- **http://myproxy.ncsa.uiuc.edu/ocsp**
- **OCSP checking code contributed to Globus**
  - http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4788

MyProxy and HSMs

- **Prototypes**
  - MyProxy repository keys protected by IBM 4758
  - MyProxy CA key protected by Aladdin eToken
- **MyProxy CA HSM support coming soon**
  - To be deployed for NCSA SLCS
  - Using OpenSSL Engine interface
  - http://bugzilla.ncsa.uiuc.edu/show_bug.cgi?id=349

MyProxy and VOMS

- **MyProxy server now understands VOMS attributes for authorization**
  - For example: services with “compute element” attribute can be authorized to renew credentials
- **MyProxy developers worked with VOMS developers on GT4 compatibility issues**
  - http://bugzilla.ncsa.uiuc.edu/show_bug.cgi?id=345
- **http://myproxy.ncsa.uiuc.edu/voms**

MyProxy Trust Provisioning

- **MyProxy Logon can install/update trust roots in ~/.globus/certificates or $X509_CERT_DIR**
  - CA certificates, signing policies, and CRLs
  - Improves client-side security via automated CA configuration and CRL updates
- **Configuration managed by MyProxy server admin**
  - Maintains up-to-date “master” certificates directory on server
- **Future work**
  - Bootstrap trust of myproxy-server certificate
  - Improved handling of expired CRLs
  - Java support
- **http://myproxy.ncsa.uiuc.edu/trustroots**

MyProxy Server Fail-Over

- **Clients try multiple server IP addresses**
- **Documentation for server replication**
  - http://myproxy.ncsa.uiuc.edu/failover.html
  - myproxy-replicate tool for primary-backup repository replication
  - CA server replication by partition of serial number space

External MyProxy Audit

- **To be conducted by Jim Kupsch from UW-Madison Computer Sciences**
  - Vulnerability Assessment of Grid Software Project led by Prof. Bart Miller
  - http://www.cs.wisc.edu/condor/CondorWeek2006/presentations/kupsch_security.ppt
- **March 7 kick-off meeting at NCSA**

GSI-OpenSSH Authorization

- **GSI-OpenSSH 3.8 and later support Globus Authorization callouts**
  - http://www.globus.org/security/callouts/
  - Service name for callout is “ssh”
  - Tested with PRIMA/GUMS

Java GSI-SSHTerm

- **Java applet/application that combines MyProxy and GSISSH functionality**
  - Developed by UK NGS, NRC Canada, …
  - http://sourceforge.net/projects/gsi-sshterm/
- **Customized for TeraGrid**
  - http://grid.ncsa.uiuc.edu/gsi-sshterm/

MyProxy and GSISSH on TeraGrid

- **All TG users assigned a TERAGRID.ORG (Kerberos) username and password**
  - Login to TeraGrid User Portal (https://portal.teragrid.org/)
  - Login to TeraGrid MyProxy CA to obtain a short-lived (NCSA) certificate
- **All TG sites run GSI-OpenSSH servers**
  - Single sign-on via Java GSI-SSHTerm
  - http://www.teragrid.org/userinfo/access/