Managing Grid Credentials

Jim Basney <jbasney@ncsa.uiuc.edu>
http://www.ncsa.uiuc.edu/~jbasney/
Senior Research Scientist
Grid and Security Technologies
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign
Credential Issuers

- Offline Certificate Authority
- Online Certificate Authority
- Online Credential Repository
Globus Simple CA

- Included in NMIR5
- Provides a simple offline certificate authority
- Users email certificate requests that CA operator signs and returns
- Integrated with MyProxy
- http://www.globus.org/security/simple-ca.html
Other Offline CA Options

- OpenCA
  - Full-featured, open source, OpenSSL-based offline CA
  - http://www.openca.org/
- Commercial CAs
KCA

- Included in NMIR5
- Online certificate authority for Kerberos sites
- Authenticate with Kerberos ticket to retrieve certificate with same lifetime as ticket
- http://www.citi.umich.edu/projects/kerb_pki/
CAACL

- Online certificate authority supporting username + password authentication
- Users retrieve long-lived certificates
- Used by SDSC and NCSA for TeraGrid
- http://www.npaci.edu/CA/
Globus Certificate Service

- Online certificate authority with no identity verification
- Third-party ID verification is over-rated!
- No need to duplicate ID verification already performed when setting up authorizations
- http://gcs.globus.org:8080/
CAcert Online CA

- Free, community, non-profit CA
- Uses web of trust to recruit registration authorities for optional identity verification
- http://www.cacert.org/
MyProxy Online Credential Repository

- Included in NMIR5
- Stores proxy and end-entity credentials, encrypted with user-chosen passphrase
- Users retrieve proxy credentials via delegation — keys never leave repository
- http://myproxy.ncsa.uiuc.edu/
MyProxy and Credential Mobility

tg-login.ncsa.teragrid.org

Obtain certificate
tg-login.caltech.teragrid.org

Store proxy
tg-login.sdsc.teragrid.org

Retrieve proxy
tg-login.uc.teragrid.org

c.a.ncsa.uiuc.edu

myproxy.teragrid.org

ca.ncsa.uiuc.edu

Obtain certificate

myproxy.teragrid.org

Store proxy

Retrieve proxy
Credential Distribution via MyProxy

- Integration with Globus Simple CA enables myproxy-admin-adduser command
- Load user credentials into the repository and distribute username + password
- Eliminate certificate request step
- Users retrieve proxies from MyProxy when needed
Credential Distribution via MyProxy

Request account
Username, password
Load user’s credentials
Retrieve proxy
Change password

Accounting system
MyProxy server
Certificate authority
Obtain user’s certificate
MyProxy and Grid Portals

- Login
- Fetch proxy
- Access data

- CHEF portal
- MyProxy server
- GridFTP server

- MyProxy and Grid Portals

- NEESgrid.png
MyProxy and Credential Renewal

- Submit job: Workload management system
- Submit job: Refresh proxy: Globus gatekeeper
- Fetch proxy: MyProxy server
MyProxy Credential Renewal with Condor-G

- Support added in Condor-G 6.7.0
- Include MyProxy information in Condor-G job submission file
- Condor-G retrieves fresh proxies on demand from MyProxy and delegates them to running jobs
MyProxy for OGSI

CredentialManagerFactory

CredentialManager Instance

CredentialManager Instance

http://myproxy.ncsa.uiuc.edu/ogsa/
Grid Logon

- Initialize grid security environment with secure password protocol
- Retrieve proxy credentials, CA certificates, CRLs, and authorization credentials
- Proposed work:
SACRED

- IETF proposed standard for online credential repositories
- RFC 3767: Securely Available Credentials Protocol
- Open source implementation in progress by NCSA MyProxy team and Brigham Young University Internet Security Research Lab
- http://sacred.sf.net/
One-Time Passwords

- Captured passwords represent a significant ongoing security risk.
- Goal: Limit lifetime of vulnerable credentials
- Integrate with grid security via online certificate authorities and credential repositories
- MyProxy OTP support in progress (early version available)
Digital Signatures

- Long-lifetime signing keys
- Integration with existing software (PKCS11, CryptoAPI)?
- Key management issues
- MyProxy support for digital signatures is planned (August 2004)
Portal Authentication

- MyProxy
- KX.509/KCA and KCT
- Shibboth
- WebISO / Cosign / Pubcookie