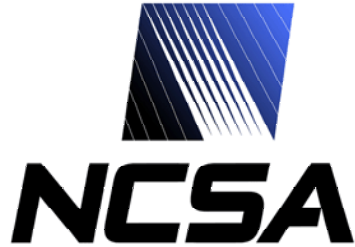


Using the **MyProxy** Online Credential Repository

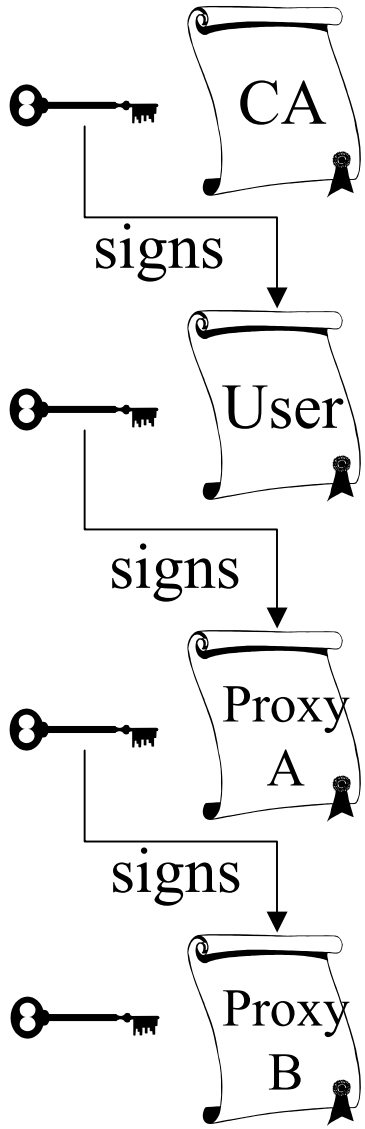
Jim Basney
NCSA
jbasney@ncsa.uiuc.edu

What is MyProxy?

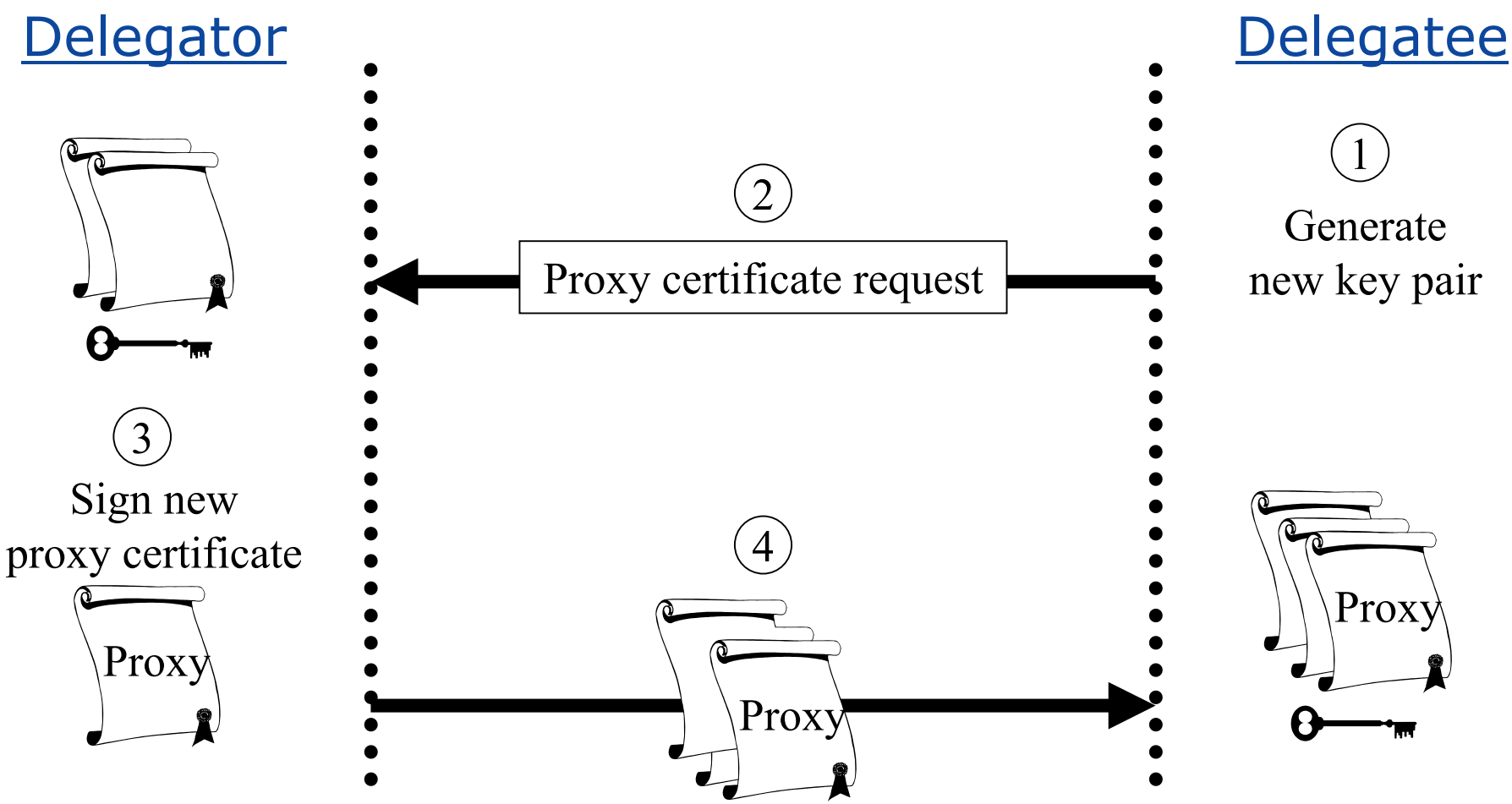
- A new component in Globus Toolkit 4.0
  - Independent Globus Toolkit add-on since 2000
- A service for securing private keys
  - Keys stored encrypted with user-chosen password
  - Keys never leave the MyProxy server
- A service for retrieving proxy credentials
  - Supporting mobility, delegation, and renewal
- A commonly-used service for grid portal security
  - Integrated with OGCE, GridSphere, and GridPort

Proxy Credentials

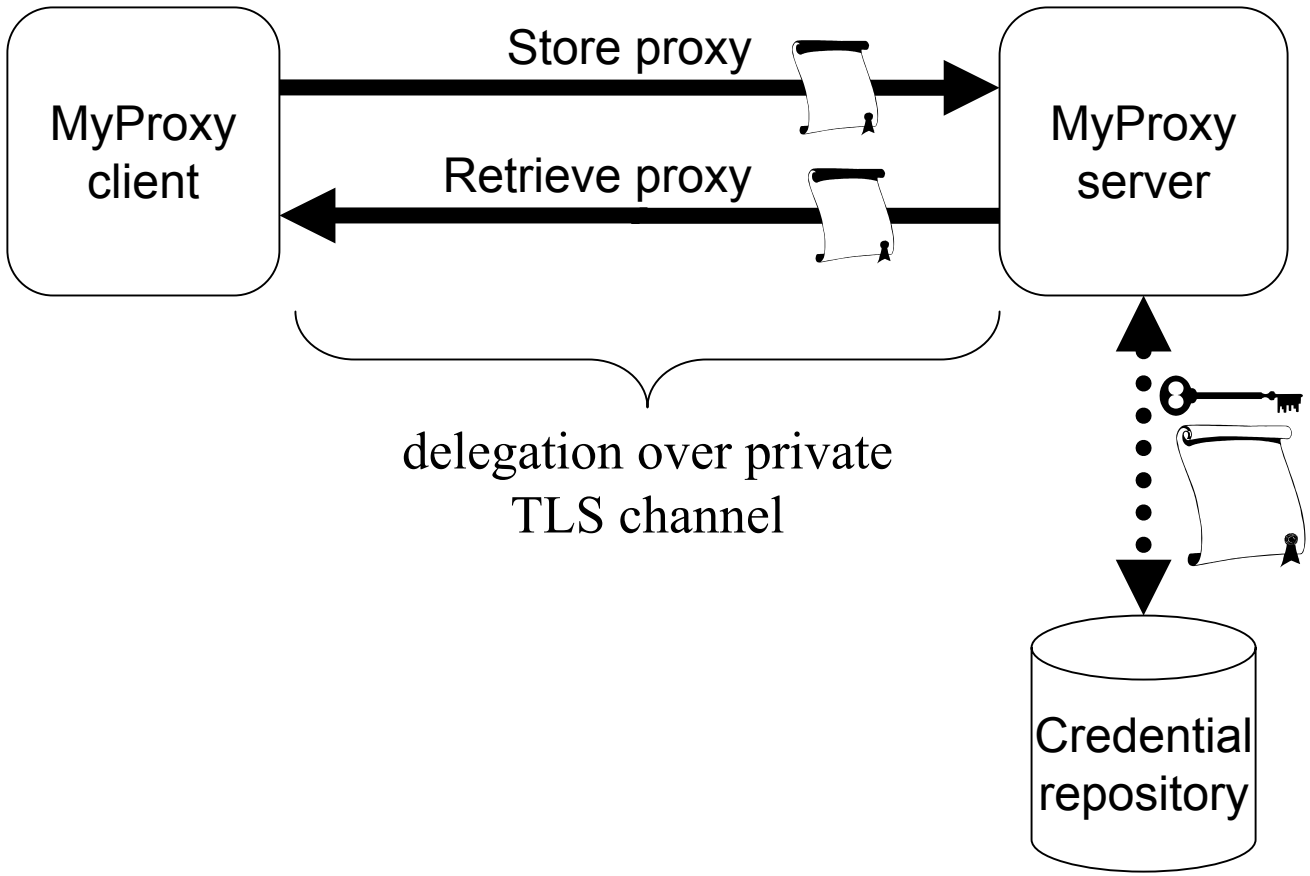
- RFC 3820: Proxy Certificate Profile
- Associate a new private key and certificate with existing credentials
- Short-lived, unencrypted credentials for multiple authentications in a session
- Credential delegation (forwarding) without transferring private keys



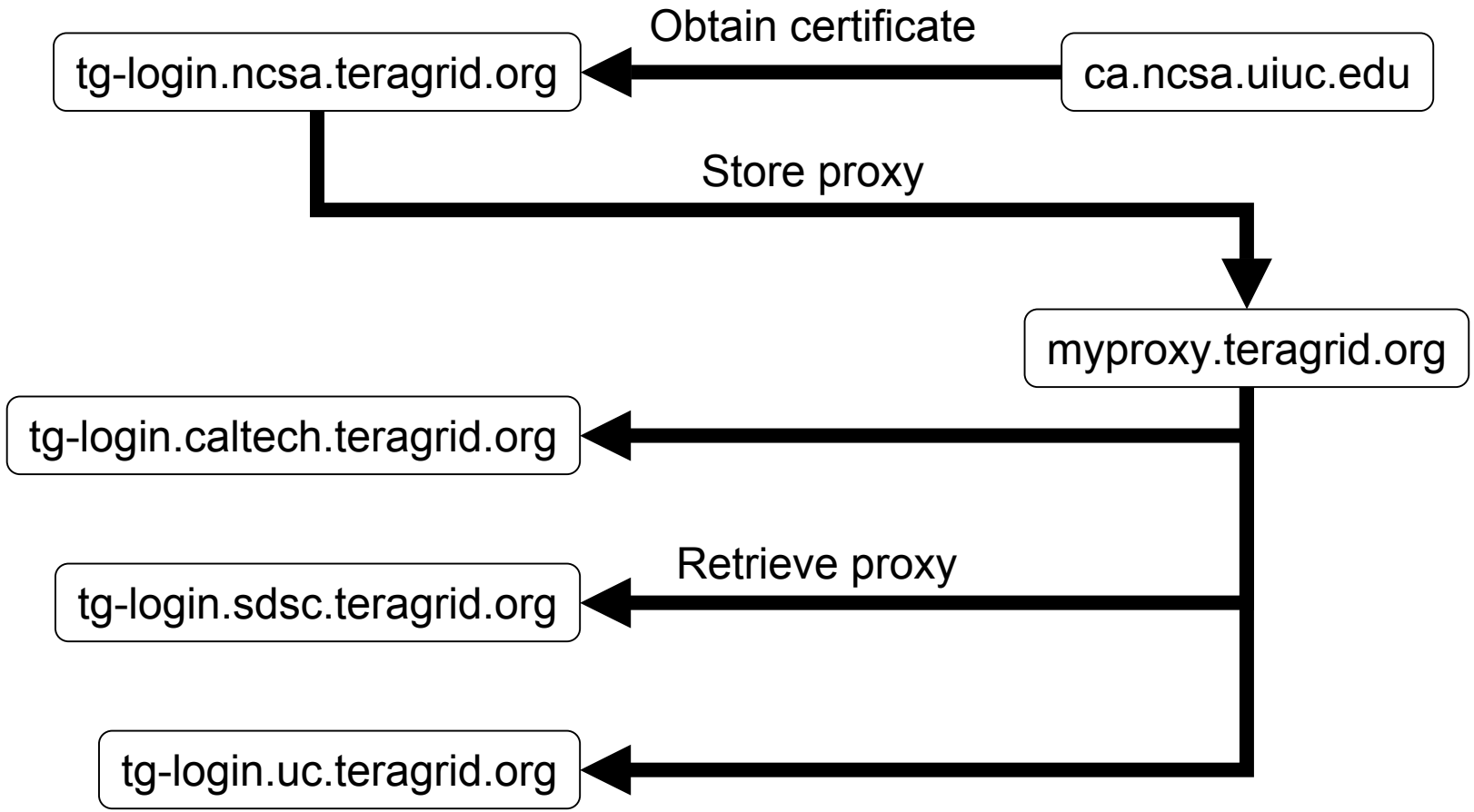
Proxy Delegation



MyProxy System Architecture

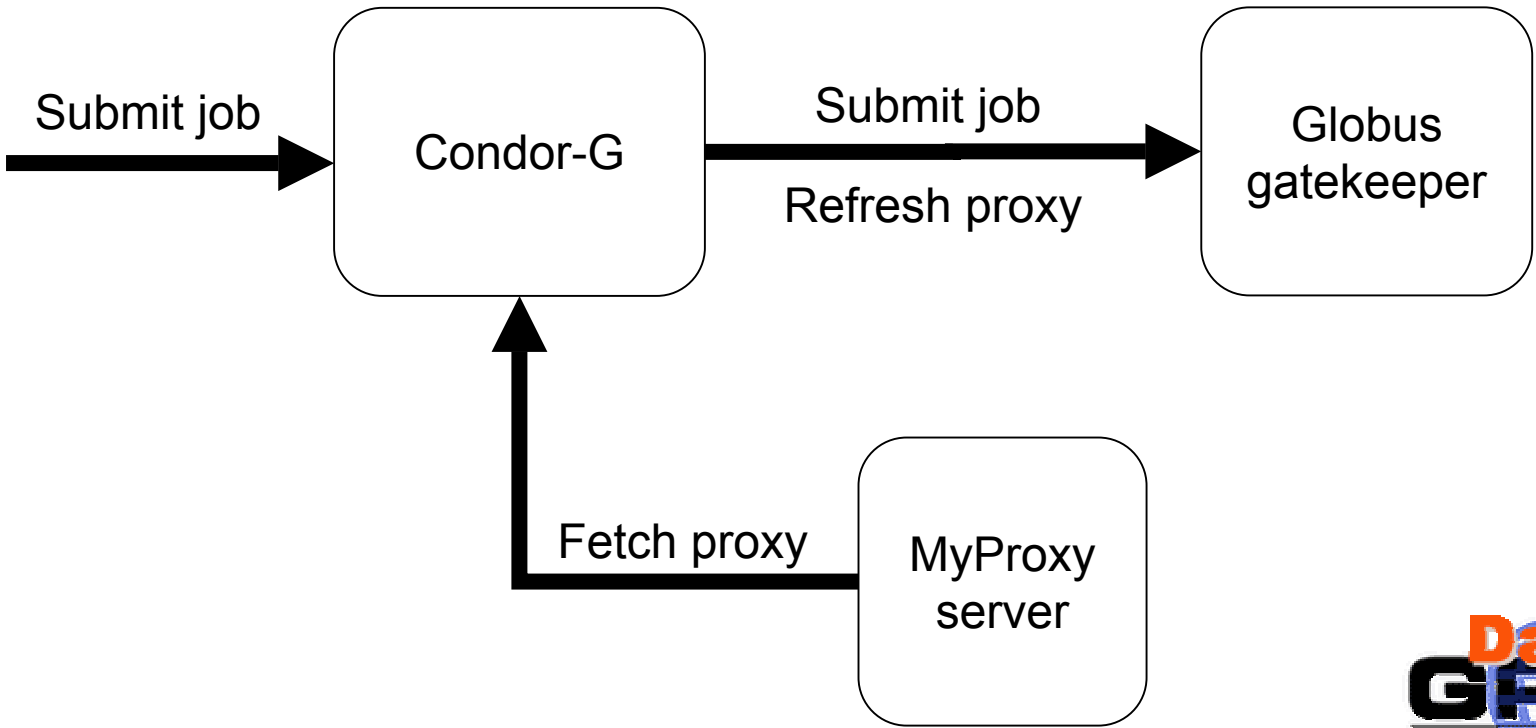


MyProxy: Credential Mobility

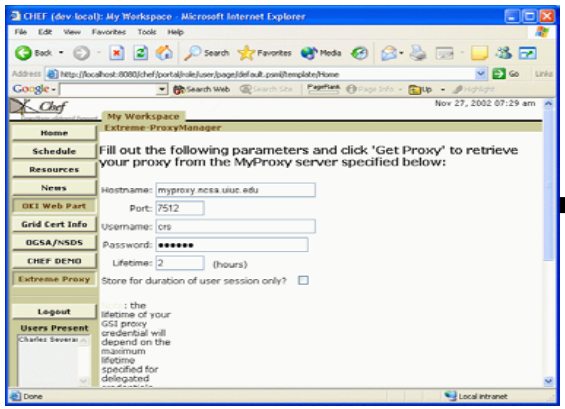


TERAGRID

MyProxy: Credential Renewal



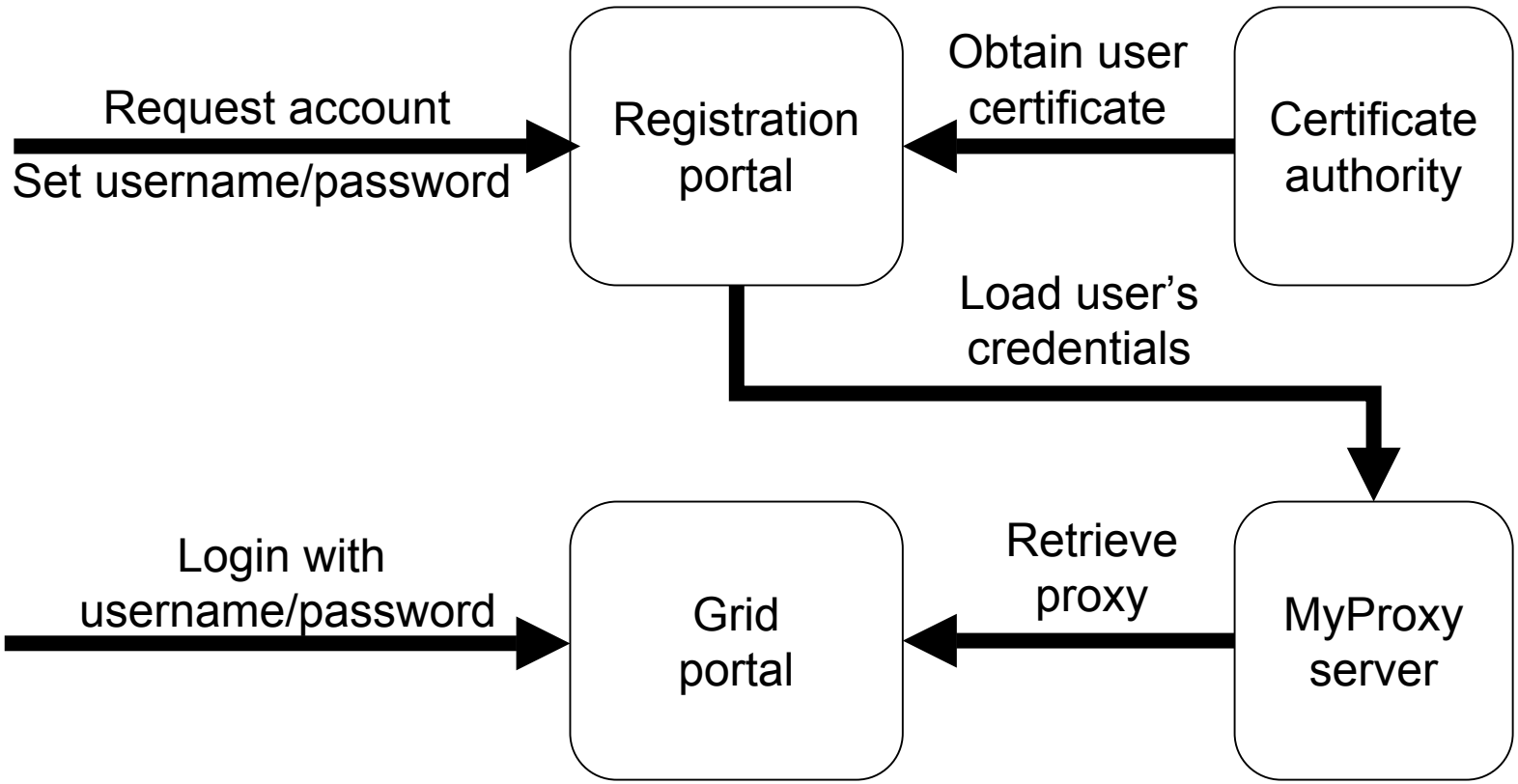
MyProxy and Grid Portals



OGCE open grid computing environment

NEESgrid

MyProxy: User Registration



PURSE: Portal-based User Registration Service

MyProxy Installation (Unix)

- As an add-on component to GT 3.x

  $ gpt-build myproxy*.tar.gz <flavor>

- Set $MYPROXY_SERVER environment variable to myproxy-server hostname

  $ export MYPROXY_SERVER=myproxy.ncsa.uiuc.edu

- Set Globus Toolkit environment

  $. $GLOBUS_LOCATION/etc/globus-user-env.sh

- Client installation/configuration complete!

MyProxy Commands

- **myproxy-init**: store proxy
- **myproxy-get-delegation**: retrieve proxy
- **myproxy-info**: query stored credentials
- **myproxy-destroy**: remove credential
- **myproxy-change-pass-phrase**: change password encrypting private key

MyProxy CoG Clients

- Commodity Grid (CoG) Kits
  - Provide portable (Java and Python) MyProxy client tools & APIs
  - Windows support
- For more information:
  - http://www.cogkit.org/

MyProxy Server Administration

- Install server certificate and CA certificate(s)
- Configure /etc/myproxy-server.config policy
  - Template provided with examples
- Optionally:
  - Configure password quality enforcement
  - Install cron script to delete expired credentials
- Install boot script and start server
  - Example boot script provided
- Use myproxy-admin commands to manage server
  - Reset passwords, query repository, lock credentials

MyProxy Server Policies

- Who can store credentials?
  - Restrict to specific users or CAs
  - Restrict to administrator only
- Who can retrieve credentials?
  - Allow anyone with correct password
  - Allow only trusted services / portals
  - Set server-wide and per credential
- Maximum lifetime of retrieved credentials
  - Set server-wide and per credential

MyProxy and SASL

- MyProxy supports additional authentication mechanisms via SASL
- One Time Passwords (SASL PLAIN with PAM)
  - Protect against stolen passwords
  - Hardware token generates OTP
  - Authenticate with OTP plus MyProxy password
  - Tested with CryptoCard tokens
- Kerberos (SASL GSSAPI)
  - Authenticate with Kerberos ticket plus MyProxy password

Related Work

- GT4 Delegation Service
  - Protocol based on WS-Trust and WSRF
- SACRED Credential Repository
  - RFC 3767
- Kerberized Online CA (KX.509/KCA)
  - Kerberos -> PKI
- PKINIT for Heimdal Kerberos
  - PKI -> Kerberos

MyProxy Community Support

- myproxy-users@ncsa.uiuc.edu mailing list
- Bug tracking: http://bugzilla.ncsa.uiuc.edu/
- Anonymous CVS access

  :pserver:anonymous@cvs.ncsa.uiuc.edu:/CVS/myproxy
- Contributions welcome!
  - Feature requests, bug reports, patches, etc.

Thank you!

Contact:
http://myproxy.ncsa.uiuc.edu/
jbasney@ncsa.uiuc.edu

Questions/Comments?