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/

CACL

- 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/

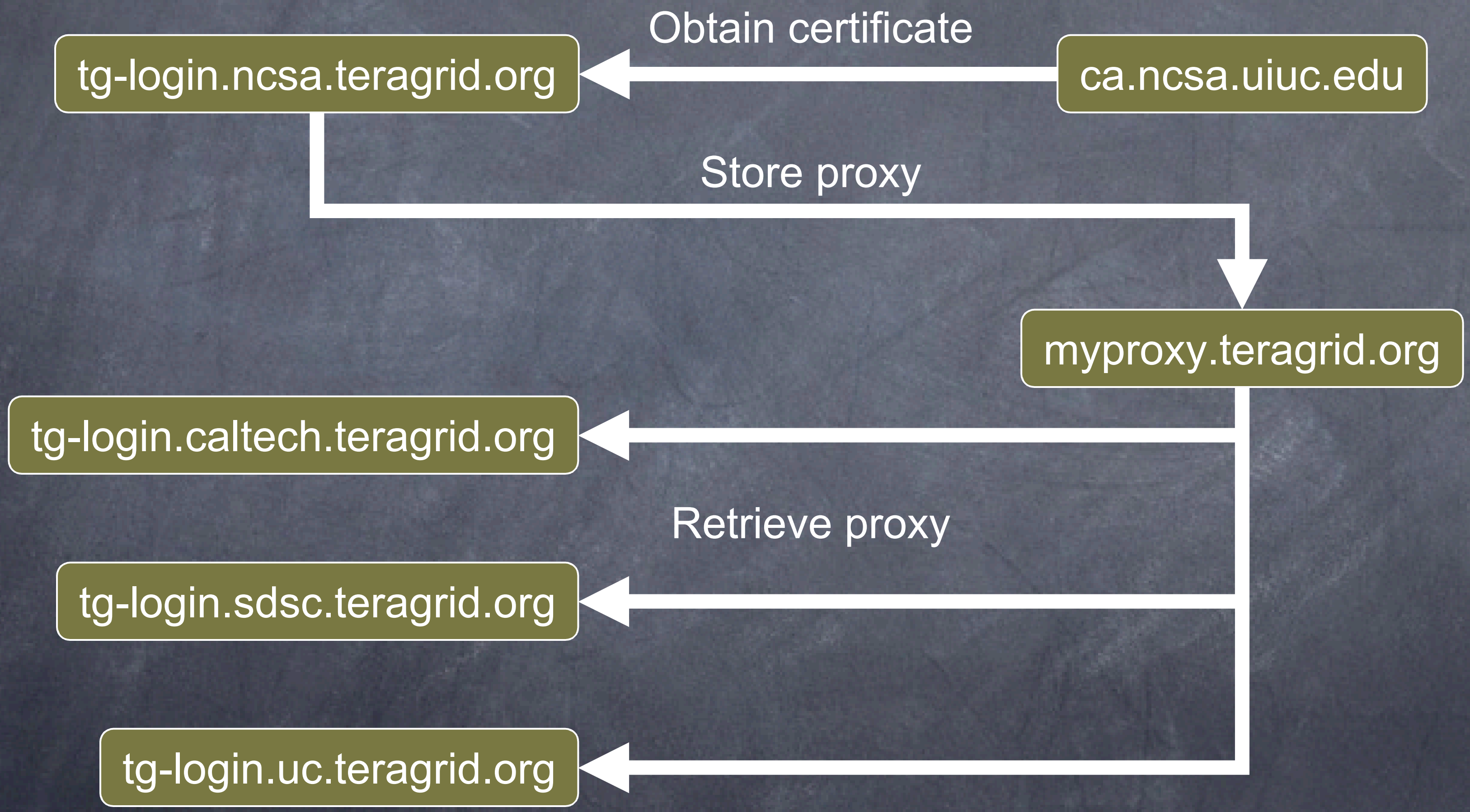
CAcert Online CA

- Free, comunity, 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



Obtain certificate

tg-login.ncsa.teragrid.org

ca.ncsa.uiuc.edu

Store proxy

myproxy.teragrid.org

tg-login.caltech.teragrid.org

Retrieve proxy

tg-login.sdsc.teragrid.org

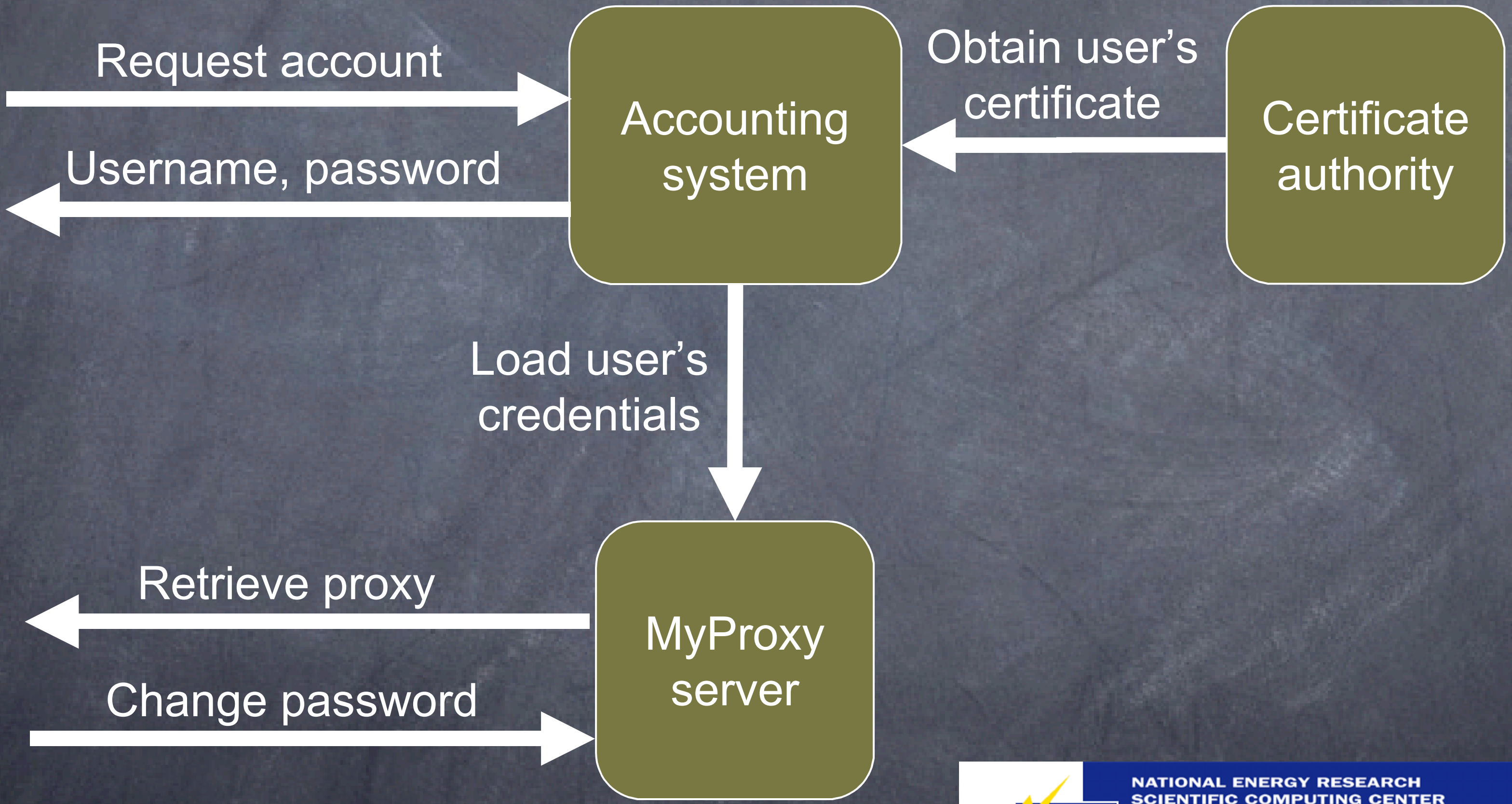
tg-login.uc.teragrid.org

TERAGRID

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

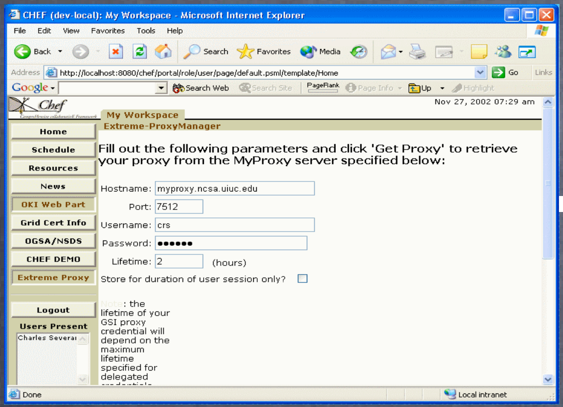
Credential Distribution via MyProxy



NERSC NATIONAL ENERGY RESEARCH SCIENTIFIC COMPUTING CENTER
Advancing Computational Science of Scale—Producing Real Results

INFORMATION POWER GRID
NASA'S COMPUTING AND DATA GRID

MyProxy and Grid Portals



Nov 27, 2002 07:29 am

My Workspace

Extreme-ProxyManager

Fill out the following parameters and click 'Get Proxy' to retrieve your proxy from the MyProxy server specified below:

Hostname: myproxy.ncsa.uiuc.edu

Port: 7512

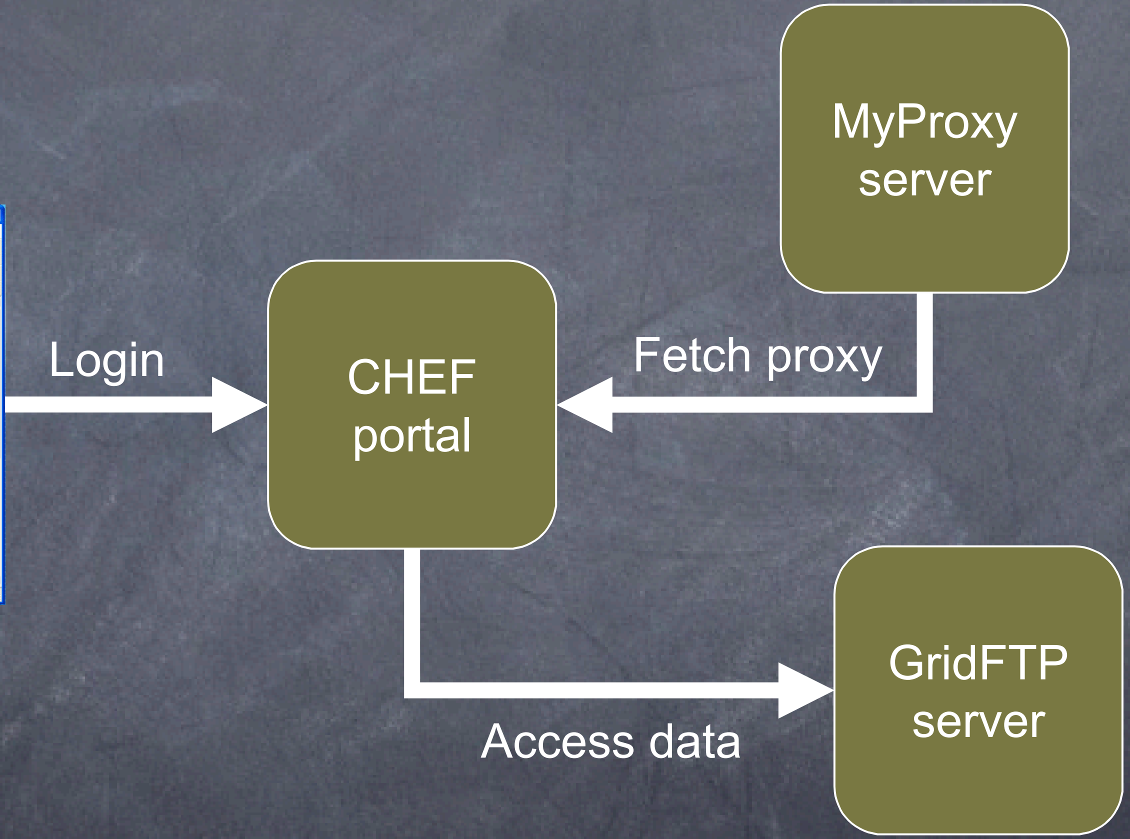
Username: crs

Password: ●●●●●●

Lifetime: 2 (hours)

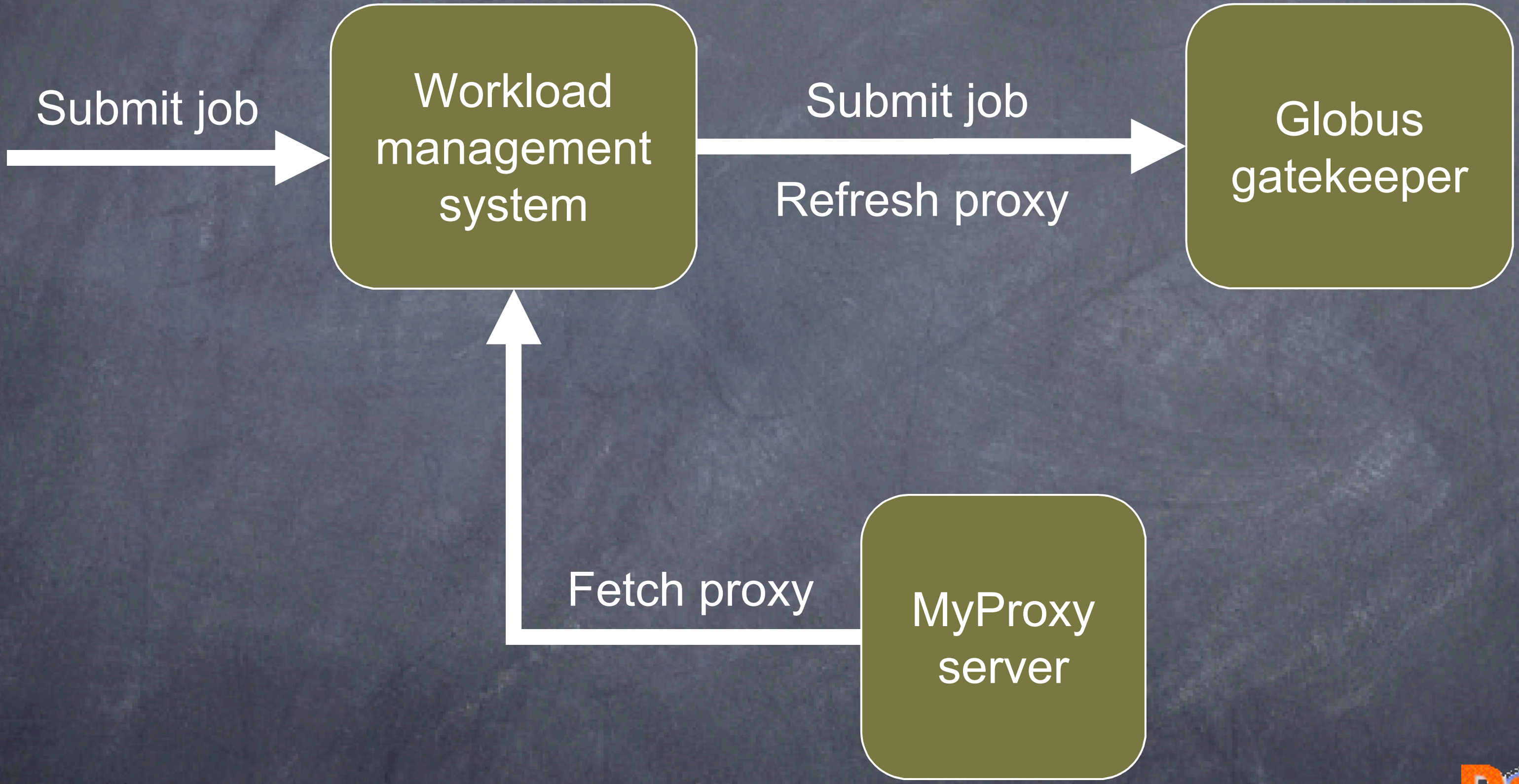
Store for duration of user session only? □

Note: the lifetime of your GSI proxy credential will depend on the maximum lifetime specified for delegated



NEESgrid

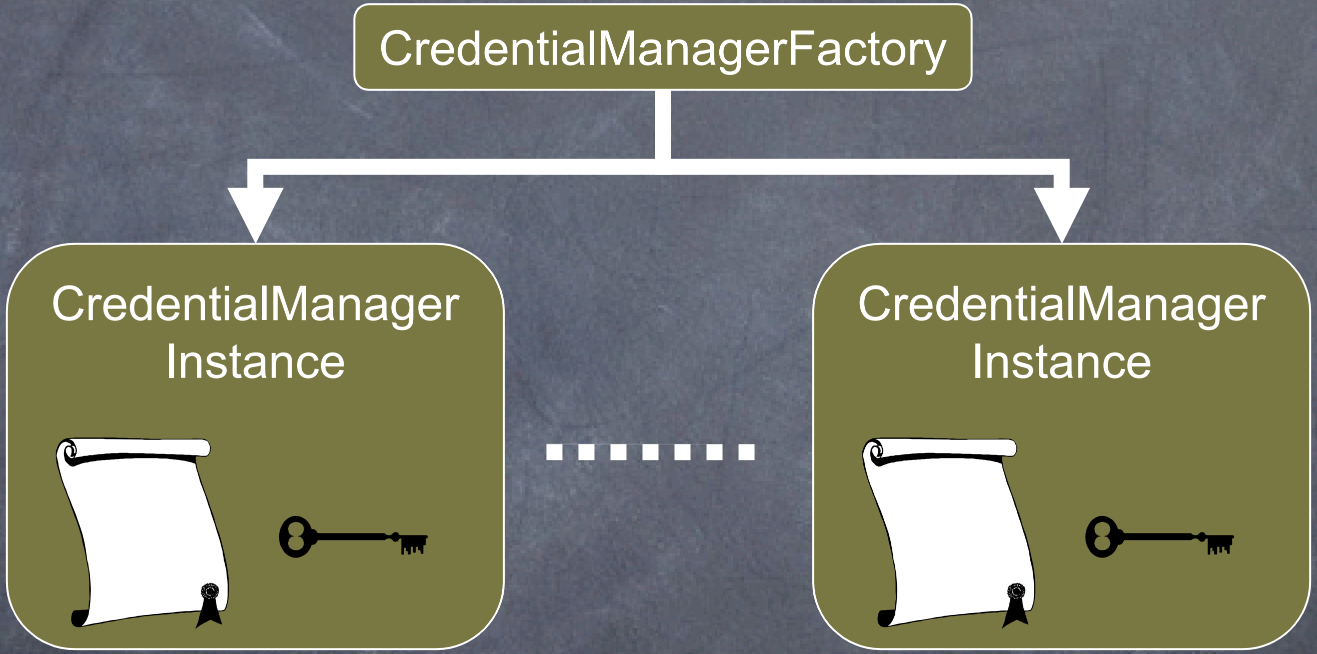
MyProxy and Credential Renewal



MyProxy Credential Renewal with Condor-G

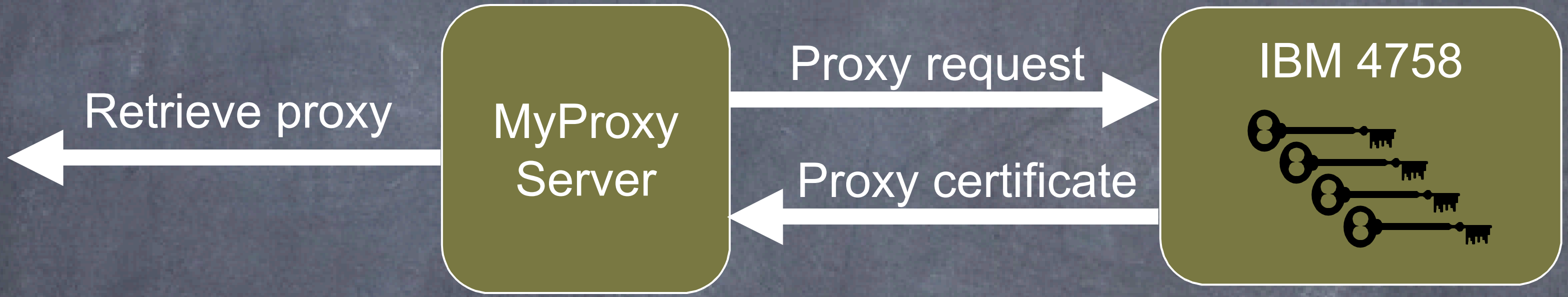
- Support added in Condor-G 6.7.0
- Include MyProxy information in Condor-G job submission file
- Condor-G retrieves fresh proxies on demand from MyProxy and delegates them to running jobs

MyProxy for OGSI



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

Hardware-Secured MyProxy



M. Lorch, J. Basney, and D. Kafura, "A Hardware-secured Credential Repository for Grid PKIs," 4th IEEE/ACM International Symposium on Cluster Computing and the Grid, April 2004.

Grid Logon

- Initialize grid security environment with secure password protocol
- Retrieve proxy credentials, CA certificates, CRLs, and authorization credentials
- Proposed work: http://www.ncsa.uiuc.edu/~jbasney/grid-logon.pdf

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