MyProxy

• A service for managing X.509 PKI credentials
  – A combined credential repository and certificate authority

• An Online Credential Repository
  – Issues short-lived X.509 Proxy Certificates
  – Long-lived private keys never leave the MyProxy server

• An Online Certificate Authority
  – Issues short-lived X.509 End Entity Certificates

• Supporting multiple authentication methods
  – Passphrase, Certificate, PAM, SASL, Kerberos

• Open Source Software
  – Included in Globus Toolkit 4.0
MyProxy Logon

• Authenticate to retrieve PKI credentials
  – End Entity or Proxy Certificate
  – Trusted CA Certificates
  – Certificate Revocation Lists

• MyProxy maintains the user’s PKI context
  – Users don’t need to manage long-lived credentials
  – Enables server-side monitoring and policy enforcement
    • For example: passphrase quality checks
  – CA certificates and CRLs updated automatically at login
MyProxy Online Credential Repository

• Stores X.509 End Entity and Proxy credentials
  – Private keys encrypted with user-chosen passphrases
  – Credentials may be stored directly or via proxy delegation protocol
  – Users can store multiple credentials from different CAs

• Access to credentials controlled by user and administrator policies
  – Set authentication requirements
  – Control whether credentials can be retrieved directly or if only proxy delegation is allowed
  – Restrict lifetime of retrieved proxy credentials
MyProxy and Grid Portals

1. Certificate Authority
2. MyProxy Server
3. USER'S SYSTEM 1
   Proxy obtained and used to interact with Grid Services directly
4. USER'S SYSTEM 2
   Standard web browser used with Web Portal, which obtains Proxy on behalf of user
5. Web Portal Server
6. GRID SERVICES
User Registration Portals

PURSE:
Portal-based User Registration Service

GAMA:
Grid Account Management Architecture
MyProxy Online Certificate Authority

- Issues short-lived X.509 End Entity Certificates
  - Leverages MyProxy authentication mechanisms
  - Compatible with existing MyProxy clients
- Ties in to site authentication and accounting
  - Using PAM and/or Kerberos authentication
  - “Gridmap” file maps usernames to certificate subjects
- Avoid need for long-lived user keys
- Server can function as both CA and repository
  - Issues certificate if no credentials for user are stored
Pluggable Authentication Modules

- Flexible, standard authentication mechanism
  - Specified by DCE RFC 86.0
  - Supported by Unix/Linux vendors

- Many available modules:
  - Authentication: Unix Password, One Time Password, Radius, Kerberos, AFS, LDAP, SQL, SMB, Netware
  - Access Control: Access, Deny, Filter, Tally, Time

- MyProxy server PAM support
  - Configure PAM authentication as sufficient or required
  - Create standard PAM configuration file for MyProxy
  - Compatible with existing MyProxy clients
Simple Authentication and Security Layer

• Authentication protocol framework
  – Specified by IETF RFC 2222
  – Used by LDAP, POP, and IMAP

• Supports multiple mechanisms:
  – PLAIN, DIGEST-MD5, GSSAPI, NTLM

• MyProxy support:
  – Configure available mechanisms for client and server
  – Tested with GSSAPI (Kerberos) and PLAIN

• Use Kerberos ticket to obtain PKI credentials from MyProxy
Example: LTER Grid Pilot Study

• Build a portal for environmental acoustics analysis

• Leverage existing LDAP usernames and passwords for portal authentication
  – Obtain PKI credentials for job submission and data transfer
  – Using MyProxy PAM LDAP authentication
Example: TeraGrid User Portal

- Use TeraGrid-wide Kerberos username and password for portal authentication
  - Obtain PKI credentials for resource access across TeraGrid sites via portal and externally
- Plan to use MyProxy CA with Kerberos PAM authentication
  - Leverage existing NCSA Online CA
Example: NERSC OTP PKI

• Address usability issues for One Time Passwords
  – Obtain session credentials using OTP authentication

• Prototyping MyProxy CA with PAM Radius authentication
  – ESnet Radius Authentication Fabric federates OTP authentication across sites
Conclusion

• **MyProxy leverages site authentication**
  – Using PAM and SASL to obtain PKI session credentials

• **MyProxy eases credential distribution**
  – User Registration Portals provide an interface for loading credentials into MyProxy
  – Online CA distributes credentials using existing MyProxy clients and authentication methods

• **For more information:**
  – jbasney@ncsa.uiuc.edu