GSI Credential Management with MyProxy

GGF8 Production Grid Management
RG Workshop
June 26, 2003

Jim Basney
jbasney@ncsa.uiuc.edu
http://myproxy.ncsa.uiuc.edu/
MyProxy

• Online repository of encrypted GSI credentials
• Provides authenticated retrieval of proxy credentials over the network
• Improves usability
  – Retrieve proxy credentials when/where needed without managing private key and certificate files
• Improves security
  – Long-term credentials stored encrypted on a well-secured server
MyProxy Software

- Server and client tools available from http://myproxy.ncsa.uiuc.edu/
  - GPT packages for Globus Toolkit 2.2 & 2.4
  - Also included in NMI Release 3.0 at http://www.nsf-middleware.org/
- Compatible client implementations also available in Commodity Grid Kits
  - http://www.globus.org/cog/
- Supported by Grid Portal toolkits
  - Grid Portal Development Kit (GPDK): http://doesciencegrid.org/projects/GPDK/
  - Grid Portal Toolkit (GridPort): https://gridport.npaci.edu/
  - Xportlet: http://www.extreme.indiana.edu/xportlet/project/
- OGSI development in progress
Grid Security Infrastructure

- **Credentials**
  - Asymmetric public/private key pair
  - X.509 certificate, signed by Certificate Authority, binds identity to key pair
- **Authentication (Who are you?)**
  - Proof of possession of private key
  - Verify CA signature on X.509 certificate
- **Authorization (What can you do?)**
  - Based on certificate identity
  - Can be mapped to local Unix account
Credential Management

- **Enrollment**: Initially obtaining credentials
- **Security**: Protecting credentials (private keys)
- **Accessibility**: Getting credentials when needed
- **Renewal**: Handling credential expiration
- **Translation**: Using existing credentials to obtain credentials for a new mechanism or realm
- **Delegation**: Granting specific rights to others
- **Control**: Monitoring and auditing credential use
- **Revocation**: Handling credential compromise
Issuing Credentials via MyProxy

• Generate credentials on user’s behalf and load into MyProxy repository
• Distribute MyProxy usernames and passphrases
  – Can use existing site usernames/passphrases
• Private key never leaves MyProxy repository
  – Proxy credentials delegated with configured max. lifetime
• Revoke credentials by removing from repository
• Provides a single point for focusing credential protection and usage monitoring
  – Enforce password policies
• Manage credentials on the user’s behalf
  – Renew credentials before they expire
  – Reset forgotten credential passphrase
Integrating MyProxy with CA

• Using Globus SimpleCA
  – myproxy-admin-adduser generates SimpleCA credentials and loads them into repository

• Using existing CA
  – Create credentials as usual
  – Load with myproxy-admin-load-credential

• MyProxy need not be the only method of credential issuance
  – Can continue to issue credentials directly to experts to manage themselves
Alternatives: Smart Cards

• An excellent solution but costly
  – User-managed, portable credential storage
  – Security analogous to car keys or credit cards
    • Must be re-issued when lost or stolen
  – Private keys stay in hardware
  – Cards can be distributed with credentials pre-loaded
  – Card standards are mature
  – Costs are decreasing but still significant
    • $20 readers, $2 cards
    • Government ID card deployments
  – Some support already in GSI libraries
• MyProxy provides a “virtual smart card”
  – When smart card support is not ubiquitous or is too expensive
Alternative: Online CAs

• A good solution with low administrative costs
  – User authenticates to online CA to obtain credentials immediately
    • No manual administrative approval required
  – Leverages existing authentication mechanisms (password, Kerberos, etc.)
  – Signs long-term or short-term credentials:
    • If long-term, then credentials are user-managed
    • If short-term, credentials retrieved on demand, without need for user key management
  – Examples: KCA and CACL

• MyProxy can be more flexible
  – Managing credentials from multiple CAs
  – In the future, managing multiple types of credentials
Credential Accessibility with MyProxy

- A MyProxy server can be deployed for a single user, a virtual organization, or a CA
- Users can delegate proxy credentials to the MyProxy server for storage
  - Can store multiple credentials with different names, lifetimes, and access policies
- Then, they can retrieve stored proxies when needed using MyProxy client tools
  - And allow trusted services to retrieve proxies
- No need to copy certificate and key files between machines
Delegation to Grid Portals

• Provide a web interface to Grid services
• Require credentials to act on user’s behalf
• Use MyProxy to delegate credentials to portal
Delegation to Grid Portals

Workstation → Load Credentials → Set Policies → Grid Portal → MyProxy Server

Username → Password → Grid Portal

Username → Password → Proxy Credential → MyProxy Server
Credential Renewal

• Long-lived tasks or services need credentials
  – Task lifetime is difficult to predict
• Don’t want to delegate long-lived credentials
  – Fear of compromise
• Instead, renew credentials with MyProxy as needed during the task’s lifetime
  – Provides a single point of monitoring and control
  – Renewal policy can be modified at any time
    • For example, disable renewals if compromise is detected or suspected
• Integration with Condor-G in progress
Credential Renewal

Submit Jobs

Home

Job Broker

Remote

Launch Job

Resource Manager

Refresh Credentials

Retrieve Credentials

Job

Enable Renewal

MyProxy

Refresh Credentials
MyProxy

• Provides a solution today for many GSI credential management issues
  – Enrollment
  – Private key security
  – Accessibility
  – Renewal
  – Passphrase-based delegation
  – Revocation and passphrase reset

• Work in progress
  – MyProxy OGSA Service
  – MyProxy Auditing
  – Credential Wallet for the Grid
MyProxy OGSA Service

• Credential manager factory
• Credential manager object leverages OGSI services
  – Query credential info via service data query
  – Remove credentials by destroying service instance
  – Monitor credential access via service notifications
  – Control credential access via standard service access control mechanisms
• Goal: A lightweight credential management service that can be easily instantiated when needed
• Good user interface is essential
MyProxy Auditing

• Develop standard OGSA audit service to which the MyProxy server logs activity

• Provide a secure query and notification interface
  – Credential owners can monitor use of their credentials and detect unauthorized use
  – Administrators can detect and investigate credential misuse
Credential Wallet for the Grid

• Provides an interface to my credentials
  – Multiple X.509 ID certificates, authorization credentials, CA certificates with CRLs
  – Supports multiple authentication mechanisms
  – Easily add, remove, modify credentials
  – Control credential access policies
  – Create authorization credentials for delegation
  – Receive event notifications

• Single sign-on unlocks wallet
  – Grid protocols negotiate for required credentials
  – Automatically retrieve needed credentials from wallet
Acknowledgements

• MyProxy Team (2002-2003)
  – NCSA: Shiva Shankar Chetan, Feng Qin, Zhenmin Li, Asita Anche, Vivek Sundaram, Praveen Appu
  – UVA: Marty Humphrey, Shaun Arnold, Dhiraj Parashar
  – Other authors/contributors: Jarek Gawor, Daniel Kouril, Jason Novotny, Miroslav Ruda, Benjamin Temko, Von Welch

• Financial Support