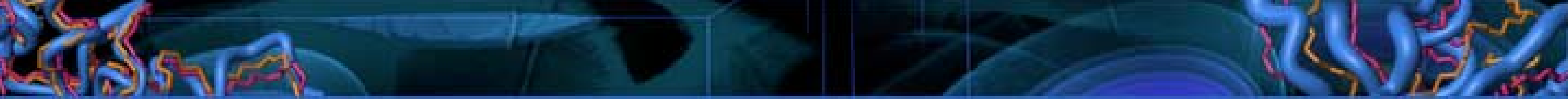


NCSA-IPG Collaboration Projects Overview

NASA IPG Workshop
February 6, 2003

Jim Basney

jbasney@ncsa.uiuc.edu
http://www.ncsa.uiuc.edu/~jbasney/

FY02 Deliverables

- **Grid Testbed**
  - Support for Grid computing between IPG and NCSA resources
    - SGI Origin 2000 and Intel Linux clusters
- **Grid Infrastructure Support and Development**
  - GSI-enabled OpenSSH
  - MyProxy Online Credential Repository

Grid Testbed Results

- **Support for Grand Challenge milestone**
  - Expedited NCSA account requests with grid-mapfile entries
  - Resolved problems encountered with Grid services at NCSA
  - Resolved compatibility issues
    - GRAM, GSISSH, GridFTP, MDS
  - Grid Information Services provided
    - NCSA resources reporting to IPG GIIS

GSI-enabled OpenSSH Overview

- **Secure single sign-on for remote login (ssh) and file transfer (scp/sftp)**
  - Adds GSI authentication and delegation to standard OpenSSH software
  - Co-exists with other SSH authentication mechanisms (password, host-based, ...)

GSISSH FY02 Results

- **NCSA supported since January 2002**
- **Packaged with Grid Packaging Tools (GPT)**
  - Support for Globus Toolkit 2.0 & 2.2
- **Tracked OpenSSH releases**
  - 3.0.2p1, 3.1p1, 3.2.3p1, 3.3p1, 3.4p1, 3.5p1
  - Support for privilege separation added
- **Added GSI authentication over SSH1 protocol for backward-compatibility**
- **Added implicit subject to login name mapping using grid-mapfile**
  - Don't need to remember different usernames at different sites

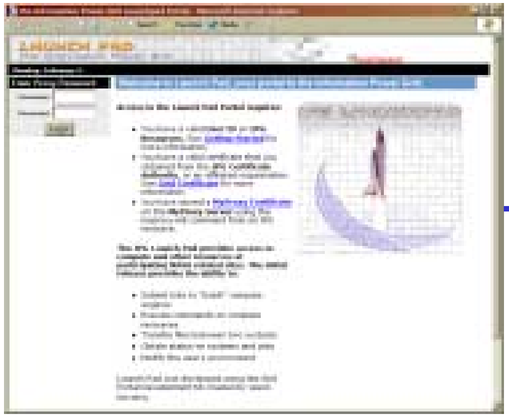
MyProxy Overview

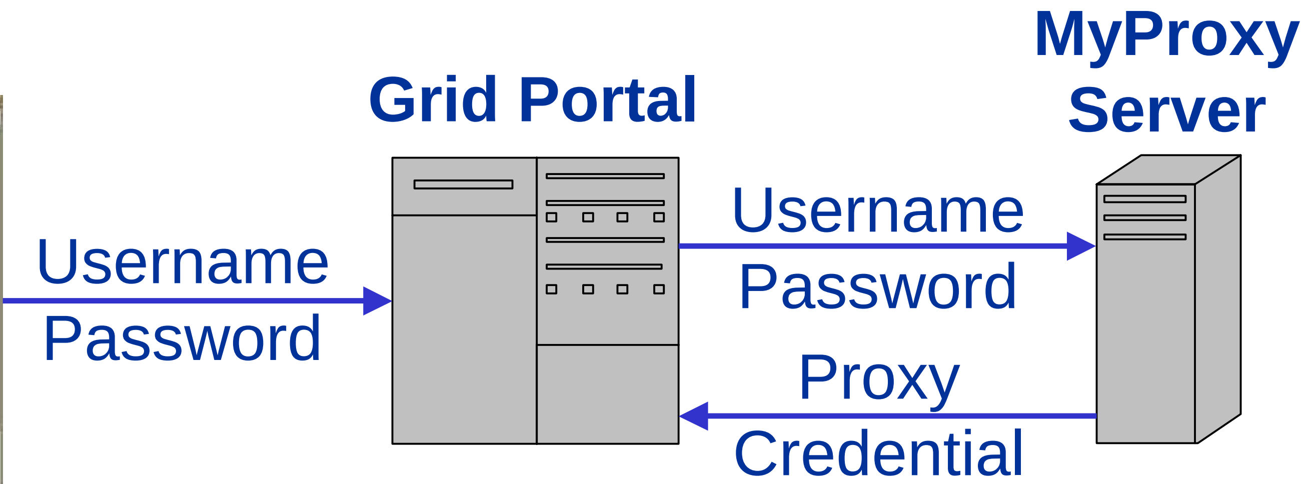
- **Online repository for Grid credentials**
  - – Credentials encrypted with user's passphrase
- **Allows Grid portals to retrieve credentials to act on your behalf**
  - – Used by LAUNCH PAD The Information Power Grid
- **Allows you to retrieve credentials when and where you need them**
- **Allows trusted services to renew your credentials when needed**

MyProxy FY02 Results

- **Packaged with Grid Packaging Tools (GPT)**
  - Support for Globus Toolkit 2.0 & 2.2
- **Added support for**
  - Users retrieving credentials directly
  - Storing multiple credentials per user
  - Per-credential access policies
  - Encrypting credentials in the repository
  - Credential renewal
- **Ongoing work**
  - Integration with Condor-G for credential renewal
  - Single sign-on to Grid portals
  - Support for storing long-term credentials with optional CA integration (myproxy-adduser)

Using MyProxy with Grid Portals





Username
Password

Grid Portal

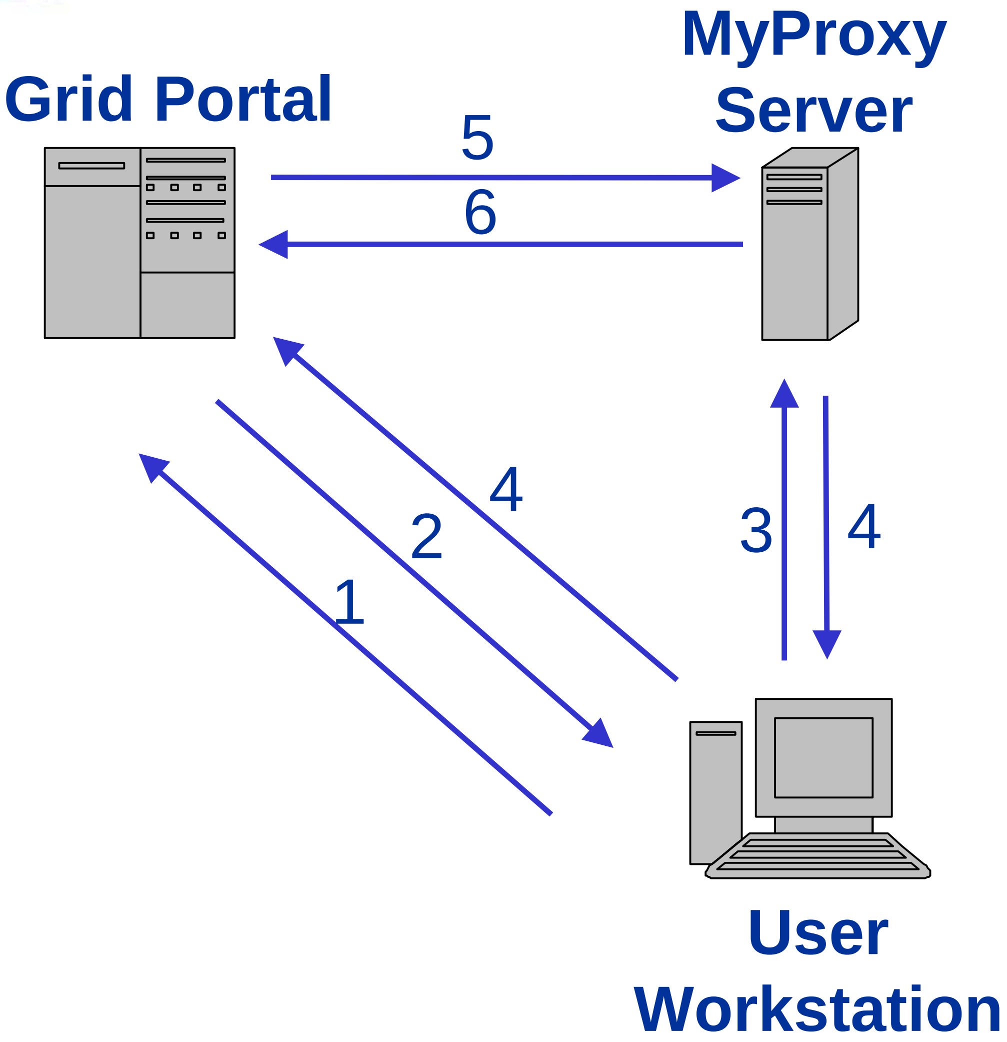
Username
Password

MyProxy Server

Proxy
Credential

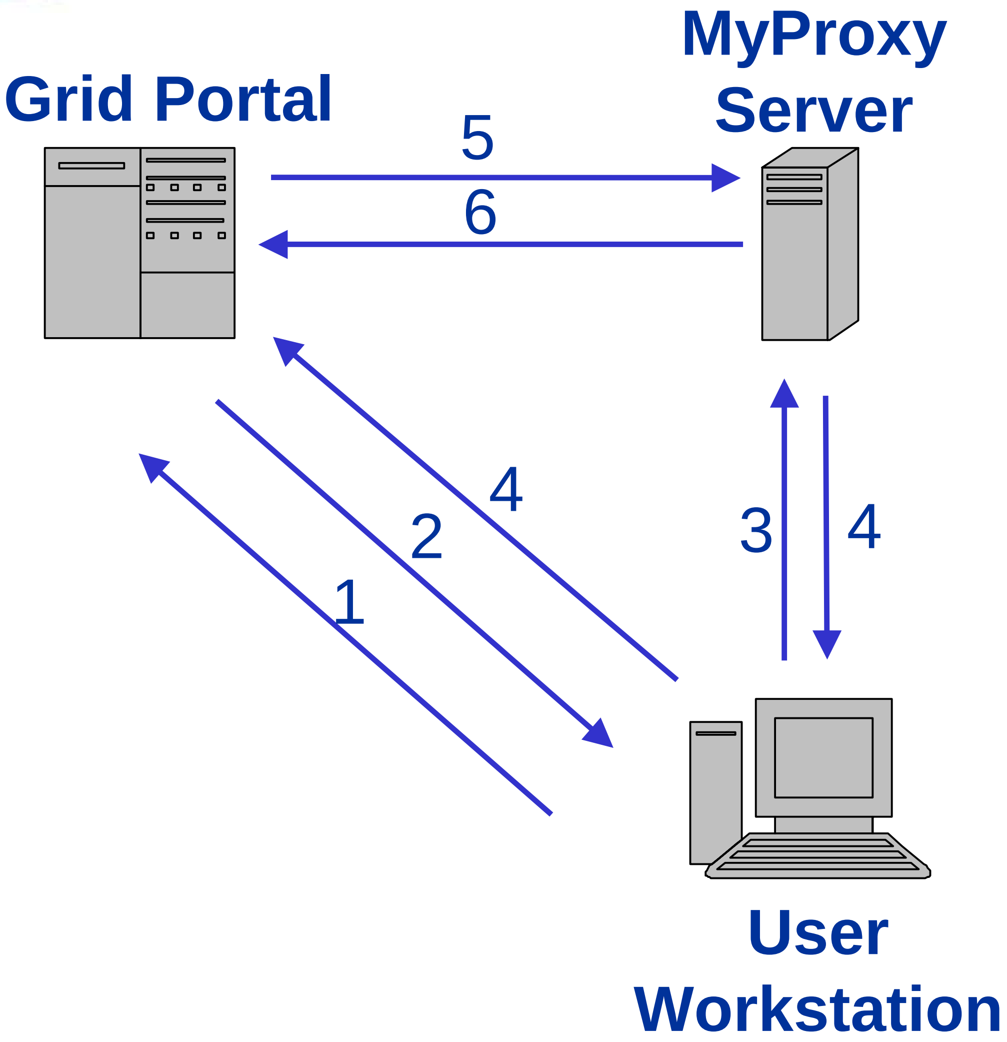
- **Drawbacks:**
  - – Sends password to portal
  - – Separate sign-on to each Grid portal

Secure Portal Sign-on with MyProxy



1. Visit portal
2. Redirect to MyProxy
3. MyProxy password-based login
4. Store MyProxy session cookie & redirect to portal with portal cookie
5. Portal authenticates with cookie
6. Portal retrieves credential

Web Single Sign-on with MyProxy



Grid Portal

MyProxy Server

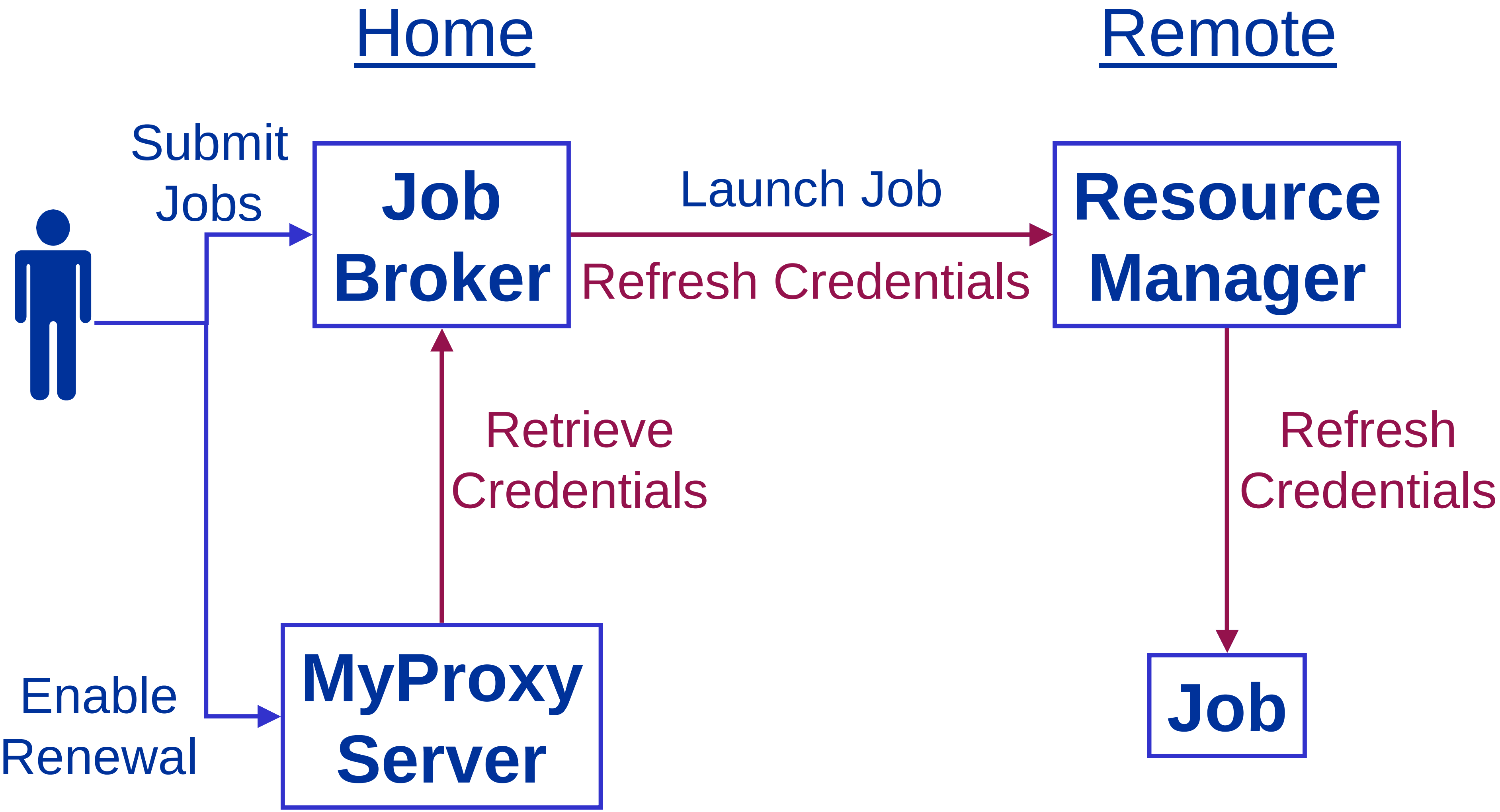
User Workstation

1. Visit another portal
2. Redirect to MyProxy
3. MyProxy login with session cookie
4. Redirect to portal with portal cookie
5. Portal authenticates with cookie
6. Portal retrieves credential

Credential Renewal

- **Long-lived jobs need credentials**
  - Job lifetime is difficult to predict
- **Don’t want to delegate long-lived credentials**
  - Fear of compromise
- **Instead, renew credentials as needed during the job’s lifetime**
  - Renewal service 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

Credential Renewal



Enterprise Credential Repository

- **Credentials generated and stored in online repository at account creation time**
  - Users retrieve short-term credentials when needed
  - Optionally allow experts to retrieve long-term credentials
- **Long-term credentials stored securely in repository**
  - Revoke credentials by removing from repository
  - Long-term credentials can be automatically renewed
  - Site-wide password policies can be enforced
  - Monitor repository to detect credential compromise
- **Unlike online CA, separates credential creation and management for more flexibility**

Managing Many Grid Credentials

- **Identity credentials**
  - Different mechanisms (X.509, Kerberos, .NET)
  - Different authorities (CAs, KDCs)
  - Different purposes (authentication, signing, encryption)
  - Different roles (project-based, security levels)
- **Authorization credentials**
  - X.509 attribute certificates
  - SAML/XACML/XrML assertions
- **Trusted credentials**
  - CA certificates and policies
  - Other certificates and public keys (SSH, PGP)

Credential Wallet

- **User interface to credential management**
  - Add, remove, or modify credentials
  - Associate policies with credentials
  - Create authorization credentials
  - Receive notification of events
- **One-stop credential access point**
  - Single sign-on unlocks credentials for a session
  - Retrieve short-term credentials into web browser
  - Contains pointers to available credential services
- **Manage credentials on my behalf**
  - Example: credential renewal