MyProxy:
A Multi-Purpose Grid Authentication Service

Jim Basney
Senior Research Scientist
NCSA
jbasney@ncsa.uiuc.edu

What is MyProxy?

- A service for managing X.509 PKI credentials
  - A credential repository and certificate authority
- An Online Credential Repository
  - Issues short-lived X.509 Proxy Certificates
  - Long-lived private keys never leave the 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, VDT, and CoG Kits
  - C, Java, Python, and Perl clients available
  - Contributions from EDG, UVA, LBNL, and others

the globus alliance
www.globus.org

NCSA

MyProxy Logon

- Authenticate to retrieve PKI credentials
  - End Entity or Proxy Certificate
  - Trusted CA Certificates
  - Certificate Revocation Lists (CRLs)
- MyProxy maintains the user's PKI context
  - Users don't need to manage long-lived credentials
  - Enables server-side monitoring and policy enforcement (ex. passphrase quality checks)
  - CA certificates & CRLs updated automatically at login

the globus alliance
www.globus.org

NCSA

MyProxy Authentication

- Key Passphrase
- X.509 Certificate
  - Used for credential renewal
- Pluggable Authentication Modules (PAM)
  - Kerberos password
  - One Time Password (OTP)
  - Lightweight Directory Access Protocol (LDAP) password
- Simple Authentication and Security Layer (SASL)
  - Kerberos ticket (SASL GSSAPI)

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
  - Map username to certificate subject via “gridmap” file or LDAP query
- Avoid need for long-lived user keys
- Server can function as both CA and repository
  - Issues certificate if no credentials for user are stored

MyProxy Online Credential Repository

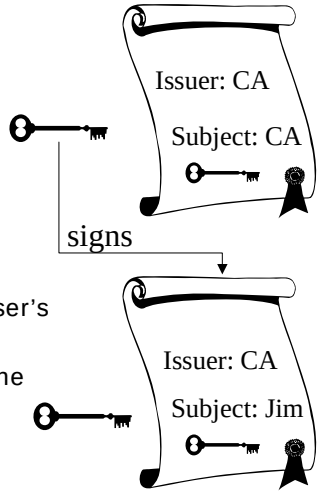
- Stores X.509 End Entity and Proxy credentials
  - Private keys encrypted with user-chosen passphrases
  - Credentials may be stored directly or via proxy delegation
  - Users can store multiple credentials from different CAs
- Access to credentials controlled by user and administrator policies
  - Set authentication requirements
  - Control whether credentials can be retrieved directly or if only proxy delegation is allowed
  - Restrict lifetime of retrieved proxy credentials
- Can be deployed for a single user, a site, a virtual organization, a resource provider, a CA, etc.

Talk Outline

- MyProxy Introduction
- PKI Introduction and MyProxy CA
- Proxy Certificates and MyProxy Repository
- MyProxy Scenarios
  - Administratively Loaded Credentials
  - Registration Portals
  - Web Portal Authentication and Delegation
  - Password-based Delegation
  - Credential Renewal
  - Web Single Sign-On (SSO)
- Demos
- Conclusion

PKI Overview

- Public Key Cryptography
  - Sign with private key, verify signature with public key
  - Encrypt with public key, decrypt with private key
- Key Distribution
  - Who does a public key belong to?
  - Certification Authority (CA) verifies user's identity and signs certificate
  - Certificate is a document that binds the user's identity to a public key
- Authentication
  - Signature [h (random, …)]



the globus alliance
www.globus.org

NCSA

PKI Authentication

Standard SSL/TLS Protocol (summarized)

Client — Server

$random_c$ →

← $certificate_s + random_s$

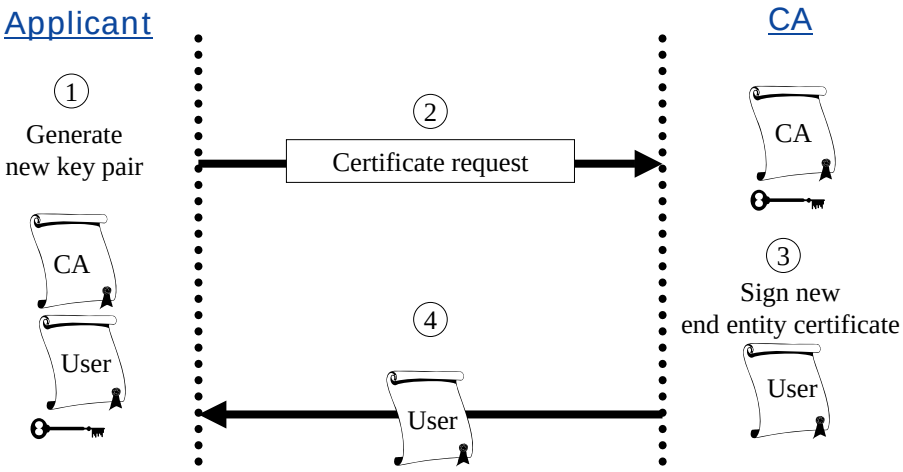
$certificate_c + \{ secret \}_{pubkey_s}$
$+ signature_c[h(random_c, random_s, \ldots)]$ →

← $\{ h(secret) \}_{secret}$

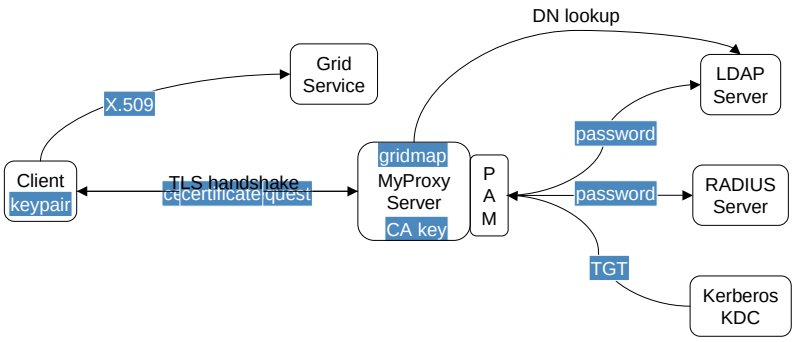
the globus alliance
www.globus.org

NCSA

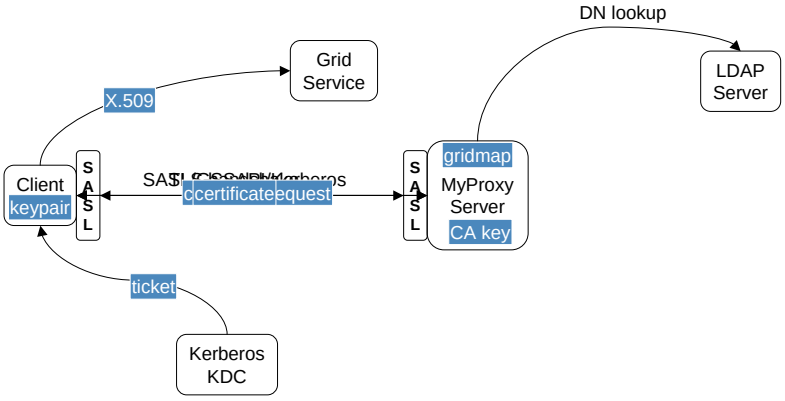
PKI Enrollment



MyProxy CA with PAM



MyProxy CA with Kerberos

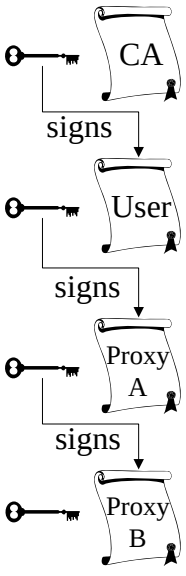


PAM/SASL Issues

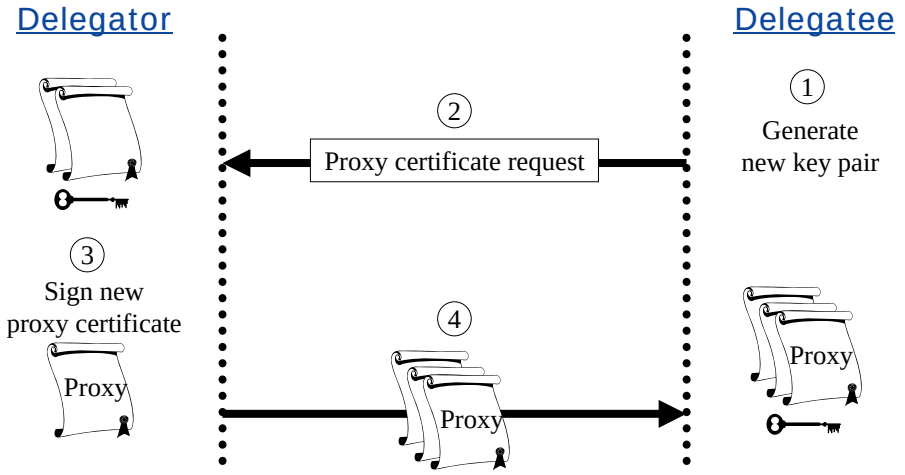
- PAM Conversation
  - PAM modules can require multiple rounds of user interaction
  - No standard protocol
    - SASL/PLAIN doesn't support multiple rounds
    - Need something like SSH keyboard-interactive protocol
- SASL client-side setup
  - Requires SASL library and configuration of SASL mechanisms
  - Alternative: native Kerberos protocol support

Proxy Credentials

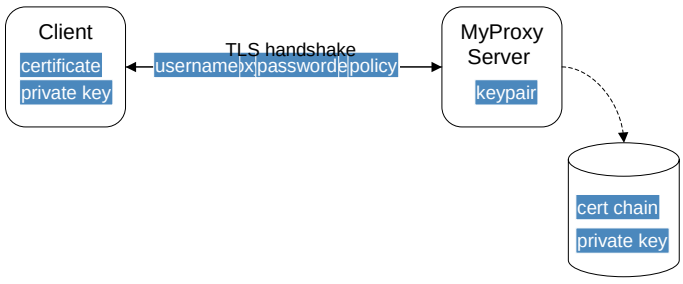
- RFC 3820: Proxy Certificate Profile
- Associate a new private key and certificate with existing credentials
- Short-lived, unencrypted credentials for multiple authentications in a session
  - Restricted lifetime in certificate limits vulnerability of unencrypted key
- Credential delegation (forwarding)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



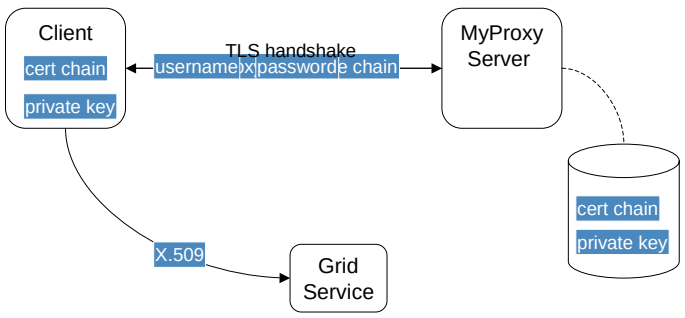
Proxy Delegation



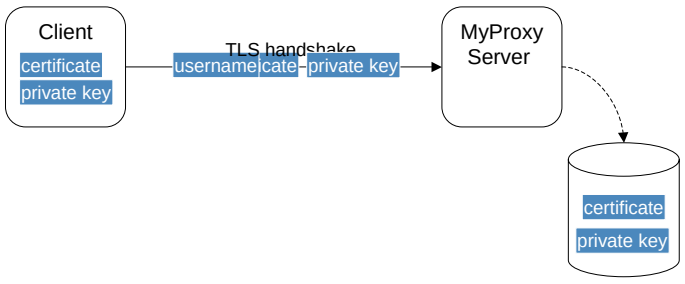
MyProxy Put



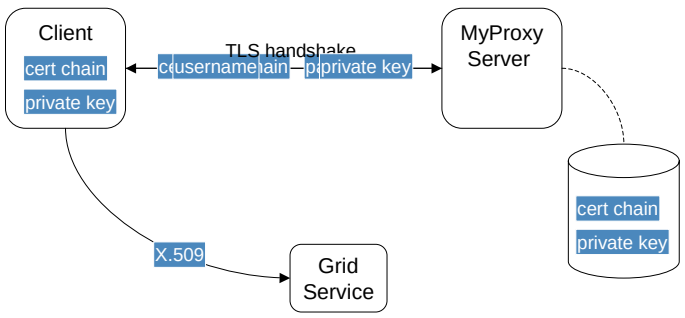
MyProxy Get



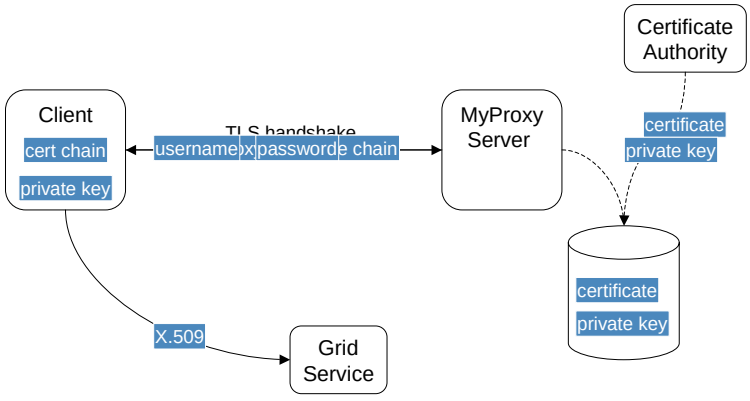
MyProxy Store



MyProxy Retrieve



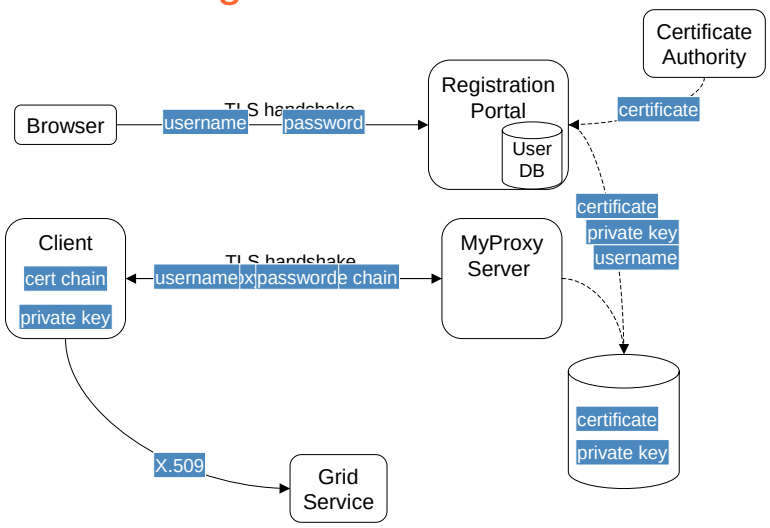
Administratively Loaded Creds



the globus alliance
www.globus.org

NCSA

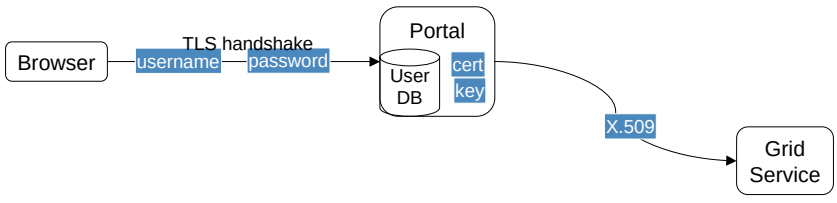
User Registration Portal



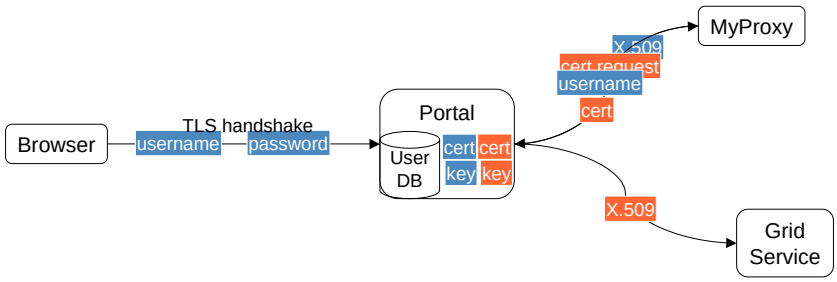
the globus alliance
www.globus.org

NCSA

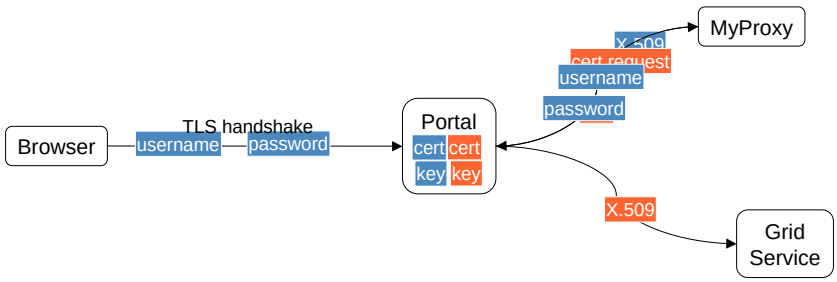
Gateway Portal



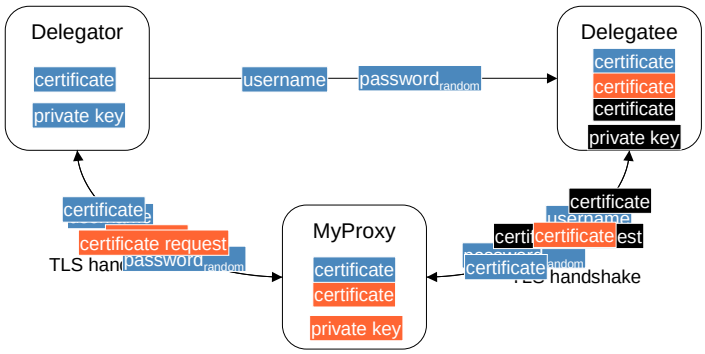
Trusted Portal



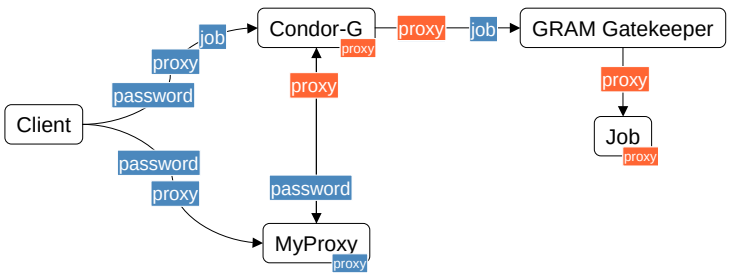
Password-based Portal Auth



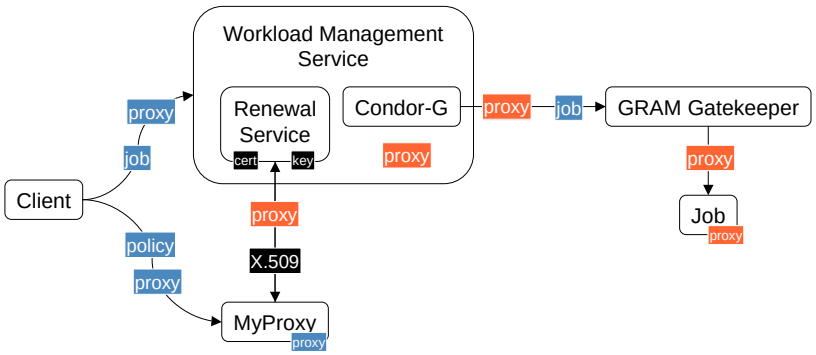
Password-based Delegation



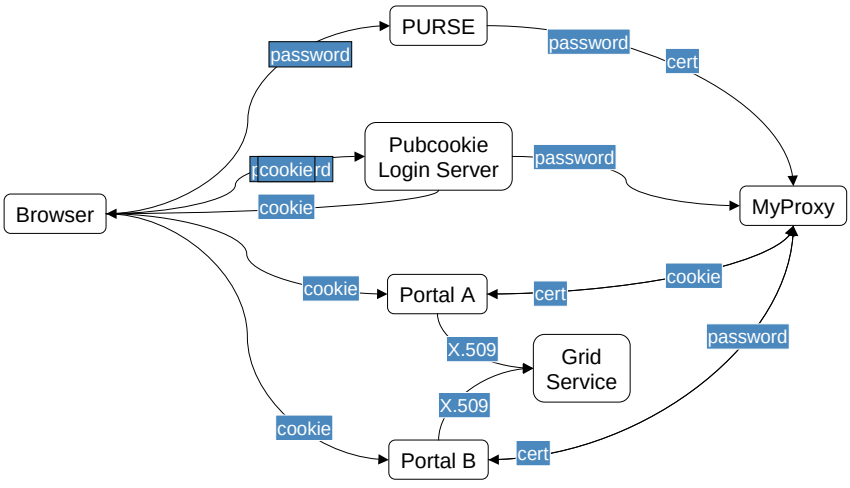
Password-based Renewal



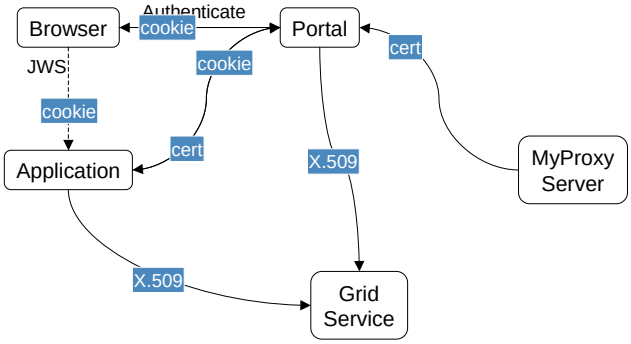
Certificate-based Renewal



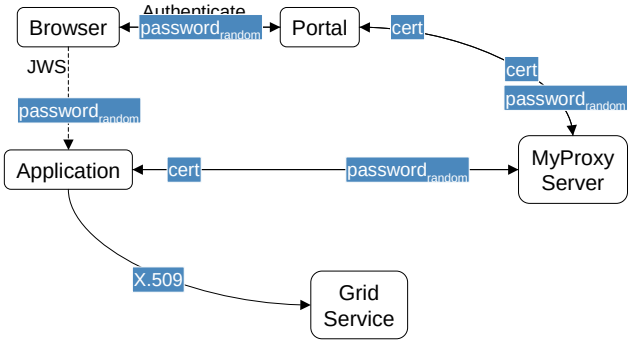
MyProxy and Web SSO



SSO for Browser and Application



SSO for Browser and Application



the globus alliance
www.globus.org

NCSA

Demonstrations

the globus alliance
www.globus.org

NCSA

Conclusion

- MyProxy: A Multi-Purpose Grid Authentication Service
  - Used in many delegation and single sign-on scenarios
- MyProxy provides practical authentication solutions
  - Minimize changes to existing software and protocols
  - Leverage community standards
    - PAM, SASL, Kerberos, LDAP, Pubcookie, Shibboleth
- Active MyProxy open source community
  - Deploy new developments via MyProxy
  - Benefit from the work of others

the globus alliance
www.globus.org

NCSA