MyProxy Development Plan
Jim Basney
October 4, 2001

1. Overview

MyProxy allows users to delegate their GSI credentials to web portals, so the portals can access Grid resources on the user's behalf (i.e., to submit jobs, transfer files, and access information services). This development plan extends MyProxy to a more general-purpose online credential repository (OCR).

The goal of the OCR is to improve the usability of GSI credentials without sacrificing security. The OCR can make the use of GSI credentials more transparent to novice users while giving additional functionality to advanced users.

2. Milestones and Deliverables

2.1. End-Entity Proxy Retrieval – October 2001

This feature allows users to retrieve a proxy credential from the MyProxy server using their MyProxy username and passphrase. Users no longer need to manually copy their GSI credentials to the different computers from which they access Grid resources and therefore do not leave copies of their credentials on multiple systems. Once the user uploads a proxy credential to the MyProxy server from the computer where his or her GSI credentials are installed, he or she can obtain a proxy credential from any computer on the Grid where the MyProxy client software is installed.

MyProxy currently requires mutual authentication between client and server for all transactions. The client must have a valid GSI credential with a subject name that matches a list of allowed services (i.e., portals) in a MyProxy server configuration file to download a proxy credential. This requirement must be relaxed to support end-entity proxy retrieval. A form of mutual authentication will still be required: clients will authenticate to the server with the username and passphrase and servers will authenticate to the clients (as before) with the server's GSI credential. Support for this feature should be optional in MyProxy servers.

2.2. Packaged MyProxy Client Distribution – November 2001

We plan to package the MyProxy software to improve ease-of-installation and promote deployment. MyProxy software should be included in Globus and Alliance Grid-in-a-Box distributions. We hope system administrators will install the MyProxy client software on the sites where users want to use it. However, it should also be easy for a novice user to download and install the client software for personal use on an end-system when needed. For example, when a user wants to access Grid resources from a system where neither the user's GSI credentials nor the MyProxy client software is installed, our goal is for the user to find it easier to download and install the MyProxy client software on that system instead of manually copying his or her GSI credentials to the system.

2.3. Unattended Proxy Renewal – November 2001

Users should be able to submit long-running jobs and jobs to execute sometime in the future without delegating long-lived proxy credentials to a scheduler. We plan to extend MyProxy to support a proxy renewal service, to allow users to delegate short-term proxies to schedulers to be renewed only as needed, under the watchful eye of MyProxy. Support for renewal can be enabled or disabled on a per-credential basis on the MyProxy server.

To support renewal, the MyProxy server will allow clients to authenticate with a current proxy credential and retrieve a new proxy with the same subject. Schedulers or applications will periodically run a MyProxy client program (or call a function in the MyProxy client API) to renew the current proxy credential before it expires. We will work with the CondorG developers to include support for proxy renewal via MyProxy in CondorG.

2.4. Kerberos Authenticated Proxy Retrieval – December 2001

This feature allows clients to authenticate to the MyProxy server with their Kerberos credentials to retrieve a GSI proxy credential. For example, this will allow users to include a call to a MyProxy client program in their login script to transparently retrieve a proxy credential when they perform a Kerberos login, giving the user a single sign-on to both the local Kerberos realm and the Grid.

Kerberos-authenticated access to proxy credentials will be configured on a per-credential basis, when the proxy is originally delegated to the MyProxy server.

2.5. Standardization

We plan to standardize a protocol for retrieving GSI credentials from an OCR and a method for storing GSI credentials in an OCR in the Global Grid Forum GSI working group.

2.5.1. GSI OCR Protocol Requirements First Draft – October 2001

2.5.2. GSI OCR Protocol Requirements Second Draft – February 2002

2.5.3. GSI OCR Protocol Standard First Draft – February 2002

3. Additional Features Under Consideration

Milestones have not yet been assigned for the following features. Each feature will be moved to the section above when a milestone for it has been set.

3.1. Scalable Repository Architecture

MyProxy should be modified to use a scalable database backend for credential storage. This will enable replication of the credential repository and support efficient query operations for finding the right credential when multiple credentials per user are supported.

3.2. Logging

Operations on the MyProxy server should be securely logged to enable auditing and troubleshooting. Administrators should have secure access to the logs, and users should be able to query the logs for transactions involving their credentials. A query interface for novice users (i.e., not SQL) should be supported.

3.3. Per-Credential Access Control

On credential upload, clients should be able to specify the identities and authentication methods that can be used to later retrieve the credential.

3.4. Multiple Credentials Per User

Users should be able to delegate multiple credentials to the OCR and retrieve the appropriate credential when needed. Support for browsing or querying the attributes of the credentials in the repository can help automate the search for the right credential.

3.5. X.509 Restricted Delegation

The MyProxy client utilities should support delegating restricted proxy credentials to the MyProxy server when a standard for X.509 restricted delegation has been established.

3.6. Community Authorization Service (CAS)

The OCR should interoperate with CAS, and the two development efforts should share a common code-base and protocols where possible.