

Proposal for Usability Enhancements to DOEGrids PKI
and a
Pilot Deployment of One-Time-Password access for Grid Proxy Generation using MyProxy

Contacts– Doug Olson, [dlolson@lbl.gov](mailto:dolson@lbl.gov) and Deb Agarwal, DAAgarwal@lbl.gov

Task 1: Usability Enhancements to DOEGrids PKI

There are two significant deficiencies with the usability of the DOEGrids PKI; a lack of command-line user interface and a lack of roaming capability for grid users.

The user interface provided by DOEGrids is web-based which is appropriate if the intended use of the signed certificates is to authenticate web-based interactions. For typical grid use the certificate needs to be stored in a user's home filesystem and accessible to command-line grid tools, meaning it must be extracted from a web browser and reformatted to be suitable for grid use. To overcome these limitations a number of examples of command-line scripts have been developed in the community that interface to the some of the web-based CA interfaces. One example of these scripts was published by PPDG¹. This example does not include the "grid admin" interface which enables authorized personnel to request and immediately retrieve service certificates necessary for identifying computers and services running on those computers.

Part A: It is proposed that a complete set of command-line user interface scripts be supported for DOEGrids by developing a "grid admin" script using the existing PPDG scripts as a basis.

In a classical PKI infrastructure used by most of the grid work in the PPDG & OSG communities, users are authenticated by access to a private key stored in their home filesystem. If a user needs to initiate grid actions away from their home filesystem they must either copy their certificate with private key to the new location or have stored a medium-lifetime proxy certificate in a myproxy server that can be accessed from any location to provide a standard short-lifetime proxy certificate for grid use. The myproxy server enables "roaming access" to the users' grid credentials, meaning the user's private key stays in one location and is used to generate the medium-lifetime certificate stored on the myproxy server.

Part B: It is proposed to deploy a MyProxy² server as a supported DOEGrids service with the same scope of allowed users as the DOEGrids CA.

Task 2: Pilot Deployment of One-Time-Password Authenticated MyProxy Service

There are a large variety of issues in the domain of cybersecurity for scientific computing. One example analysis of the issues is listed in the report from a recent HEP Cybersecurity Workshop³. We can advance work on one aspect of the problem of user credential management and to leverage the existing ESnet Radius testbed infrastructure.

We propose to add a Radius server PAM module to the MyProxy server described in Task 1B that will authenticate with an existing Cryptocard server (via Radius). In addition we will identify up to 20 people for whom we will issue Cryptocard tokens who can then use these tokens for One-Time-Password access to the MyProxy server for the purpose of generating short-lifetime grid proxy certificates. After 6 months of usage we will write a report of recommendations regarding the feasibility and deployment considerations for a large-scale deployment.

¹ <http://www.ppdg.net/RA/cert-scripts/>

² <http://grid.ncsa.uiuc.edu/myproxy/>

³ <http://hpcrd.lbl.gov/HEPCybersecurity/>