November 19, 2008

Scott Koranda
The Authentication and Authorization Subcommittee of the LIGO Computing Committee
University of Wisconsin-Milwaukee
P.O. Box 413, 2200 E. Kenwood Blvd.
Milwaukee, WI 53201-0413

Dear Scott,

On behalf of myself and the DOE Grids Policy Management Authority (PMA) we appreciate the opportunity to assist LIGO in developing a new authentication and authorization infrastructure. Supporting a distributed user community, both economically and effectively, is a challenging undertaking that entails a careful consideration of constraints and options. It is clear from the documents prepared by the LIGO Computing Committee that LIGO committed considerable effort towards designing its new infrastructure.

Over the last several weeks I, Jim Basney, Mike Helm, and Dhivakaran Muruganantham have enjoyed discussing with you alternative ways of managing certificates; principally methods involving a MyProxy server in conjunction with either the present DOE Grids Certificate Service or a possible future DOE Grids Short-Lived Credential Services (SLCS). In your document *Which Certificate Authority Should LIGO Use?* (August 15, 2008, LIGO DCC T080174-00-Z) you identify the three issues which would raise concerns for The America's Grid Policy Management Authority (TAGPMA):

1. **The MyProxy server would generate public/private key pairs on behalf of LIGO users, and issue a certificate request**. The DOE Grids PMA appreciates the inconvenience experienced by LIGO users in managing their private keys and certificates. Certificates are not intuitive to most computer users and the tools for managing and utilizing certificates in a grid computing environment are primitive.

   The DOE Grids Policy Management Authority (PMA) is bound by its accreditation from the International Grid Trust Federation (IGTF). The IGTF *Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure Version 4.2* Section 1 states "… end-entities, who will themselves posses and control their key pair and their activation data." Permitting another tool such as a MyProxy server to manage the key pair would be in direct conflict with this Authentication Profile.

   The DOE Grids PMA has no ready solution to this conflict.

2. **The MyProxy server would store the user's private key unencrypted.** Here the conflict lies with DOE Grids own Certificate Policy (CP) / Certificate Practice Statement (CPS) Version 2.10 Section 2.1.1 Subscriber Obligations which states "...Always using the pass phrase to encrypt the stored private key ...."

Fortunately, International Grid Trust Federation (IGTF) *Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure Version 4.2* provides some flexibility regarding the protection of the private key. Section 3 only states "The private key associated with any certificate must not be disclosed to or shared with end-entities other than the one to which the certificate was issued." The IGTF Authentication Profile does not specify the protections that must be applied to the private key.

The DOE Grids PMA itself has noted that Section 2.1.1 is overly specific. For example, smart cards and other tokens can be used to store private keys yet it is not clear that these devices employ encryption to protect the private keys. The DOE Grids PMA will pursue revising its CP/CPS to permit users greater flexibility in protecting their private keys.

3. **System administrators of the MyProxy server would have access to the users' private keys.** Again, the DOE Grids Policy Management Authority (PMA) is bound by its accreditation from the International Grid Trust Federation. The IGTF Authentication Profile Section 3 states "The private key associated with any certificate must not be disclosed to or shared with end-entities other than the one to which the certificate was issued." Allowing the MyProxy server system administrators to have access to the end user's private keys would be in conflict to DOE Grids accreditation.

   The DOE Grids PMA has no simple solution to the MyProxy server's need to store private keys in an unencrypted format.

In summary DOE Grids is unable to provide an end-user certificate service that would support the MyProxy infrastructure being architected by the LIGO Authentication and Authorization Subcommittee of the LIGO Computing Committee. Two of LIGO's requirements directly conflict with requirements of DOE Grids accreditation authority, The America's Grid Policy Management Authority.

Perhaps DOE Grids could provide other forms of certificate services, non-end user services, to LIGO. Alternatively, DOE Grids has been actively contemplating the issues involved in authenticating distributed users to distributed resources. DOE Grids has been studying technologies such as Shibboleth and OpenID, seeking methods that alleviate distributed users of the burdens of managing multiple credentials. DOE Grids would like to pursue opportunities to work with LIGO in investigating and perhaps deploying solutions based on these federated authentication models.

If you have any questions, comments, or would like to continue discussing LIGO's needs and how DOE Grids can participate, please contact either myself or Mike Helm.

Regards

John Volmer
Chairman, DOE Grids Policy Management Authority