IGI PUBLISHING **ITJ 4918**

701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Grid and High Performance Computing, Volume 1, Issue 2
edited by **Emmanuel Udoh and Frank Zhigang Wang © 2009, IGI Global**

Interoperable PKI Data Distribution in Computational Grids

Massimiliano Pala, Dartmouth College, USA

Shreyas Cholia, Lawrence Berkeley National Laboratory, USA

Scott A. Rea, Dartmouth College, USA

Sean W. Smith, Dartmouth College, USA

ABSTRACT

One of the most successful working examples of virtual organizations, computational grids need authentication mechanisms that inter-operate across domain boundaries. Public Key Infrastructures (PKIs) provide sufficient flexibility to allow resource managers to securely grant access to their systems in such distributed environments. However, as PKIs grow and services are added to enhance both security and usability, users and applications must struggle to discover available resources-particularly when the Certification Authority (CA) is alien to the relying party. This article presents how to overcome these limitations of the current grid authentication model by integrating the PKI Resource Query Protocol (PRQP) into the Grid Security Infrastructure (GSI). [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Authentication; PKI; PRQP; Resource Discovery*

AUTHENTICATION IN VIRTUAL ORGANIZATIONS

Computational grids provide researchers, institutions and organizations with many thousands of nodes that can be used to solve complex computational problems. To leverage collaborations between entities, users of computational grids are often consolidated under very large Virtual Organizations (VOs).

Participants in VOs need to share resources, including data storage, computational power and network bandwidth. Because these resources are valuable, access is usually limited, based on the requested

resource and the requesting user's identity. In order to enforce these limits, each grid has to provide secure authentication of users and applications.

Erroneously granting access to unauthorized or even malicious parties can be dangerous even within a single organization---and is unacceptable in such large VOs.

Moreover, the dynamic nature of grid VOs requires the authentication mechanisms to be flexible enough to easily allow administrators to manage trust and quickly re-arrange resource-sharing permissions. Indeed, VOs are usually born from the aggregation of already existing organizations and constitute an umbrella that groups the participating organizations rather than replacing them. Authentication must allow individual organizations to maintain control over their own resources.

The Problem. When participating in a VO, an organization must solve the problem of securely identifying resource requesters that come from outside its boundaries. PKIs offer a powerful and flexible tool to solve the potential authentication nightmare. Nonetheless, grid and VO administrators are still striving to find an acceptable solution to address interoperability issues that originate from the way VOs differ in policies, infrastructures and resource control.

Consider the situation where access to grid resources is managed via a Web portal. SSL mutual authentication can be enabled at the portal to implement strong authentication based on grid-approved PKI credentials. To do this, the portal administrator needs to set up the SSL Trust List to only allow credentials from approved CAs; the portal also needs to know how to validate the entire trust chain for that credential (that is, the end entity certificate presented, its issuer and the issuer's issuer, and so forth) up to the approved self-signed grid trust anchor.

To do this validation, the portal needs to know how to access services such as the location of the CA certificate and revocation data for each of these intermediate CAs. However, the portal cannot count on having pre-configured details for them. Even if it did---or if the information was packaged in each end entity certificate---this information may change over time, rendering this critical data stale. Having some way to dynamically discover service entry points of interest for grid-approved authorities (or indeed, the very authorities themselves) would solve a number of issues and would also provide for more flexible implementation options for the grid authorities, potentially lowering the costs of future service changes, and facilitating the future offering of additional services.

Our Proposed Solution. In order to help VOs to more efficiently address PKI interoperability issues we propose the adoption of the *PKI Resource Query Protocol* (PRQP) which enables discovery of resources and services in inter and intra PKI environments. We also propose an enhancement to the PRQP and we discuss its integration into the Grid Security Infrastructure (GSI).

AUTHENTICATION IN GRIDS

According to Ian Foster, a *grid* is a system that "coordinates resources that are not subject to centralized control, using standard, open, general-purpose protocols and interfaces, to deliver nontrivial qualities of service" (I. Foster, 2002). In order for the grid computing model to be successful, users and VOs must access a wide variety of