Contribution ID: **95**                                    Type: **Oral Presentation**

# Federated Access to Grids

*Tuesday, 12 April 2011 14:30 (30 minutes)*

## URL

http://www.project-moonshot.org/

## Overview

Grids have established its own PKI-based Authentication & Authorization Infrastructure (AAI), which was not linked to any existing identity management systems and therefore it is not sometimes well perceived by the users. Even if the situation is changing and Grids are aiming at utilization of identity federations, there still remain crucial aspects that prevent from smooth usage of federated identities in Grids.

One basic issue is a way of obtaining a credential to routine access Grids, which should be simple to use, yet secure enough. Utilization of federated identities is highly desired by the users and several solutions have been adopted recently, as seen e.g. with the Terena TCS certification authority. Another useful approach is transparent credential conversion, which allows to obtain Grid credentials without users' explicit intervention. We will demonstrate how the federated Moonshot infrastructure can provide such a conversion, opening Grids to a larger user base.

## Impact

Current identity federations are limited in the number and type of applications supported. The most prevalent federations are closely tied with web (e.g., Shibboleth) or network access (Eduroam). However, none of these federations is suitable for facilitating access to the Grid. The Moonshot architecture, on the other hand, is open for any type of services regardless the service protocols and/or interfaces they use.

Having Moonshot supported by the Grid environment would increase the number of potential users and also make their management easier. In particular, we propose an integration of the Moonshot and PKI so that users can easily obtain credentials needed to join the Grid, based on their federated identities. Identity federations also maintain sets of attributes assigned to the users, which may also be valuable for the Grid, too. For instance, the resource providers and/or VO managers could specify access control rules based on these attributes (e.g., users' affiliation). The big advantage of the federation

model is that the attributes are kept current and therefore can be relyied upon by their consumers.

## Description of the work

Moonshot is a set of technology for providing federated access to applications. At a technical level, federation decouples management of credentials within an organization from authentication proofs between organizations. Many existing technologies such as Security Assertion Markup Language (SAML), RADIUS, and Diameter support federation. However these existing technologies are focused on a single application domain. SAML provides federation for the web and web services, RADIUS and Diameter provide federation for network access. Moonshot integrates RADIUS federation into most application protocols, whose users can then leverage from federated access. At the same time, SAML is fully supported and provides rich attributes to describe federated subjects. The Moonshot infrastructure builds upon components that are well-known and understood, and have been in use for a long time. Unlike other federation middlewares (e.g. Shibboleth), Moonshot is not tied with the web environment and can be utilized by non-web applications. The Moonshot architecture is based on open standards and the Moonshot community actively contributes to the ABFAB working group of the IETF.

Moonshot is a good fit for the grid because many grid components, particularly grid middleware components, do not use web technologies. We are seeking ways how Grids can benefit from the Moonshot infrastructure. In the contribution, we will demonstrate the design and current achievements focusing on users running jobs on the grids using a Moonshot-generated id. As the result, the users will be able to use their federated identity to launch and control jobs. Finally, we will also demonstrate the flexibility of Moonshot by demonstrating how a particular grid service can be plugged into the Moonshot infrastructure so that users could use the service without having to obtain a certificate first. For this purpose, we will show how the gLite Logging and Bookkeeping service can be adapted to natively support Moonshot.

## Conclusions

A federated identity is very convenient means for authentication of users and passing additional information about them. Current identity federations are not general enough to fit the Grid environment, though. The aim of this contribution is to introduce the Moonshot project, which fills in the gap between existing identity federations and applications that cannot be integrated with them due to completely different underlaying technologies.

Moonshot can make the access to the Grid easier for the users, since they could mostly use the credentials they use also for other services. Also the resource poroviders could benefit from this integration and rely on the users' attributes propagated from their identity providers.

While the Moonshot project is quite young and the work is still in progress, we plan to demonstrate its benefits for the Grid communtity to provide a notion of its potential.

**Primary authors:** KOURIL, Daniel (CESNET); JENSEN, Jens (STFC Rutherford Appleton Laboratory); HOWLETT, Josh (JANET); PROCHAZKA, Michal (CESNET); HARTMAN, Sam (Painless Security)

**Presenter:** KOURIL, Daniel (CESNET)

**Session Classification:** Technologies for Distributed Computing

**Track Classification:** DCI - Implementation