Federated Identity Management within CRISP*

A. Montiel González[1], *K. Schwarz*[1], *and P. Malzacher*[1]
[1]GSI, Darmstadt, Germany

The Cluster of Research Infrastructures for Synergies in Physics (CRISP) project is a collaboration between different institutions and facilities related to physics research. In this scope, a pan-European Federated Identity Management (FIM) system is under development.

Introduction

FIM solves the Single-Sign-On (SSO) access across multiple organizations using the same identification data.

The core protocol for enabling federated access to applications is Security Access Markup Language (SAML)[1]. SAML is the standard for exchanging authentication and authorization data between security domains, with Shibboleth[2] being its most extended implementation.

FIM especially benefits research communities, which try to have a common vision and follow the same roadmap[3].

At GSI/FAIR, like in most distributed high energy physics communities, the implementation to solve authentication and authorization is done with x.509. Besides, access to traditional web services is supported by local accounts as well as access to local computing resources. Shibboleth would enable browser-based applications to be accessed in a federated way through a wide set of authentication methods, including: x.509, OpenID and Kerberos. But this infrastructure would not solve the non-web-based applications. In this case, Moonshot[4] is interesting as it also relies on SAML for exchanging identity assertions.

The approach within CRISP is to continue developing the Shibboleth based Umbrella[5] system to bridge to other federations. In addition, we also evaluate Moonshot.

Umbrella

Umbrella is a FIM solution adopted from the Photon/Neutron community to provide federated access to experimental data. It provides a unique EU-wide identifier of users and solves the problem of having to remember accounts spread in the different web user offices(WUO)-web interface to the resources. This tool is currently implemented in several organizations within this community and it is under development at GSI/FAIR. Umbrella has only one Identity Provider(IdP) provisioning identification of users. This Umbrella account is the only one to be remembered by the user. The IdP stores minimal information about the users, enough to uniquely identify them. The users can link their account in the local organizations to their Umbrella account, so they are able to access already existing resources through this single account.

The authorization phase is completely delegated to the local WUOs.

Implementation and ongoing activities

An Umbrella system has been deployed as a testbed in a virtual machine(VM), with both IdP and Service Provider(SP) components. Since many users hold a x.509 certificate already, the first development is to create a bridge that would authenticate users holding such certificate to Umbrella resources, and, eventually, vice-versa. To accomplish this, another VM has been deployed with Shibboleth IdP and SP. The IdP handles login through x.509 and the SP federates access to a secured resource by using such certificate installed in the browser. It is still ongoing work to develop the software needed to bridge these credentials to the Umbrella.

Another line of development is to provide federated access to non web based applications. Moonshot proposes a solution for this case. It relies on three key security technologies: Extensible Authentication Protocol, Generic Security Services API and SAML. The main advantage lies on leaving the authentication phase to the eduroam infrastructure, which is extensively adopted, and to enable enriching of edu-tokens via SAML. A testing infrastructure has been deployed to try this solution. This testbed consist of a Home Institution(HI) and a Visited Institution(VI). The eduroam federation has been simulated with local RADIUS servers and clients. The HI has several VMs connected to the same internal network running the following services: Kerberos-Ldap implementation as Authentication-Authorization-Accounting system, IdP from Shibboleth, a RADIUS server, and a Moonshot ssh server. These are connected to the visited institution through two channels: JRadius, which is an open-source application that allows to simulate RADIUS traffic, and through SAML messages between the IdP and the SP. The VI runs the following services: the visited RADIUS server, the SP and the moonshot ssh client. The functionality of HI and VI has been demonstrated. Integration between them still needs to be implemented.

References

[1] https://www.oasis-open.org/standards/#samlv2.0

[2] http://shibboleth.net/

[3] D. Broeder et al, “Federated Identity Management for Research Collaborations”, TNC 2012, April 2012

[4] https://community.ja.net/groups/moonshot

[5] https://umbrella.psi.ch

*Work supported by the European Commission under the 7th Framework Program Grant Agreement 283745.