Contribution ID: **84** Type: **Presentations**

Federated Grid Access Using EMI Security Token Service

Thursday, 11 April 2013 14:10 (20 minutes)

Impact

As the majority of Grid infrastructures will require X.509 credentials for the foreseeable future, we consider hiding of the complexity of the X.509 end-entity certificate and private key management from the users as the most important feature of the EMI STS. As most of the users do not need their end-entity certificate for anything else except the Grid proxy initialization, EMI STS can provide them with their Grid proxy certificate directly, and thus avoid many unnecessary complexities from the users perspective. As Security Assertion Markup Language (SAML) can be considered as the de-facto standard in the national and international federations, federated Grid access use cases concentrate on the EMI STS use cases of transforming the SAML assertions into the Grid proxies.

As it was stated before, any party capable of producing specified request messages and understanding response messages can act as a client for the EMI STS: they just need to obtain the used security token somehow to be included in the request message. In our case, the client just needs to have a trusted SAML assertion in order to exploit it in the communication with the EMI STS for obtaining a Grid proxy.

This talk discusses different alternatives on integrating the EMI STS with SAML-based identity federations. Integration points exist for most of the federation software, including Shibboleth Identity Provider and Microsoft ADFS. This talk analyzes what are the biggest pros, cons and challenges in both technology and policy perspectives for different alternatives. The related existing solutions are also analyzed and how some of them can be used together with the STS for providing totally new use cases, including access to the Cloud resources in addition to the Grid.

Summary

On the security and particularly the digital identity management side, the highlight of the final EMI release (EMI-3 Monte Bianco) is the Security Token Service (STS): a new general purpose service for transforming the existing user credentials from a certain format to another format. The service is based on open Web Services (WS) standards (WS-Trust and WS-Security) in order to enable wide set of both Web browser and non-browser based use cases. This talk focuses on the use cases where users can obtain their Grid credentials using existing federated identities.

URL

https://forge.switch.ch/redmine/projects/sts/wiki

Description

EMI Security Token Service (STS) is a partial implementation of the STS service defined in the OASIS WS-Trust specification. It is defined as a service that can be used for transforming an existing security token into another security token format. Security token, on the other hand, is defined in the WS-Security specifications as a collection of claims that can be attached into a Web Service message.

The incoming security token formats that are supported by EMI STS implementation are username/password token and SAML assertion. From these formats, EMI STS can issue X.509 certificates and X.509 proxy certificates by using an online CA for issuing the certificates and VOMS for issuing the VO attributes. By enabling the token transformation, STS establishes a trust relationship between different security and application domains, like between SAML and X.509 for instance.

From the clients' point of view EMI STS is a Web Service that, like any other Web Services, is accessed using the SOAP protocol. This means that any party capable of producing specified request messages and understanding response messages can act as a client for the EMI STS. As the SOAP protocol is extremely widely adopted, many building blocks exist for implementing a client to STS. This is not dependent on the platform, programming language or even deployment: the STS client can be for instance a simple command-line tool, a local heavy client with rich GUI, or a Web portal.

Primary author: MIKKONEN, Henri (Helsinki Institute of Physics)

Presenter: MIKKONEN, Henri (Helsinki Institute of Physics)

Session Classification: Federated Identity Management Workshop

Track Classification: Community Platforms (Track Lead: P Solagna and M Drescher)