Contribution ID: **57** Type: **Oral**

OpenSAML extension library and API to support SAML2.0 - XACML protocol for interoperable authorisation infrastructure in distributed Grid applications

Wednesday, February 13, 2008 2:20 PM (20 minutes)

Authorisation is an important component of the Grid security infrastructure. AuthZ decision is typically based on the AuthZ policy that contains a set of access control rules depending on user credentials or attributes. In many cases AuthZ service is a part of the application platform and uses a policy specific to application. Consistency of the access control enforcement can be achieved by introducing the Site Central AuthZ Service (SCAS) that will allow applying common policies centrally and leave a possibility for applying local policies and enforcement mechanisms.

The proposed SAML-XACML library and API provide all necessary functionality for the PEP (bound to the Grid resource or application) to call out to external SCAS. The API provides the helper classes to create and parse SAML-XACML messages and also extendible functionality for policy Obligations handling. The proposed functionality is specifically targeted to support pool account management when submitting Grid job to WNs

3. Impact

The library is being tested with the G-PBox as one of the suggested SCAS implementations. G-PBox is a XACML based Policy Decision Point (PDP) that provides also reach functionality for hierarchical policy management what is considered as an important component of cross and inter-organisational access control management. C-based implementation of the SAML-XACML protocol provided by Globus will allow also using LCAS/LCMAPS service as a SCAS. AuthZ decision made by SCAS can be conveyed to the gLexec at WNs in a form of SAML assertions and enforced there.
Additional benefits of using OpenSAML as a platform for implementing SAML-XACML protocol is that this will allow future easy integration of the EGEE/Grid AuthZ infrastructure with the primary Shibboleth/SAML based universities and NREN Authentication and Authorisation Infrastructure (AAI). In this case users can use their general purpose credentials issued by their home organisations to access Grid services and applications.

4. Conclusions / Future plans

This development has been done in the framework of the gJAF development and EGEE-OSG AuthZ interoperability initiative, and may be one of the modules in achieving interoperability in the grid. SAML-XACML protocol is recommended as a protocol to access Grid AuthZ service. The library and API have being contributed to the Internet2 OpenSAML project.
Further development includes formal definition of the SAML-XACML AuthZ profile for Grid applications, attributes in use and Obligations handling API.

Provide a set of generic keywords that define your contribution (e.g. Data Management, Workflows, High Energy Physics)

Authorization,SCAS,gJAF,G-PBox

1. Short overview

The proposed OpenSAML extension library and API implements SAML2.0 profile of XACML may provide a basis for interoperability between different AuthZ services. It supports communication between two major components of the generic AuthZ service architecture: Policy Enforcement Point (PEP) and Policy Decision

Point (PDP). The library and API are implemented as pluggable modules that can be used with different Java based AuthZ services e.g. gLite Java AuthZ Framework (gJAF), GT- AuthZ, G-PBox.

Primary authors: FORTI, Alberto (Unknown); SAGEHAUG, Hakon Tuvin (Unknown); VENTURI, Valerio (Unknown); DEMCHENKO, Yuri (Unknown)

Presenters: SAGEHAUG, Hakon Tuvin (Unknown); VENTURI, Valerio (Unknown)

Session Classification: Data Management

Track Classification: Existing or Prospective Grid Services