OpenSAML extension library and API to support SAML2.0 profile of XAMCL protocol, for interoperable authorization infrastructure in distributed Grid application

Håkon Sagehaug, University of Bergen
Yuri Demchenko, University of Amsterdam
Valerio Venture, CNAF, INFN
Alberto Forti, CNAF, INFN

EGEE User Forum
11-14 February 2008, Clermont-Ferrand, France

Information Society and Media

Outline

- Overview of XML standards involved
- Introduction of the SAML 2.0 profile of XACML
- The provided extension and API
- Authorization
- Use of the library
- Handling of XACML obligations
- Testing
- Status and work further

Overview of SAML

- **Security Assertion Markup Language(SAML) is a XML specification, defining syntax and processing semantics about security assertions**
- **Security assertion here means a package of information that supplies zero or more assertion statements made by a SAML Authority**
- **In SAML there is defined three different assertion statements**
  - Authentication, information about when, who and by what the subject was authenticated
  - Attributes, the asserted subject is associated with these attributes
  - Authorization Decision, the action of granting access or not to a asserted subject

Overview of XACML

- **eXtensible Access Control Markup Language(XACML) is a specification in XML for writing access control policies in XML and how to interpret them**
- **In XACML one operates with a context and two of the main elements in the context is**
  - Request, which is a message for asking for a authorization decision
  - Response, containing the authorization decision

SAML 2.0 profile of XACML

- **The SAML2.0 profile of XACML is combining SAML2.0 and XACML**
- **Now able to use SAML for sending queries and statements about authorization decisions and policies**
- **Introduces some new elements**
  - XACMLAuthorizationDecisionQuery
    - Made for containing a AuthZ decision query from a PEP to the PDP
  - XACMLAuthorizationDecisionStatement
    - The result of the AuthZ decision from PDP to PEP
  - XACMLPolicyQuery
    - Used for requesting a XACML Policy or PolicySet
  - XACMLPolicyStatement
    - Contains the returned policy or set
- ***Query is sending a request**
- ***Statement is the response**

The provided extension and API

- **Implements the SAML2.0 profile of XACML in Java**
- **It is build as an extension to the OpenSAML code**
- **Has the same features as OpenSAML in respect to be able to work with the XML elements as Java-object,each element has**
  - *Builder
  - *Impl
  - *Marshaller
  - *Unmarshaller
- **If familiar with OpenSAML, the extension is easy to use**
- **If not, there is a programming guide on the projects web page (address on the last slide)**

Authorization in Grid

- **Authorization is the act of giving users access to resources**
- **Authorization decision is based upon policies**
- **Two possible places for these policies to be located**
  - Locally
  - Centrally, through Site Central Authorization Service(SCAS), where every service is contacting a central authorization service
- **Often we have two major components in a authorization infrastructure**
  - Policy Enforcement Point(PEP) on the resource side for protecting the resource, where the authorization is initiated and later enforced
  - Policy Decision Point(PDP), where the authorization decision is made.
- **If these two components are distributed from each other they need to communicate**

Use of the extension and API

- For communication between different authorization components(e.g. PEP and PDP/SCAS)
- Since it's an XML specification the data that goes on the wire is just XML
- That gives the possibility of having different implementation of the profile at the different functional elements.
- The library and API provides helper classes for creating and validating SAML-XACML messages.
- Implemented as pluggable module so it can be used in different Java based AuthZ frameworks
  - gLite Java Authorization Framework
  - Globus Toolkit AuthZ
  - G-PBox

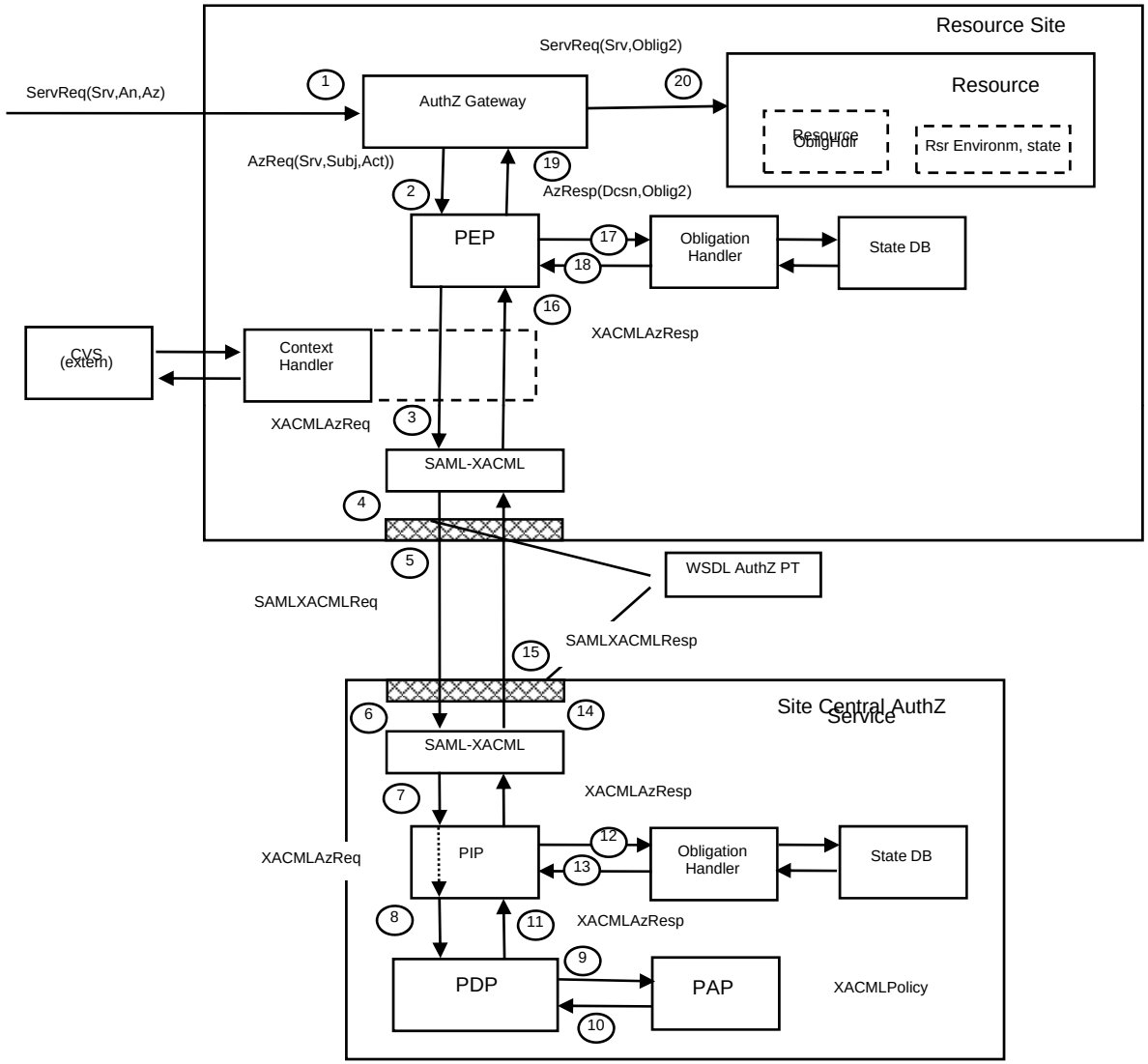
Use of the extension and API

- Globus is providing the C implementation of this profile, then Local Credential Authorization Service(LCAS)/Local Credential Mapping Service(LCMAPS) also can be used as SCAS and be called out to
- Decisions from here can be conveyed to be used from gLexec at the Worker Node(WN) and enforced there

Handling of Obligation

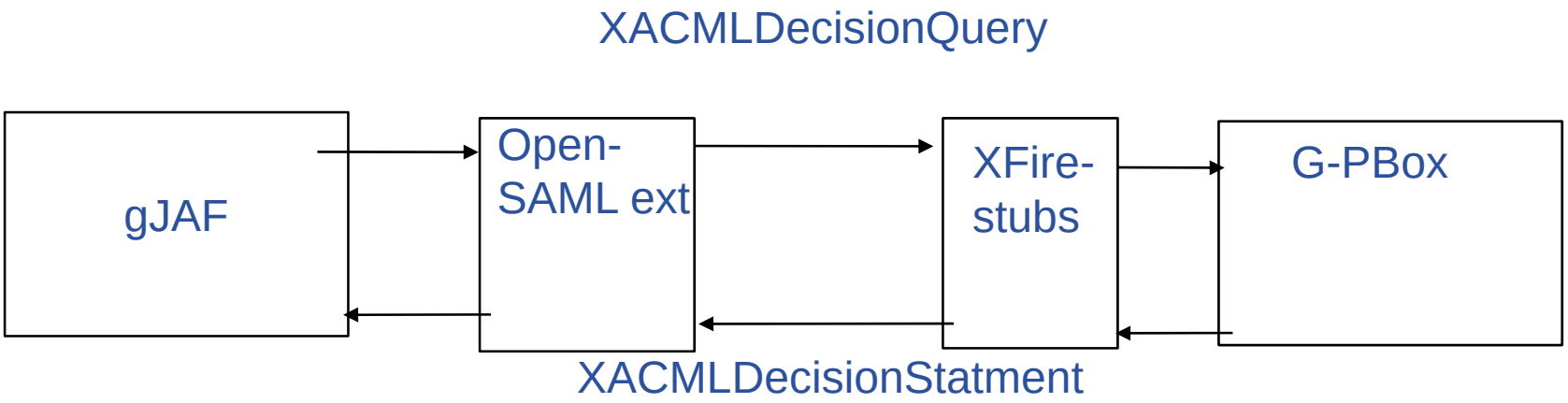
- **Another issue that can be handled elegant with this extension is handling of obligations from PDP. Obligations is defined as actions that should be preformed by the PEP in conjunction with the enforcement of an authorization decision(XACML Spec). Such obligations can be mapping of users to pool account at WN**

SAML XACML data flow



Testing sequence

- G-PBox is one of the suggested SCAS implementation
- It contains different policies and also a XACML Policy Decision Point
- Using gJAF as policy enforcement point and G-PBox as Policy decision point
- Used the web service interface for G-PBox for communication



Stages is the testing

- The user wants to be authorized for using some resource
- gJAF extracts the needed information from the voms-proxy certificate
- Creates a XACMLAuthzDecisionQuery and sends it to G-PBox by using the web service interface
- G-PBox evaluates the query against some XACML policy, using the sunxacml PDP
- G-PBox creates a XACMLDecisionSatement wrappers it inside a SAMLResponse and sends it back to gJAF
- Back at gJAF the response from G-PBox is handled and we get out the account which the user is supposed to be mapped to

Other benefits

- **Easy integration of EGEE/Grid Authz infrastructure with Shibboleth and SAML based universities.**
- **If Grid AuthZ infrastructure and Shibboleth/SAML based universities is combined, that means that users can use their general purpose credentials, from their home organization, for accessing Grid services and applications**
- **This will ease the use of the Grid**

Status and further work

- **The code has been committed to the Internet 2 OpenSAML 2.0 project**
- **Further work of AuthZ interoperability consists of defining**
  - attributes for common XACML-compatible policies
  - obligation handling API
- **Links**
  - Home page of the project: http://www.bccs.uib.no/~hakont/SAMLXACMLExtension/