omii europe

open middleware infrastructure institute

SAML support in VOMS

Valerio Venturi

EGEE JRA1 AH Meeting, Amsterdam 20/23 February 2008

Outline

- **Standardization effort**
- **Service description**
- **Integration**

Standardization Effort

- **Goal was add SAML support to VOMS**
- **Attribute Exchange profile edited in the OGSA AuthZ WG**
- **SAML Query/Response profile**
- **X.509 Deployment**
- **XACML Attributes**

VOMS SAML

- **Service implementing the Attribute Exchange Profile**
  - That is, SAML Query/Response profile + X.509 subjects + attributes requirements
- **It does the same thing the classic VOMS server does**
  - releases signed assertions containing attributes about a subject
- **Differences**
  - uses SAML attribute assertions instead of ACs
  - has a Web Service interface

VOMS SAML

- **No API, no voms-proxy-init**
  - WS approach, get the WSDL and use whatever SOAP and XML tools you prefer
    - example code in the distribution using Axis, XFire, JAXB, XMLBeans, libcurl, libxml; coming soon gSOAP, OpenSAML
  - Binding to a proxy only one of the possible uses
    - more later

Service Interface

- **A single operation, AttributeQuery**
  - Input : samlp:AttributeQuery
    - Who's doing the query, whose attributes is querying for, which attributes is querying for
  - Output : samlp:Response
    - Who’s answering, what’s the status, and the assertion
- **An attribute assertion associates a principal with a set of attributes**
  - The asserting entity, the subject of the assertion, conditions under which the assertion is valid, the attributes, and a signature
- **A SAML Attribute Profile for VO related attributes is currently being discussed in the OGF OGSA Authorization WG**

Implementation

- **Web service**
  - To be deployed in a servlet container
    - Used with Tomcat with gLite trustmanager
  - Uses Axis
    - But custom serialization that uses OpenSAML since Axis has problems with SAML schemas
      - There is SOAP support in OpenSAML, will move from Axis
- **SAML**
  - uses OpenSAML
    - currently release candidate 2
- **Database layer**
  - Uses Hibernate as VOMS Admin does

Status

- **First release due February 29**
  - Alpha available since April 07, beta since November 07, both used for OMII-Europe developments, testing and demonstrations
- **Those impatiently willing to test it can enroll in the OMII-Europe VO and use the present deployment**
- **Fancy a deployment for gLite developers?**
  - Could serve the DTEAM VO
  - I didn't dare asking Maria Dimou about either using a machine at CERN mort connecting to the database from CNAF
    - The db replicas that are going to be available at CNAF soon would be easier
    - An official endorsement from JRA1 would help

Middleware Integration

- **VOMS releases SAML assertion, so what?**
- **Assertions are used by Grid services to drive authorization decisions**
- **Commonly used in push mode for attribute retrieval**
  - get attributes and push them to the service
- **How to do that?**
  - In an extension of the proxy certificate, the way VOMS does now with ACs
  - In the SOAP Header, using WS-Security

Middleware Integration

- **Just as ACs, SAML assertions may be put in an extension of the proxy certificate**
  - Proved a very simple and effective way of carrying attributes to Grid services
- **This is the way GridShib has used SAML assertions when integrating Shibboleth and GT**
  - https://spaces.internet2.edu/display/GS/X509BindingSAML
- **One may also have voms-proxy-init doing that**
- **Advantage would be the integration would be nearly painless**

Middleware Integration

- **In OMII-Europe we have experimented using WS-Security to carry SAML assertions in the SOAP Header**
  - One of the main goal was the availability of VOMS on UNICORE, which doesn't use proxies
    - Using the SOAP Header works both with EECs and proxies
- **Defined in the 'Web Services Security: SAML Token Profile 1.1'**
  - defines the use of SAML assertions as security tokens from the <wsse:Security> header block defined by the WSS: SOAP Message Security specification
- **Full example of client service inteaction available with the source code**
  - Comprises validation of the XML signature

Middleware Integration

- **Advantages**
  - It's standard
  - Works with EECs
    - Not only useful for proxies-unaware middleware as UNICORE
    - Why use proxies, that aren't safe (or as safe as EECs), when you can use EECs?
      - Using resources that don't need a delegation step
  - Decoupling of authentication from attributes
    - You don't need to get the client certificate and extract the attributes
    - For services deployed in a container, let the container do the X.509 dirty jobs and care only about the XML

- **Disadvantages**
  - Only for Web Services
  - Coupling is used for assuring against attributes escalation
    - You have a proxy with an AC, you cannot ask for attributes that are not in the AC already

Ongoing integrations

- **CREAM BES**
  - Uses VOMS SAML assertions as well as VOMS proxies
  - More in next talk
- **UNICORE**
  - uses VOMS SAML assertions for authorization
  - Tested with the UNICORE OGSA BES, available for any UNICORE service
- **Globus Toolkit**
  - Two components in OMII-Europe that are based on GT are integrating VOMS SAML assertions
    - Writing a PIP for the authz framework, and we are in touch with GT developers to eventually feed it back to them
      - May come handy if GT AuthZ were choosen as a PEP for the new authz framework

gLite Integration

- **SAML assertions mentioned in the EGEE III DoW**
  - 'extension in the use of SAML-based attributes for authorisation'
  - 'support the use of SAML attributes in VOMS'
  - 'development of the gLite authorization framework .. support for the use of SAML assertions '
- **How to use them probably to be discussed in the next weeks**
  - There's a service you can use
  - There's experience you can leverage on
    - Integration in CREAM BES
- **Suggestion: try to maintain the availability under UNICORE and GT**

gLite Integration

- **Need to move VOMS-SAML code into EGEE context**
- **Branding issue to be sorted out at a higher level**
- **Shouldn't be too painful**
  - Code currently only in the INFN SVN
  - Built with ETICS, and packaged nearly the gLite way
    - uses /opt/omii instead of /opt/glite

- valerio.venturi@cnaf.infn.it
- **jra1voms@omii-europe.org**