VOMS Developments

Vincenzo Ciaschini

JRA1 All-Hands

Helsinki 18-20/06/07

Globus Dependency Removal

- **Step 0:**
  - APIs capable of interpreting the AC without globus.
    - DONE (VOMS 1.7.0)
- **Step 1:**
  - Server to be contacted indifferently with GSI and SSL. APIs capable of contacting the server via both GSI and SSL.
    - Scheduled for VOMS 1.8.0 (approx. October)
- **Step 2:**
  - Server and clients speaking only SSL. Breaks protocol compatibility with VOMS < 1.8.0
    - Not before VOMS 1.9.0 (depending on TCG)

Globus Dependency Removal

- **Deployment Procedure:**

- **When 1.8.0 comes out:**
  - Upgrade the servers to 1.8.0.
  - Start linking applications against the SSL libraries.

- **When 1.9.0 comes out:**
  - Upgrade the clients to 1.9.0.
  - APIs libraries will silently remove GSI and use SSL instead.

Shorter FQANs

- **Finally implement the shorter FQANs, e.g:**
  - `/atlas` instead than:
  - `/atlas/Role=NULL/Capability=NULL`
- **Current APIs can already deal with this, since 1.5.x.**
- **Optional, disabled by default.**
- **Longer form will be deprecated.**
- **Scheduled for 1.8.0**
- **Shorter form will become the default in 1.9.0**

Aliased Identities

- **The possibility to have two or more different identities (certificates) for the same user.**
  - See VOMS-Admin presentation for details admin-side.
  - Credentials will belong to the identity which contacted the server.
  - The different credentials would be considered synonyms.
  - Will require a DB schema change => sync update of voms & voms-admin.

- **Scheduled for VOMS 1.8.0**

Syslog Logging

- Allows logging to be done on syslog (different levels) as well as on private files.
- Respecting David's document.
- In VOMS 1.8.0 (Done. Now under conformance testing)

APIs Additions

- **Allow parsing of FQANs standalone.**
  - e.g: pass FQAN /atlas/prod/Role=sgm[/Capability=NULL], get: (/atlas/prod, sgm, “NULL”)

Other Platform Support

- **Integration of patch from Apple.**
  - Patch accepted, but integration stopped pending resolution of copyright issues.
  - In VOMS 1.8.0 (tentatively)

- **Fixing of lib64 issue.**
  - In VOMS 1.7.x

omii europe

open middleware infrastructure institute

VOMS & SAML

Valerio Venturi

JRA1 All-Hands, Helsinki, 18-20/6/07

OMII-Europe

- **OMII-Europe is an EU-funded project which has been established to source key software components that can interoperate across several heterogeneous Grid middleware platforms**
- **The emphasis is on the re-engineering of software components rather than on the development of new technology. OMII-Europe will develop a repository of quality-assured Grid services running on these existing major Grid infrastructures.**
- **Component being re-engineered with relevant standard bodies**
  - **Job Submission (OGF OGSA-BES WG)**
  - **Database (OGF DAIS WG)**
  - **Virtual Organisation Management (OGF OGSA Authorization WG)**
  - **Accounting (OGF RUS WG)**

OMII-Europe JRA1 VOM Activity

- **OMII-Europe is extending VOMS to support recommendation emerging from the OGF OGSA Authorization WG**
  - **Web Service**
  - **Using SAML V2.0 Deployment Profile for X.509 Subjects,OASIS Committee Draft (undergoing public comment)**
- **VOMS is being integrated in UNICORE**
  - **using the re-engineered service**
  - **UNICORE Job Submission with authorization based on VOMS attributes demonstrated at OGF 20**
  - **Wider integration undergoing**

VOMS SAML Service

- **Same semantic of the Attribute Certificate based service**
  - **Using SAML for protocols and assertions**
    - **What was expressed using RFC 3821 Attribute Certificate is expressed using saml:Assertion elements**
    - **SAML protocols elements are used for the interface**
- **Web Service exposing operation following "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0"**
  - **A single operation**
    AttributeQuery(samlp:AttributeQuery)
    returns: samlp:Response

VOMS SAML Service

- **AttributeQuery allows to specify**
  - **The subject whose attributes the requestor wants to know**
  - **The attributes requested**

```
<AttributeQuery ID=... Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer Format=...  xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
   CN=Valerio Venturi,L=CNAF,OU=Personal Certificate,O=INFN,C=IT
  </Issuer>
  <Subject xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
   <NameID Format=...>
    CN=Valerio Venturi,L=CNAF,OU=Personal Certificate,O=INFN,C=IT
   </NameID>
  </Subject>
  <!-- here Attribute elements to request attribute -->
</AttributeQuery>
```

- **Subject must match Issuer**
  - **Going to provide support for Query (attribute pull mode, third party request for a Subject's attributes)**
    - **In parallel with AC based VOMS, discussing authorization issues**

VOMS SAML Service

- **Response contains**
  - **An Assertion element (digitally signed)**

```
<saml:Assertion ID=... IssueInstant=... Version="2.0"    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer Format=...>
   CN=omii002.cnaf.infn.it,L=CNAF,OU=Host,O=INFN,C=IT
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   ... signature data ...
  </ds:Signature>
  <saml:Subject>
   <saml:NameID Format=...>
    CN=Valerio Venturi,L=CNAF,OU=Personal Certificate,O=INFN,C=IT
   </saml:NameID>
   <saml:SubjectConfirmation Method=...>
    ... binding to subject's X.509 data ...
   </saml:SubjectConfirmation>
  </saml:Subject>
 continue next page
```

VOMS SAML Service

```
<saml:Conditions NotBefore=... NotOnOrAfter=...>
  <saml:AttributeStatement>
    <saml:Attribute Name="group-membership-id" NameFormat=...>
      <saml:AttributeValue xsi:type="xs:string">
        /omiieurope
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

- Issuer
- Subject
  - Distinguished Name following RFC 2253
- Conditions element set duration
- Attribute element contains FQAN and GA
  - finalizing attribute naming (more in sequent slides)

VOMS SAML Service

- **Uses**
  - **Tomcat**
    - **tested version 5.5.20**
    - **used Tomcat default HTTPS connectors so far, plans to support Tomcat+TrustManager HTTPS in a few weeks**
  - **Axis**
    - **version 1.4**
  - **OpenSAML**
    - **version 2.0 supporting SAML V2.0 is still Tecnology Preview, official release expected soon**
- **Built in ETICS under the OMII-Europe project**
- **Will undergo OMII-Europe QA process before released made public available**
- **Prototype available for testing and internal development in the OMII-Europe Evaluation Infrastructure at CNAF**

SAML VOMS Tokens

- **Attribute Certificate normally used in conjunction with users' proxy certificates**
  - **Embedded in an extension of the users' proxies**
- **GridShib doing the same for SAML assertions**
  - **Bind an ASN.1 SEQUENCE of <saml:Assertion> elements at a well-known, non-critical X.509 v3 certificate extension**
- **Exploring alternatives**
  - **WS-Security gives a way to transport security tokens with SOAP messages**
    - **In the SOAP Header**
    - **UNICORE OGSA-BES using WS-Security for the prototype and UNICORE planning to use it for VOMS integration**
    - **Supported in the WS-I Basic Security Profile**

VOMS SAML Attributes

- **MUST provide clear indications on how VOMS information are expressed using SAML**
  - **Going to have a SAML V2.0 VOMS Attributes Profile**
    - Synchronize with others using SAML Attributes
    - **Naregi guys post to OGSA AuthZ WG**
      - They're using voName, group and role attributes (in their own namespace naregi:vo)
    - **VASH guys is going to face the same problem**
  - **Going to use XACML profile for SAML Attributes due to interoperability within OGSA AuthZ WG specs**

VOMS SAML FQANs

- **Expressing FQANS as SAML Attribute elements**
  - **Natural to use AttributeValue elements with type xsd:string**

```
<saml:Attribute Name="FQAN" NameFormat=...>
  <saml:AttributeValue xsi:type="xs:string">
    a FQAN
  </saml:AttributeValue>
  <saml:AttributeValue xsi:type="xs:string">
    another FQAN
  </saml:AttributeValue>
</saml:Attribute>
```

  - **Problems with SAML specs**
- **Going to differentiate FQANs expressing only group information**

```
<saml:Attribute Name="a-sounding-name" NameFormat=...>
  <!-- attribute values with FQANs here -->
</saml:Attribute>
```

```
<saml:Attribute Name="a-sounding-name" NameFormat=...>
  <!-- attribute values with FQANs here -->
</saml:Attribute>
```