Common VO SAML attribute profile

Andrea Ceccanti (INFN)

EMI SAML task force

Common VO attribute profile

- Goal:
  - converge on the definition of SAML VO attributes understood by the three middlewares
- Requirements
  - Simple mapping of SAML to XACML attributes used in policies
  - Use dci-sec registered namespace
    - http://dci-sec.org/
- Attributes
  - VO membership
  - Group membership
  - Role possession

VO membership attribute

- Name:
  - http://dci-sec.org/saml/attribute/virtual-organization
- The attribute value contains a set of strings defining the name of the VO the subject is member of
- Example:

```
<Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="http://dci-sec.org/saml/attribute/virtual-organization">
  <AttributeValue xsi:type="xs:string">atlas</AttributeValue>
</Attribute>
```

Groups attribute

- Name:
  - http://dci-sec.org/saml/attribute/group
- This multi-valued attribute represents the SAML assertion subject's VO group membership.
- Attribute value is a unix like absolute path with the VO name as the mandatory root
  - The profile defines the “dci-sec:group” type for this
- Example:

```
<Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="http://dci-sec.org/saml/attribute/group">
   <AttributeValue xsi:type="dci-sec:group">/atlas/production</AttributeValue>
   <AttributeValue xsi:type="dci-sec:group">/atlas/analysis</AttributeValue>
</Attribute>
```

Role attribute

- Name:
  - http://dci-sec.org/saml/attribute/role

- This multi-valued attribute represents the roles assigned to the subject. Roles must be scoped at the group or VO level using an attribute (defined by the profile) in the attribute value element.

- Example:

```
<Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="http://dci-sec.org/saml/attribute/role">
    <AttributeValue
        xsi:type="dci-sec:role"
        dci-sec:group="/atlas/production">SoftwareManager</AttributeValue>
</Attribute>
```

Primary attribute

- Name:
  - http://dci-sec.org/saml/attribute/primary
- This single-valued attribute represents the default membership attribute assigned to the subject. The type of the attribute value must be dci-sec:role or dci-sec:group. The attribute value must be present in the group / role attribute in the same assertion.
  - Role attribute values must be scoped
- Example:

```
<Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="http://dci-sec.org/saml/attribute/primary">
    <AttributeValue
        xsi:type="dci-sec:role"
        dci-sec:group="/lhcb">pilot</AttributeValue>
</Attribute>
```

Compliance with the common profile

- Compliant Attribute Authorities are not limited to issue **only** the attributes defined in the profile but must express group and role membership according to the profile rules
  - VOMS SAML will issue also VOMS-specific attributes (fqans, generic attributes, ...) and will have a profile for those attributes
  - UVOS will also issue other attributes that are relevant to UNICORE
- A version of VOMS SAML compliant with the profile will be part of EMI-1 release

Links

- The SAML TF wiki page:
  - https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SAML
- The current Common profile proposal:
  - https://twiki.cern.ch/twiki/bin/view/EMI/CommonProfileStrawmanProposalV2
- Send comments and feedback to
  - emi-jra1-sec-saml@eu-emi.eu

Thank you

EMI is partially funded by the European Commission under Grant Agreement INFSO-RI-261611