EUROPEAN MIDDLEWARE INITIATIVE

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

Profile XML Schema types

- **dci-sec:vo**
  - Pattern: \w[-_.:\w]*
  - Example: emi

- **dci-sec:group**
  - Pattern: (/\w[-_.:\w]*)+
  - Example: /emi/test:group

- **dci-sec:role**
  - Pattern: \w[-_.:\w]*
  - Example: VO-Admin

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. Attribute value XSD type is dci-sec:vo.

- 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="dci-sec:vo">atlas</AttributeValue>
</Attribute>
```

Group 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>
```

Primary Group

- Name: http://dci-sec.org/saml/attribute/group/primary

- This single-valued attribute represents the SAML assertion subject's primary group membership.

- Example:

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

Role attribute

- Name: http://dci-sec.org/saml/attribute/role
- This multi-valued attribute represents the roles assigned to the subject. AttributeValue type is dci-sec:role.
- Roles MUST be scoped to a group using the dci-sec:scope attribute. The group pointed by the dci-sec:scope attribute must appear in the http://dci-sec.org/saml/attribute/group attribute included in the SAML assertion.
- 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:scope="/atlas/production">SoftwareManager</AttributeValue>
</Attribute>
```

Primary Role attribute

- Name: http://dci-sec.org/saml/attribute/role/primary
- This single-valued attribute represents the primary role assigned to the subject. AttributeValue type is dci-sec:role.
- All http://dci-sec.org/saml/attribute/role constraints apply also to this attribute
- Example:

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

- EMI-1 VOMS SAML currently implement VO profile as described in this presentation
  - Example of generated SAML assertion available on the SAML TF wiki page

Links

- The SAML TF wiki page:
  - https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SAML
- VO Attribute Profile v 1.0:
  - https://twiki.cern.ch/twiki/bin/view/EMI/CommonSAMLProfileV1_0
- Send comments and feedback to
  - emi-jra1-sec-saml@eu-emi.eu

EUROPEAN MIDDLEWARE INITIATIVE

Thank you

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