EMI Common XACML Profile

Valery Tschopp (SWITCH)

EMI XACML task force

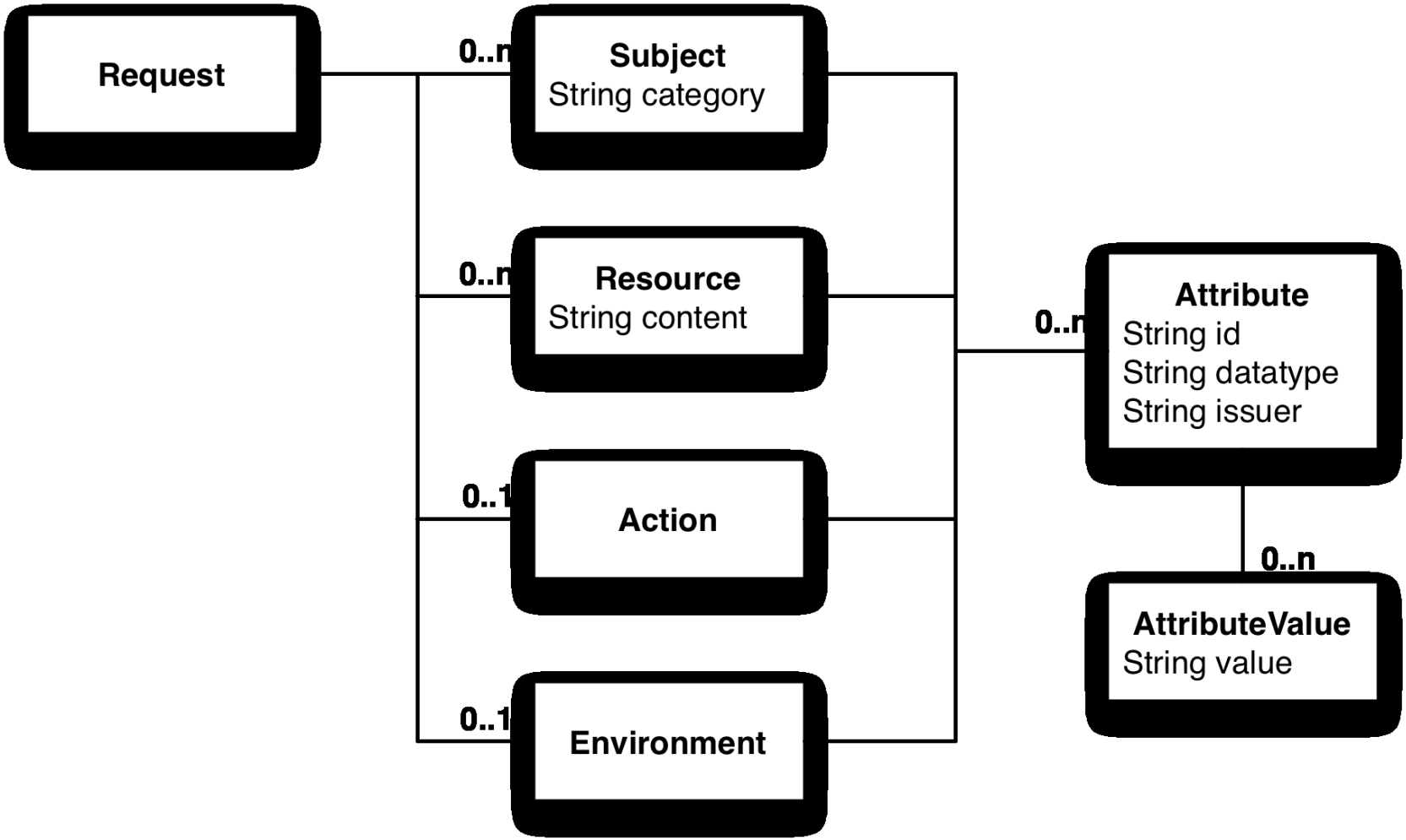
Common XACML Profile

- Goal
  - Define a common XACML profile for interoperable authorization between the three EMI middleware stacks.
- Requirements
  - In sync with the common SAML attribute profile
  - Uses dci-sec.og registered namespace
    - http://dci-sec.org/xacml/…

Common XACML Profile

- XML Namespaces used
  - http://dci-sec.org/xacml/attribute
  - http://dci-sec.org/xacml/datatype
  - http://dci-sec.org/xacml/algorithm
  - http://dci-sec.org/xacml/action
  - http://dci-sec.org/xacml/profile

XACML Authorization Request



Attribute DataTypes

- **Group DataType**

  Identifier:

  http://dci-sec.org/xacml/datatype/group

  Pattern: (/\w[-_.:\w]*)+

  Example: "/emi/test:group"

- **Role DataType**

  Identifier:

  http://dci-sec.org/xacml/datatype/role

  Pattern: (/\w[-_.:\w]*)+

  Example: "VO-Admin"

Environment Attribute

- **Profile Identifier**

  Identify the profile implemented by the request sender. MUST be present in the request

  AttributeId:

  http://dci-sec.org/xacml/attribute/profile-id

  DataType:

  http://www.w3.org/2001/XMLSchema#anyURI

  Value:

  http://dci-sec.org/xacml/profile/common-ce/1.0

Subject Attributes

- **Subject Identifier**

  Identify the submitter of the job to the CE. MUST be present in the request.

  AttributeId:

  urn:oasis:names:tc:xacml:1.0:subject:subject-id

  DataType:

  urn:oasis:names:tc:xacml:1.0:data-type:x500Name

  Value:

  X.509 distinguished name of the end-entity certificate. The DN format is RFC2253.

Subject Attributes (cont.)

- **Subject Identifier (Example)**

```
<ctx:Subject>
  <ctx:Attribute

AttributeId=”urn:oasis:names:tc:xacml:1.0:subject:subject-id”
    DataType=”urn:oasis:names:tc:xacml:1.0:data-type:x500Name”>
     <ctx:AttributeValue>
       CN=John Doe,DC=example,DC=org
     </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Subject Attributes (cont.)

- **Subject Issuer**

  DNs of all the root CA and all subordinate CA within the certificate chain identifying the job submitter. MUST be present in the request.

  AttributeId:

  http://dci-sec.org/xacml/attribute/subject-issuer

  DataType:

  urn:oasis:names:tc:xacml:1.0:data-type:x500Name

  Value:

  X.509 distinguished name of the root and issuing CAs of the certificate chain. The DN format is RFC2253.

Subject Attributes (cont.)

- **Subject Issuer (Example)**

```
<ctx:Subject>
  <ctx:Attribute
   AttributeId=”http://dci-sec.org/xacml/attribute/subject-issuer ”
    DataType=”urn:oasis:names:tc:xacml:1.0:data-type:x500Name”>
     <ctx:AttributeValue>
       CN=Example Issuing CA,DC=example,DC=org
     </ctx:AttributeValue>
    <ctx:AttributeValue>
       CN=Example Root CA,O=Example Org,C=CH
     </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Subject Attributes (cont.)

- **Virtual Organization (VO)**

  The subject's virtual organization membership.

  AttributeId:

  http://dci-sec.org/xacml/attribute/virtual-organization

  DataType:

  http://www.w3.org/2001/XMLSchema#string

  Value(s):

  Names of virtual organizations the subject is member of.

Subject Attributes (cont.)

- **Virtual Organization (Example)**

```
<ctx:Subject>
  <ctx:Attribute
    AttributeId=”http://dci-sec.org/xacml/attribute/virtual-organization”
    DataType=”http://www.w3.org/2001/XMLSchema#string”>
     <ctx:AttributeValue>
       atlas
     </ctx:AttributeValue>
    <ctx:AttributeValue>
       vo.example.org
     </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Subject Attributes (cont.)

- **Group**

  The subject group membership.

  AttributeId:

  http://dci-sec.org/xacml/attribute/group

  DataType:

  http://dci-sec.org/xacml/datatype/group

  Value(s):

  Names of the group the subject is member of.

Subject Attributes (cont.)

- **Group (Example)**

```
<ctx:Subject>
 <ctx:Attribute
  AttributeId=”http://dci-sec.org/xacml/attribute/group”
  DataType=”http://dci-sec.org/xacml/datatype/group”>
   <ctx:AttributeValue>
     /atlas/analysis
   </ctx:AttributeValue>
   <ctx:AttributeValue>
     /mygroup/test
   </ctx:AttributeValue>
 </ctx:Attribute>
</ctx:Subject>
```

Subject Attributes (cont.)

- **Primary Group**

  The subject primary group membership.

  AttributeId:

  http://dci-sec.org/xacml/attribute/group/primary

  DataType:

  http://dci-sec.org/xacml/datatype/group

  Value:

  Name of the primary group the subject is member of. The primary value MUST be present in the Group attribute value(s).

Subject Attributes (cont.)

- **Primary Group (Example)**

```
<ctx:Subject>
  <ctx:Attribute
    AttributeId=”http://dci-
sec.org/xacml/attribute/group/primary”
    DataType=”http://dci-sec.org/xacml/datatype/group”>
     <ctx:AttributeValue>
       /atlas/analysis
     </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Subject Attributes (cont.)

- **Role**

  Represents the roles assigned to the subject. The subject role MUST be scoped to a particular group or VO name.

  AttributeId:

  http://dci-sec.org/xacml/attribute/role

  DataType:

  http://dci-sec.org/xacml/datatype/role

  Issuer:

  Define the Group or VO scope name. MUST be present in the respective attribute (Group or VO)

  Value(s):

  Names of the role assigned to the subject.

Subject Attributes (cont.)

- **Role (Example)**

```
<ctx:Subject>
  <!-- role scoped to the group -->
  <ctx:Attribute
    AttributeId=”http://dci-sec.org/xacml/attribute/role”
    DataType=“http://dci-sec.org/xacml/datatype/role”
    Issuer="/atlas/analysis”>
   <ctx:AttributeValue>
     SoftwareManager
   </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Subject Attributes (cont.)

- **Primary Role**

  Represents the primary role assigned to the subject. The primary role MUST be scoped.

  AttributeId:

  http://dci-sec.org/xacml/attribute/role/primary

  DataType:

  http://dci-sec.org/xacml/datatype/role

  Issuer:

  Define the Group or VO scope name. MUST be present in the respective attribute (Group or VO)

  Value:

  Name of the primary role of the subject.

Subject Attributes (cont.)

- **Primary Role (Example)**

```
<ctx:Subject>
  <ctx:Attribute
     AttributeId=”http://dci-
sec.org/xacml/attribute/role/primary”
     DataType=“http://dci-sec.org/xacml/datatype/role”
     Issuer="/atlas/analysis”>
    <ctx:AttributeValue>
      SoftwareManager
    </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Subject Attributes (cont.)

- **Resource Owner**

  Identify the owner of the resources.

  AttributeId:

  http://dci-sec.org/xacml/attribute/resource-owner

  DataType:

  urn:oasis:names:tc:xacml:1.0:data-type:x500Name

  Value:

  X.509 distinguished name of the resource owner. The DN format is RFC2253.

Subject Attributes (cont.)

- **Resource Owner (Example)**

```
<ctx:Subject>
 <ctx:Attribute
  AttributeId=" http://dci-sec.org/xacml/attribute/resource-owner"
  DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name">
   <ctx:AttributeValue>
    CN=Batman,DC=Metropolis,DC=com
   </ctx:AttributeValue>
 </ctx:Attribute>
</ctx:Subject>
```

Resource Attributes

- **Resource Identifier**

  Identifies the CE, or a logical grouping of CEs, upon which the action to be authorized will be executed. MUST be present in the request.

  AttributeId:

  urn:oasis:names:tc:xacml:1.0:resource:resource-id

  DataType:

  http://www.w3.org/2001/XMLSchema#string

  Value:

  Identifier of the resource

Resource Attributes (cont.)

- **Resource Identifier (Example)**

```
<ctx:Resource>
  <ctx:Attribute

AttributeId=”urn:oasis:names:tc:xacml:1.0:resource:resource-id”
   DataType=”http://www.w3.org/2001/XMLSchema#string”>
     <ctx:AttributeValue>
       http://example.org/ce/cream-ce-1
     </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Resource>
```

Action Attributes

- **Action Identifier**

  Identifies the action being performed on the CE. MUST be present in the request.

  AttributeId:

  urn:oasis:names:tc:xacml:1.0:action:action-id

  DataType:

  http://www.w3.org/2001/XMLSchema#string

  Value:

  Action to be authorized on the resource.

Action Attributes (cont.)

- **Action Identifier Values**
  - We should define a list of Action values. This list is not an absolute constraint, but should be used if applicable.
  - CREAM CE action values (as example):

http://glite.org/xacml/action/ce/job/register
http://glite.org/xacml/action/ce/job/cancel
http://glite.org/xacml/action/ce/job/purge
http://glite.org/xacml/action/ce/job/get-info
http://glite.org/xacml/action/ce/job/suspend
http://glite.org/xacml/action/ce/job/resume
http://glite.org/xacml/action/ce/job/list
http://glite.org/xacml/action/ce/job/set-lease
http://glite.org/xacml/action/ce/lease/list
http://glite.org/xacml/action/ce/lease/get
http://glite.org/xacml/action/ce/lease/set
http://glite.org/xacml/action/ce/lease/delete
http://glite.org/xacml/action/ce/enable-job-submission
http://glite.org/xacml/action/ce/disable-job-submission

Action Attributes (cont.)

- **Action Identifier Values (cont.)**
  - A-REX actions (as example):
    - **AttributeId**: http://www.nordugrid.org/schemas/policy-arc/types/a-rex/joboperation **AttributeValue**: Create
    - **AttributeId**: http://www.nordugrid.org/schemas/policy-arc/types/a-rex/joboperation **AttributeValue**: Modify
    - **AttributeId**: http://www.nordugrid.org/schemas/policy-arc/types/a-rex/joboperation **AttributeValue**: Read
    - **AttributeId**: http://www.nordugrid.org/schemas/policy-arc/types/a-rex/operation **AttributeValue**: Admin
    - **AttributeId**: http://www.nordugrid.org/schemas/policy-arc/types/a-rex/operation **AttributeValue**: Info
  - EMI Execution Service actions:
    - Unknown, require examples or requirements

Thank you

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