Table of Contents

Common CE XACML Authorization Profile (v.0)

First draft for the common CE XACML authorization profile.

Introduction

References

[XACML]
OASIS Standard, eXtensible Access Control Markup Language, Version 2.0, February 2005. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[XACML-CREAM]
XACML Profile for the gLite CREAM CE (Draft). https://edms.cern.ch/document/1078881/

[SAML-EMI]
EMI Common SAML Attributes. https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SAML

[RFC2253]
http://www.ietf.org/rfc/rfc2253.txt

Notation

The examples use the following namespace prefixes:

The prefix `ctx`
stands for the XACML context namespace (`urn:oasis:names:tc:xacml:2.0:context`)

XML Namespaces

The XACML common CE profile syntax is defined in a schema associated with the following XML namespaces:

- `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`

Subject Attributes

Subject Identifier

Identify the submitter of the job to the CE. The attribute 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`

AttributeValue Multiplicity
`1`

Value(s)
X.509 distinguished name of the end-entity certificate. The DN format is RFC2253, e.g. "CN=John Doe,DC=example,DC=org"

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 Issuer

DNs of the subject of all the root certificate authority and all subordinate certificate authorities within the certificate chain identifying the job submitter. The attribute SHOULD be present in the request.

For example, assume:

- certificate C is the end entity certificate
- subordinate certificate authority B signed certificate C
- root certificate authority A signed subordinate certificate authority B

then this attribute would contain the subject DN for certificate authorities A and B.

AttributeId
`http://dci-sec.org/xacml/attribute/subject-issuer`
DataType
`urn:oasis:names:tc:xacml:1.0:data-type:x500Name`
AttributeValue Multiplicity
`1..N`
Value(s)
X.509 distinguished name of the authority(ies) which issued the job submitter's identity. The DN format is RFC2253.

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=QV Schweiz ICA,OU=Issuing Certificate Authority,O=QuoVadis Trustlink Schweiz AG,C=CH
    </ctx:AttributeValue>
    <ctx:AttributeValue>
      CN=QuoVadis Root Certification Authority,OU=Root Certification Authority,O=QuoVadis Limited
    </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Virtual Organization (VO)

The subject's virtual organization membership.

TODO: add link to the common SAML profile

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

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

AttributeValue Multiplicity

`1..N`

Value(s)

Names of virtual organizations the subject is member of.

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>
```

Comments

Aleksandr Konstantinov

Maybe accompanied by issuer - like VOMS SN.

Group Membership

The subject group membership.

TODO: add link to the common SAML profile.

AttributeId

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

DataType

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

AttributeValue Multiplicity

`1..N`

Value(s)

Names of the group the subject is member of.

Example

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

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

Group name or VO name scope of the role.

AttributeValue Multiplicity

`1..N`

Value(s)

Names of the role assigned to the subject.

Example

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

Questions

- is an attribute uniquely identified by the {AttributeId, DataType, Issuer} tuple (see [XACML] 5.37 AttributeDesignatorType)?

Primary Membership

Represents the default membership attribute assigned to the subject. The membership is either a scoped role or a group.

AttributeId

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

DataType

`http://dci-sec.org/xacml/datatype/role` or
`http://dci-sec.org/xacml/datatype/group`

Issuer

If the primary membership is a scoped role, then it contains the role scope. Otherwise the **Issuer** is not set.

AttributeValue Multiplicity

`1`

Value(s)

Name of the primary role assigned to the subject, or name of the primary group the subject is member of.

Example

```
<ctx:Subject>
  <ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/primary
     DataType= http://dci-sec.org/xacml/datatype/role
```

```
     Issuer="atlas">
    <ctx:AttributeValue>
      Tester
    </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Questions

- isn't it too complicate ?
- better to use 2 different attributes
  `http://dci-sec.org/xacml/attribute/role/primary` and
  `http://dci-sec.org/xacml/attribute/group/primary` ?

Comments

Aleksandr Konstantinov
: maybe add VO to Role and Group.

Resource Owner

Identify the owner of the resource.

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

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

AttributeValue Multiplicity
: `1`

Value(s)
: X.509 distinguished name of the end-entity certificate.

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=Jane Doe,DC=example,DC=org
    </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Subject>
```

Comments

- This attribute is required by UNICORE

Resource Attributes

Resource Identifier

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

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

DataType
`http://www.w3.org/2001/XMLSchema#string`
AttributeValue Multiplicity
`1`
Value(s)
???

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>
```

Questions

- Is the **DataType** `...#string` correct to identity a resource, why not `...#anyURI` ?
- Should we formalize the resource identifier values ?

Comments

Karsten Schwank
: I think it is a good idea to formalize the the values, otherwise I could imagine the risk of duplicates within a large system is too big and formalized values would keep the policies human readable. Depending on the kind of formalization this could even allow further automatic, semantic evaluation of the policies. Same thing for the actions.

Krzysztof Benedyczak
: I vote for URI. In our case {UNICORE} it is an URL of the Web Service.

Aleksandr Konstantinov
: too generic. Or it needs an attribute/scoping to define which kind of identifier it is - URL, SN, WS-Addressing, path. Also it is not clear to me how to specify resource at service which can't be represented as combined URL. Like job handled by Execution Service - with job id XML-ized and ES represented by URL or EPR.

Action Attributes

Action Identifier

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

Identifier
`urn:oasis:names:tc:xacml:1.0:action:action-id`
DataType
`http://www.w3.org/2001/XMLSchema#string`
AttributeValue Multiplicity
`1`
Value(s)
???

TODO:

- define the list of action value

Questions

- values multiplicity: `1` or `1..N` ?

Comments

Krzysztof Benedyczak
: My remark is that here (in opposite what is in the current CREAM profile) we want any string - without any restrictions. However we may obey some predefined actions if those are applicable.

Aleksandr Konstantinov
: probably needs some scoping to define kind of service involved. Or there need to be some rules how to compose the string representing action which would allow to distinguish "create" action of Storage from "create" of ES.

Environment Attributes

Profile Identifier

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

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

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

AttributeValue Multiplicity
: `1`

Value(s)
: The attribute value MUST be `http://dci-sec.org/xacml/profile/common-ce/1.0`

Example

```
<ctx:Environment>
  <ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/profile-id
      DataType= http://www.w3.org/2001/XMLSchema#anyURI >
     <ctx:AttributeValue>
       http://dci-sec.org/xacml/profile/common-ce/1.0
     </ctx:AttributeValue>
  </ctx:Attribute>
</ctx:Environment>
```

Data-types

Defines the **DataType** s used in the XACML attributes.

Group DataType

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

TODO: add description and link to the common SAML profile

Role DataType

Identifier

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

TODO: add description and link to the common SAML profile

FQAN DataType

Identifier

```
http://dci-sec.org/xacml/datatype/fqan
```

TODO: add description and link to the common SAML profile

Question

- is the FQAN still needed ???

This topic: EMI > XACMLCommonCEProfile
Topic revision: r14 - 17-Dec-2010 - 17:50:29 - ValeryTschopp