Table of Contents

Common XACML Authorization Profile, Version 1.1.1

Revised version 1.1.1 of for the **Common XACML Authorization Profile** for EMI.

History

Version	Date	Comment	Author/Partner
1.0	05/05/2011	Initial version 1.0 of the profile.	Valery Tschopp/SWITCH
1.1	08/11/2011	Revised version 1.1 of the profile. Comments from XACML working group integrated.	Valery Tschopp/SWITCH
1.1.1	13/11/2012	Revised version 1.1.1 of the profile. XACML actions for EMI-ES added.	Valery Tschopp/SWITCH, Aleksandr Konstantinov

Introduction

Document Identifier: http://dci-sec.org/xacml/profile/common-authz/1.1

Location:
https://twiki.cern.ch/twiki/pub/EMI/EmiJra1T4XACML/EMI-DOC-JRA1-CommonXACMLProfile-v1.1.1.doc

Contact: emi-jra1-sec@eu-emiNOSPAMPLEASE.eu

Glossary

Authorization decision
: The result of evaluating applicable policy, returned by the **PDP** to the **PEP**. A function that evaluates to `Permit`, `Deny`, `NotApplicable` or `Indeterminate`, and (optionally) a set of **obligations**.

Decision request
: The request sent by a **PEP** to a **PDP** to render an **authorization decision**.

Obligation
: An operation specified in a policy that should be performed by the **PEP** in conjunction with the enforcement of an **authorization decision**.

PAP
: Policy Administration Point. The system entity that creates policies.

PDP
: Policy Decision Point. The system entity that evaluates applicable policy and renders an **authorization decision**.

PEP
: Policy Enforcement Point. The system entity that performs access control, by making **decision requests** and enforcing **authorization decisions**.

Normative 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/

[XACML-WN]

XACML Grid Worker Node Authorization Profile, Version 1.0.1.
https://edms.cern.ch/document/1058175
[SAML-EMI]
EMI Common VO SAML Attributes Profile, Version 1.0.1.
https://twiki.cern.ch/twiki/bin/view/EMI/CommonSAMLProfileV1_0_1
[RFC2253]
LDAPv3 Distinguished Names. http://www.ietf.org/rfc/rfc2253.txt

Notation

The examples use the following XACML namespace prefixes:

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

XML Namespaces

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

- `http://dci-sec.org/xacml/action`
- `http://dci-sec.org/xacml/attribute`
- `http://dci-sec.org/xacml/profile`
- `http://dci-sec.org/xacml/obligation`

Decision Request

The `Request` element is a top-level element in the XACML context schema.The `Request` element contains `Subject`, `Resource`, `Action` and `Environment` elements.

Environment Attributes

Within the element `Request` of the XACML context, the `Environment` element contains a set of attributes of the environment, that are relevant to an authorization decision and are independent of a particular subject, resource or action.

Profile Identifier Attribute

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`
AttributeValue
The attribute value MUST be `http://dci-sec.org/xacml/profile/common-authz/1.1`

Example

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

```
    <xacml-ctx:AttributeValue>
      http://dci-sec.org/xacml/profile/common-authz/1.1
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Environment>
```

Subject Attributes

Within the element `Request` of the XACML context, the `Subject` element identifies a subject, an actor, by listing a sequence of attributes associated with the subject.

Subject Identifier Attribute

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`
AttributeValue
X.509 distinguished name of the end-entity certificate. The value MUST be in RFC2253 format, e.g. "CN=John Doe,DC=example,DC=org"

Example

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

Subject Issuer Attribute

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`
AttributeValue(s)
X.509 distinguished name of the authority(ies) which issued the job submitter's identity. The value MUST be in RFC2253 format.

Example

```
<xacml-ctx:Subject>
  <xacml-ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/subject-issuer
      DataType= urn:oasis:names:tc:xacml:1.0:data-type:x500Name >
    <xacml-ctx:AttributeValue>
      CN=QV Schweiz ICA,OU=Issuing Certificate Authority,O=QuoVadis Trustlink Schweiz AG,C=CH
    </xacml-ctx:AttributeValue>
    <xacml-ctx:AttributeValue>
      CN=QuoVadis Root Certification Authority,OU=Root Certification Authority,O=QuoVadis Limited
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Subject>
```

Virtual Organization (VO) Attribute

The subject's virtual organization membership.

AttributeId
`http://dci-sec.org/xacml/attribute/virtual-organization`
DataType
`http://www.w3.org/2001/XMLSchema#string`
AttributeValue Multiplicity
`1..N`
AttributeValue(s)
Name of the virtual organization(s) the subject is member of. The value MUST respect the following grammar:

```
vo ::= [a-zA-Z0-9][a-zA-Z0-9_.-]*
```

Example

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

Group Attribute

The subject group membership.

AttributeId
`http://dci-sec.org/xacml/attribute/group`
DataType
`http://www.w3.org/2001/XMLSchema#string`
AttributeValue Multiplicity
`1..N`
AttributeValue(s)
Groups the subject is member of. The value MUST respect the following grammar:

```
group ::= '/' groupname | group '/' groupname
groupname :: = [a-zA-Z0-9][a-zA-Z0-9_.-]*
```

The first path element of each group MUST be the VO name. i.e. if the VO name is `atlas`, then each group must start with `/atlas`

Example

```
<xacml-ctx:Subject>
  <xacml-ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/group
      DataType= http://www.w3.org/2001/XMLSchema#string >
    <xacml-ctx:AttributeValue>
      /dteam
    </xacml-ctx:AttributeValue>
    <xacml-ctx:AttributeValue>
      /atlas/analysis
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Subject>
```

Primary Group Attribute

The subject primary group membership.

AttributeId
`http://dci-sec.org/xacml/attribute/group/primary`
DataType
`http://www.w3.org/2001/XMLSchema#string`
AttributeValue Multiplicity
`1`
AttributeValue
Primary group of the subject. The value MUST also appear in the `http://dci-sec.org/xacml/attribute/group` attribute values and MUST respect the same format.

Example

```
<xacml-ctx:Subject>
  <xacml-ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/group/primary
      DataType= http://www.w3.org/2001/XMLSchema#string >
    <xacml-ctx:AttributeValue>
      /atlas/analysis
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Subject>
```

Role Attribute

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

AttributeId
`http://dci-sec.org/xacml/attribute/role`
DataType
`http://www.w3.org/2001/XMLSchema#string`
Issuer
Scope of the roles. The **Issuer** value expressed MUST have a corresponding `http://dci-sec.org/xacml/attribute/group` attribute value.
AttributeValue Multiplicity
`1..N`
AttributeValue(s)
Role assigned to the subject. The value MUST respect the following grammar:

```
role ::= [a-zA-Z0-9][a-zA-Z0-9_.-]*
```

Example

```
<xacml-ctx:Subject>
  <!-- role scoped to group /atlas/analysis -->
  <xacml-ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/role
      DataType= http://www.w3.org/2001/XMLSchema#string
      Issuer="/atlas/analysis">
    <xacml-ctx:AttributeValue>
      SoftwareManager
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
  <!-- roles scoped to group /dteam -->
  <xacml-ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/role
      DataType= http://www.w3.org/2001/XMLSchema#string
      Issuer="/dteam">
    <xacml-ctx:AttributeValue>
      Tester
    </xacml-ctx:AttributeValue>
    <xacml-ctx:AttributeValue>
      Developer
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Subject>
```

Primary Role Attribute

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

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

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

Issuer
Scope of the primary role. The **Issuer** value expressed MUST have a corresponding `http://dci-sec.org/xacml/attribute/group` attribute value.

AttributeValue Multiplicity
`1`

AttributeValue
Primary role assigned to the subject. The value MUST also appear in the `http://dci-sec.org/xacml/attribute/role` attribute values and MUST respect the same format.

Example

```
<xacml-ctx:Subject>
  <xacml-ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/role/primary
     DataType= http://www.w3.org/2001/XMLSchema#string
     Issuer="/dteam">
    <xacml-ctx:AttributeValue>
      Tester
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Subject>
```

Subject Key Info Attribute

Identify the effective end-entity user by its certificate and chain.

AttributeId
`urn:oasis:names:tc:xacml:1.0:subject:key-info`

DataType
`http://www.w3.org/2001/XMLSchema#base64Binary`

AttributeValue Multiplicity
`1..n`

AttributeValue
The base64 encoded DER certificate and its chain used to identify the subject. The base64 encoded DER private key MUST NOT be included. It is RECOMMENDED that the chain be ordered such that the last certificate in the chain be the certificate closest to the root CA, the second to last should be the certificate signed by the previous, etc.

The base64 encoded DER certificate is basically the base64 part of a PEM encoded certificate, but **without** the PEM header (`-----BEGIN CERTIFICATE-----`) and footer (`-----END CERTIFICATE-----`).

Example

```
<xacml-ctx:Subject>
  <xacml-ctx:Attribute
     AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info"
     DataType="http://www.w3.org/2001/XMLSchema#base64Binary">
    <xacml-ctx:AttributeValue>
MIIECDCCAvCgAwIBAgIKG8PTQQAAAAAQbjANBgkqhkiG9w0BAQUFADBnMQswCQYD
VQQGEwJDSDFAMD4GA1UEChM3U3dpdGNoIC0gVGVsZWluZm9ybWF0aWtkaWVuc3Rl
...
ALXkXETM6VNPCbVUi6DmigpKj0qaSSGsgE72jcnpwXer25D8+6z+7cNdR6VCn8y9
RNoce0bwhE8qQ5h7tGpjAVM0Rjb/ycyjZTmGcw==
    </xacml-ctx:AttributeValue>
    <xacml-ctx:AttributeValue>
MIIEZTCCA02gAwIBAgISSWITCHslcs+CA+cRLSign+KUMA0GCSqGSIb3DQEBBQUA
MGwxCzAJBgNVBAYTAkNIMUAwPgYDVQQKEzdTd2l0Y2ggLSBUZWxlaW5mb3JtYXRp
...
40YjA+j0Mli6VNJT2f6QOID82qombUPIYmWyxbSIZ2+zEm3xId7TCzIUQfZnOvmW
j0w6J+YaW/fFsyEPDCwnBYI82Nsr78RYxR9CkonpYaP/tTCKsFnY4qPp6nAth9cH
tJ4b/PueM3bpawb2mH1jomBolTCsbA==
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Subject>
```

Resource Attributes

Within the element `Request` of the XACML context, the `Resource` element specifies information about the resource to which access is requested, by listing a sequence of attributes associated with the resource.

Resource Identifier Attribute

Identifies the data, service or system component, 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`

AttributeValue
The unique identifier of the data, service or system component. It is RECOMMENDED to use an URI like identifier (e.g. `http://example.org/cream-ce-1`)

Example

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

```
    <xacml-ctx:AttributeValue>
      http://example.org/ce/cream-ce-1
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Resource>
```

Resource Owner Attribute

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`
AttributeValue
X.509 distinguished name of the end-entity certificate owning the resource. The value MUST be in RFC2253 format.

Example

```
<xacml-ctx:Resource>
  <xacml-ctx:Attribute AttributeId= http://dci-sec.org/xacml/attribute/resource-owner
      DataType= urn:oasis:names:tc:xacml:1.0:data-type:x500Name >
    <xacml-ctx:AttributeValue>
      CN=Jane Doe,DC=example,DC=org
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Resource>
```

Comments

- This attribute is used by UNICORE.

Action Attributes

Within the element `Request` of the XACML context, the `Action` element specifies the requested action on the resource, by listing a set of attributes associated with the action.

Action Identifier Attribute

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`
AttributeValue
Identifier of the action being performed. It is RECOMMENDED to use an action identifier in the URI form `http://dci-sec.org/xacml/action/<ACTION>`, where `<ACTION>` defines the action being performed.

Attribute Values

To represent any action, you SHOULD use the following value: `http://dci-sec.org/xacml/action/ANY`

For the EMI Execution Service (EMI-ES), the following action attribute values have been defined:

Attribute Value (EMI-ES)	Description
`http://www.eu-emi.eu/es/2010/12/creation`	Operation to submit job - activity in terms of EMI ES - description to service
`http://www.eu-emi.eu/es/2010/12/activity`	Covers operation which allow to obtain information about jobs handled by service - list, status, extended status (info)
`http://www.eu-emi.eu/es/2010/12/activitymanagement`	Operations which affect status of activity - pause, cancel, etc. - and operations to obtain information about activity - status, extended status
`http://www.eu-emi.eu/es/2010/12/resourceinfo`	Operations to obtain information about service
`http://www.gridsite.org/namespaces/delegation-21`	Operations to perform X.509 delegation procedure

If the service supports staging data and want to perform additional authorization, it SHOULD use the action value `http://www.eu-emi.eu/es/2010/12/creation` for staging into StageIn location. And it SHOULD use the action value `http://www.eu-emi.eu/es/2010/12/activitymanagement` for authorizing access to session directory and staging from StageOut location.

Example

```
<xacml-ctx:Action>
  <xacml-ctx:Attribute AttributeId= urn:oasis:names:tc:xacml:1.0:action:action-id
     DataType= http://www.w3.org/2001/XMLSchema#string >
    <xacml-ctx:AttributeValue>
      http://dci-sec.org/xacml/action/ANY
    </xacml-ctx:AttributeValue>
  </xacml-ctx:Attribute>
</xacml-ctx:Action>
```

Authorization Decision

The `Response` element is a top-level element in the XACML context schema. The `Response` element encapsulates the authorization decision. It includes a sequence of one or more results, with one `Result` element per requested resource.

Obligations

The `Result` element represents an authorization decision result for the requested resource. It MAY includes a set of obligations that MUST be fulfilled by the PEP. If the PEP does not understand or cannot fulfill an obligation, then it MUST act as if the PDP had denied access to the requested resource.

The `Obligation` element contains an identifier for the obligation and a set of attribute assignment that form arguments of the action defined by the obligation.

Map User to Local Environment Obligation

This obligation is used within a policy to signify that a permitted job must be run under a particular user within a local environment . It is up to the a PEP to determine the effective user mapping for the local environment, based on the subject information of the decision request.

Identifier

`http://dci-sec.org/xacml/obligation/map-local-user`

FulfillOn

`Permit`

AttributeAssignment

None supported

Example

```
<xacml:Obligation
   ObligationId= http://dci-sec.org/xacml/obligation/map-local-user
   FulfillOn= Permit  />
```

Map User to POSIX Environment Obligation

This obligation is used to indicate the job MUST be mapped to the local POSIX account specified by the given attribute assignments.

Identifier

`http://dci-sec.org/xacml/obligation/map-local-user/posix`

FulfillOn

`Permit`

AttributeAssignment(s)

The following attributes are supported:

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

The user-id, group-id, and primary group-id attributes, when used in this obligation MUST provide the POSIX login name, primary group name, and secondary group names.

Example

```
<xacml:Obligation
   ObligationId= http://dci-sec.org/xacml/obligation/map-local-user/posix
   FulfillOn= Permit >
  <xacml:AttributeAssignment
   AttributeId= http://dci-sec.org/xacml/attribute/user-id
   DataType= http://www.w3.org/2001/XMLSchema#string >
     jsmith
  </xacml:AttributeAssignment>
  <xacml:AttributeAssignment
   AttributeId= http://dci-sec.org/xacml/attribute/group-id/primary
   DataType= http://www.w3.org/2001/XMLSchema#string >
    staff
  </xacml:AttributeAssignment>
  <xacml:AttributeAssignment
   AttributeId= http://dci-sec.org/xacml/attribute/group-id
   DataType= http://www.w3.org/2001/XMLSchema#string >
    staff
  </xacml:AttributeAssignment>
  <xacml:AttributeAssignment
   AttributeId= http://dci-sec.org/xacml/attribute/group-id
   DataType= http://www.w3.org/2001/XMLSchema#string >
    data
  </xacml:AttributeAssignment>
</xacml:Obligation>
```

Obligation Attribute Assignments

The `AttributeAssignment` element is used for including arguments in an `Obligation` element.

User-Id Attribute Assignment

Identifier
`http://dci-sec.org/xacml/attribute/user-id`
DataType
`http://www.w3.org/2001/XMLSchema#string`
Multiplicity
`1`

Gives the login name, or username, of the user within the local environment. Within an obligation, this attribute assignment SHALL appear only once.

Group-Id Attribute Assignment

Identifier
`http://dci-sec.org/xacml/attribute/group-id`
DataType
`http://www.w3.org/2001/XMLSchema#string`
Multiplicity
`1..N`

Gives the names of the group to which the user is a member. If a primary group-id attribute is also provide in the obligation, then the primary group-id name MUST also appear in this list.

Primary Group-Id Attribute Assignment

Identifier
`http://dci-sec.org/xacml/attribute/group-id/primary`
DataType
`http://www.w3.org/2001/XMLSchema#string`
Multiplicity
`1`

The primary group name of the user specified in the obligation. Within an obligation, this attribute assignment SHALL appear only once.

-- ValeryTschopp - 20-Oct-2011

This topic: EMI > CommonXACMLProfileV1_1
Topic revision: r12 - 2013-01-31 - ValeryTschoppExCern