

# Table of Contents

<b>Common SAML attribute profile Strawman proposal v. 2.....</b>	<b>1</b>
Required information.....	1
SAML Attribute naming.....	1
Attribute name comparison.....	1
Profile specific XML attributes.....	1
Profile specific XML data types.....	1
Attribute definitions.....	2
Virtual organization (VO).....	2
Groups.....	2
Roles.....	2
Primary VO membership attribute.....	3

# Common SAML attribute profile Strawman proposal v. 2

This is the strawman proposal for a SAML EMI common attribute profile. This document is structured following the convention suggested by OASIS on SAML attribute profile document structure (more or less).

## Required information

**Identification:** <http://dci-sec.org/saml/profile/virtual-organization/1.0>

**Contact information:** [emi-jral-sec-saml@eu-emiSPAMNOT.eu](mailto:emi-jral-sec-saml@eu-emiSPAMNOT.eu)

**Description:** ...

**Updates:** ...

## SAML Attribute naming

The NameFormat XML attribute in <Attribute> elements MUST be

`urn:oasis:names:tc:SAML:2.0:attrname-format:uri`

## Attribute name comparison

Two <Attribute> elements refer to the same SAML attribute if and only if their Name XML attribute values are equal in the sense of URI matching rules [TODO: insert correct reference here].

## Profile specific XML attributes

No additional XML attributes are defined for use with the <Attribute> element.

## Profile specific XML data types

The following XML schema types are used in this schema

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
  targetNamespace="http://dci-sec.org/saml/profile/virtual-organization/1.0"
  elementFormDefault="qualified" xmlns="http://www.w3.org/2001/XMLSchema"
  xmlns:dci-sec="http://dci-sec.org/saml/profile/virtual-organization/1.0">

  <annotation>
    <documentation></documentation>
  </annotation>

  <simpleType name="group">
    <restriction base="string">
      <pattern value="insert_here_pattern_to_match_unix_paths"></pattern>
    </restriction>
  </simpleType>

  <simpleType name="role">
    <restriction base="string">
    </restriction>
  </simpleType>
```

```

    </simpleType>

    <attribute name="vo" type="string"/>
    <attribute name="group" type="dci-sec:group"/>

</schema>

```

## Attribute definitions

### Virtual organization (VO)

This multi-valued attribute represents the SAML assertion subject's virtual organization membership.

**Name:** `http://dci-sec.org/saml/attribute/virtual-organization`

The `<AttributeValue>` elements contains a string 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/
  <AttributeValue xsi:type="xs:string">atlas</AttributeValue>
  <AttributeValue xsi:type="xs:string">example.vo.org</AttributeValue>
</Attribute>

```

### Groups

This multi-valued attribute represents the SAML assertion subject's VO group membership.

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

Each `<AttributeValue>` element is of type `dci-sec:group`. Each attribute value may also have a `dci-sec:vo` attribute to scope the group to a specific vo (when the scope is not evident from the attribute value itself).

```

<Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="http://dci-sec.org/

  <AttributeValue xsi:type="dci-sec:group">/atlas/production</AttributeValue>

  <AttributeValue
    xsi:type="dci-sec:group"
    dci-sec:vo="example.vo.org">analysis</AttributeValue>

</Attribute>

```

### Roles

This multi-valued attribute represents the roles assigned to the subject.

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

Each `<AttributeValue>` element is of type `dci-sec:role`. Each attribute value may also have an optional `dci-sec:group` to scope it to a specific group. The `dci-sec:vo` attribute may also be used to link a role to a specific VO.

```

<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>

    <!-- below an example of vo scoped role attribute -->
    <AttributeValue
      xsi:type="dci-sec:role"
      dci-sec:vo="example.vo.org">CrustyTheClown</AttributeValue>

  </Attribute>

```

## Primary VO membership attribute

This single-valued attribute represents the default membership attribute assigned to the subject

**Name:** <http://dci-sec.org/saml/attribute/primary>

The <AttributeValue> either a string that refers to either a group or role which is part of the groups or roles attributes defined above. The xml schema type used for the attribute value is used to understand if it's a primary group or role attribute.

```

<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:group">/atlas/production</AttributeValue>
</Attribute>

```

-- AndreaCeccanti - 09-Nov-2010

---

This topic: EMI > CommonProfileStrawmanProposalV2

Topic revision: r1 - 09-Nov-2010 - 17:33:32 - AndreaCeccanti



Copyright &© by the contributing authors. All material on this collaboration platform is the property of the contributing authors.

Ideas, requests, problems regarding TWiki? Send feedback