EUROPEAN MIDDLEWARE INITIATIVE

VIRTUAL ORGANIZATION ATTRIBUTE PROFILE

EMI DOCUMENT

Document identifier:	**EMI-SAML-VO-Attribute-Profile-v1.1.odt**
Date:	**13/10/2011**
Activity:	
Lead Partner:	
Document status:	
Document link:	

Abstract:
This document describes a common EMI SAML profile for expressing Virtual Organization membership attributes.

Document Log

Issue	Date	Comment	Author / Partner
1			Andrea Ceccanti
2			
3			

Document Change Record

Issue	Item	Reason for Change
1		
2		
3		

TABLE OF CONTENTS

Table of Contents

1. COMMON VIRTUAL ORGANIZATION PROFILE

The EMI Common Virtual Organization attribute profile defines the representation of Virtual Organization membership attributes as SAML attributes.

1.1. REQUIRED INFORMATION

Identification: `http://dci-sec.org/saml/profile/virtual-organization/1.0`

Contact information: emi-jra1-sec-saml@eu-emiSPAMNOT.eu

Description: Given below.

Updates: None.

1.2. SAML ATTRIBUTE NAMING

The `NameFormat` XML attribute in `<Attribute>` elements MUST be:

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

1.2.1 SAML 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 (RFC 3986).

1.3. PROFILE SPECIFIC XML ATTRIBUTES

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

1.4. PROFILE SPECIFIC XML DATA TYPES

The following XML schema types are used in this profile:

```
<?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">

    <attribute name="scope" type="xsd:string"/>

</schema>
```

1.5. ATTRIBUTE DEFINITIONS

1.5.1 Virtual organization

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 (of type `xsd:string`) define the name of the VO the subject is member of.

Constraints:

- The VO attribute value MUST respect the following grammar:

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

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="xsd:string">atlas</AttributeValue>

  <AttributeValue xsi:type="xsd:string">example.vo.org</AttributeValue>

</Attribute>
```

1.5.2 Groups

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

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

The `<AttributeValue>` elements (of type `xsd:string`) define the VO groups the subject is member of.

Constraints:

- Each group attribute value MUST respect the following grammar:

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

Example:

```
<Attribute

      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="http://dci-sec.org/saml/attribute/group">

  <AttributeValue xsi:type="xsd:string">/atlas</AttributeValue>

  <AttributeValue xsi:type="xsd:string">/atlas/it</AttributeValue>

</Attribute>
```

1.5.3 Primary group

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

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

The `<AttributeValue>` element (of type `xsd:string`) defines the primary group for the subject.

Constraints:

- The value expressed by this attribute MUST also appear in the `http://dci-sec.org/saml/attribute/group` attribute included in the SAML assertion.
- All the constraints defined for the `http://dci-sec.org/saml/attribute/group` attribute are to valid also for this attribute.

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="xsd:string">/atlas/it</AttributeValue>

</Attribute>
```

1.5.4 Roles

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

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

The `<AttributeValue>` elements (of type `xsd:string`) define the roles the subject is member of. Each `<AttributeValue>` MUST be scoped to a group using the `dci-sec:scope` attribute.

Constraints:

- Each role attribute value MUST respect the following grammar:

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

- The value of the `dci-sec:scope` attribute must respect the grammar defined for group names, i.e.:

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

- 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="xsd:string"

      dci-sec:scope="/atlas/it">lcgadmin</AttributeValue>

</Attribute>
```

1.5.5 Primary role

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

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

The `<AttributeValue>` element (of type `xsd:string`) defines the primary role for the subject. The `<AttributeValue>` MUST be scoped to a group, using the `dci-sec:scope` attribute.

Constraints:

- All the constraints specfied for the `http://dci-sec.org/saml/attribute/role` attribute values apply to this attribute.
- The value expressed by this attribute MUST also appear in the `http://dci-sec.org/saml/attribute/role` 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/primary">

   <AttributeValue

      xsi:type="xsd:string"

      dci-sec:scope="/atlas/it">lcgadmin</AttributeValue>

</Attribute>
```