VOMS SAML Status

Andrea Ceccanti

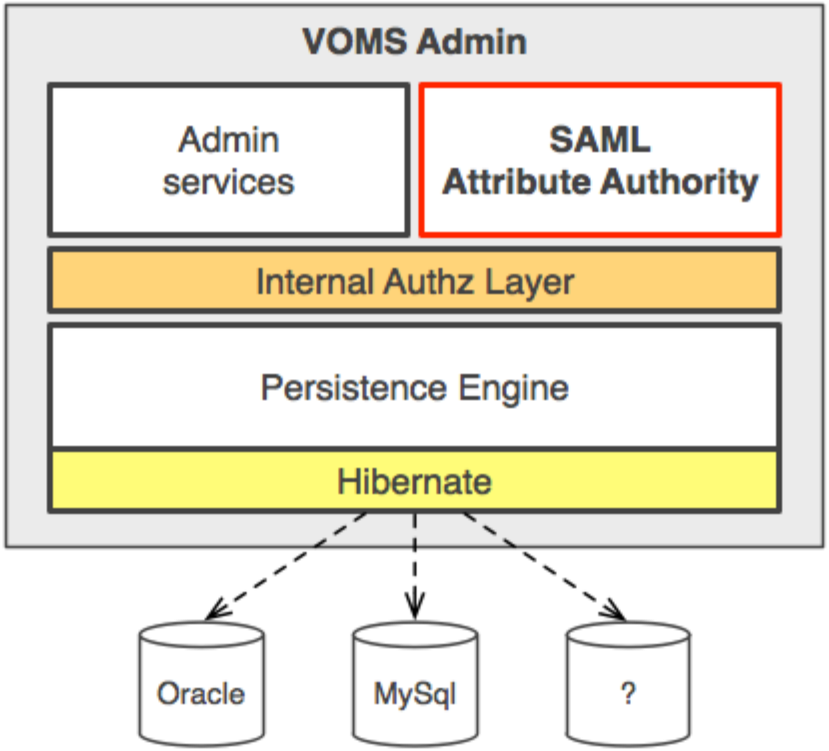
EMI Security Workshop
May 2010, CERN

www.eu-egee.org

Information Society and Media

What is VOMS SAML?

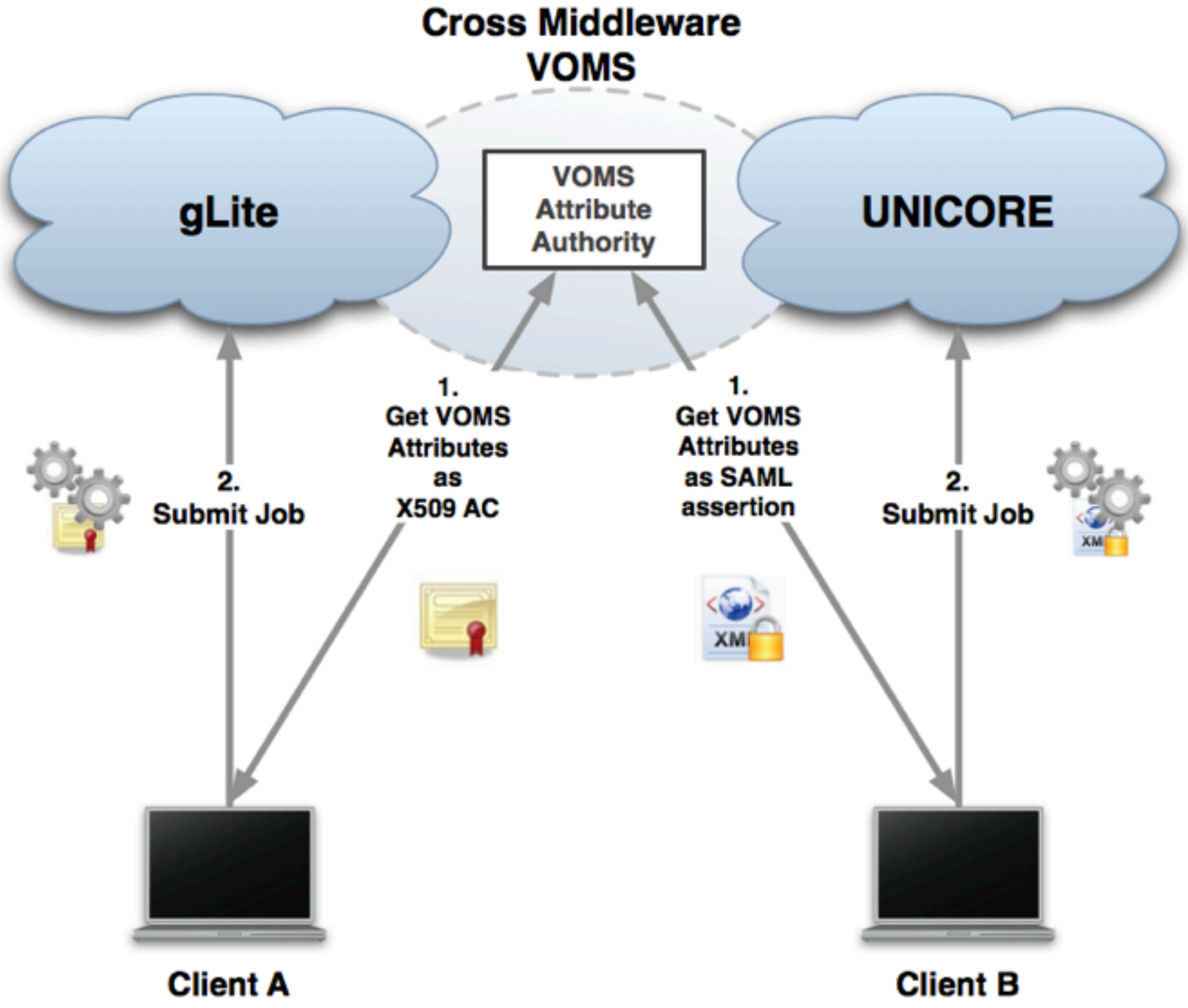
- An **Attribute Authority** that issues signed **SAML** assertions containing VO membership information
  - VOMS FQANs
  - VOMS generic attributes



- Part of VOMS Admin
  - starting with v. 2.0.18
  - in production since several months
    - no real use, though...

- Goal:
  - cross-Middleware VO management

Cross-Middleware VOMS



The VOMS SAML web service

```
Response attributeQuery(AttributeQuery query)
```

- **Users can request roles and order the attributes that will be included in the SAML assertion**
  - The ordering in the request is reflected in the issued assertion

- **The service can be configured to only return the FQANs that have been explicitly requested**
  - but the default is the “traditional” VOMS behaviour, i.e. always return all group FQANs

- **No assertions are issued for suspended users**

A VOMS SAML assertion

```
<saml:Assertion>
  <saml:Issuer>...</saml:Issuer>

  <saml:Subject>
    <saml:NameID Format="...X509SubjectName">
     CN=Andrea Ceccanti,L=CNAF,OU=Personal Certificate,O=INFN,C=IT
    </saml:NameID>
  </saml:Subject>

  <saml:Conditions NotBefore=”...” NotAfter=”...”/>

  <saml:AttributeStatement>
    <saml:Attribute Name="...voms-fqan" NameFormat="urn:...">
      <saml:AttributeValue xsi:type="xs:string">
        /dteam
      </saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string">
        /dteam/italy
      </saml:AttributeValue>
    </saml:Attribute>
 </saml:AttributeStatement>
...
</saml:Assertion>
```

the VOMS server that issues the assertion

Subject information, i.e., the DN

Validity information

The Bag of VOMS attributes

Service Configuration details

- VOMS SAML must be explicitly activated in the VOMS Admin configuration (since v.2.5.3):

```
voms.aa.activate_saml_endpoint = true
```

- VOMS SAML needs access to host certificate and private key to sign the assertions:

```
voms.aa.certificate = /etc/grid-security/hostcert.pem
voms.aa.key = /etc/grid-security/hostkey.pem
```

- You can configure the max lifetime for issued assertions:

```
voms.saml.max_assertion_lifetime = 720
```

Standardization

- **The protocol to obtain credentials has been standardized:**
  - http://www.ogf.org/documents/GFD.158.pdf
- **There is no attribute profile for VOMS SAML yet**
  - But we could use/extend the work already done in Argus profiles as a starting point
- **The current implementation encodes FQANs as**
  - Attribute name: http://authz-interop.org/xacml/subject/voms-fqan
  - Data type: http://www.w3.org/2001/XMLSchema#string
  - Multiplicity: 1..N