UNICORE

CROWN

OpenGridForum
OPEN FORUM | OPEN STANDARDS

the globus alliance

gLite
Lightweight Middleware for Grid Computing

omii europe
open middleware infrastructure institute

Interoperability in OMII – Europe

(using the new standard compliant SAML-based VOMS to handle attribute-based authz.)

Morris Riedel (FZJ), Valerio Venturi (INFN), Vincenzo Ciaschinni (INFN)

Middleware Security Group Meeting, Stockholm, 12th June 2007

Outline

- **OMII – Europe in Context**
- **Production VOMS**
- **New SAML-based VOMS**
- **Interoperability and SAML-based VOMS**
- **Interoperability Scenario: VOMS-based Jobs**
- **PDP – Problem and Solutions**
- **Cross-Grid use case example: WISDOM**
- **Conclusions**
- **CFP: Int.Grid Interoperability&Interoperation Workshop**
- **SAML-based VOMS request/response example**

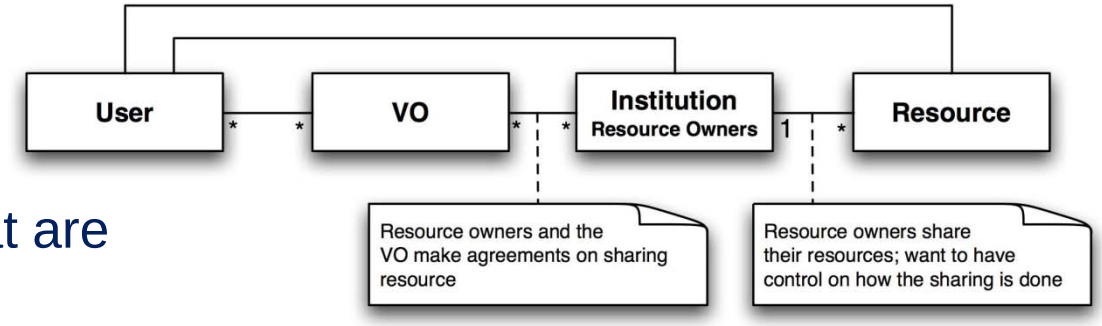
OMII – Europe: Interoperability Highway

OMII – Europe in Context

- **One goal of OMII – Europe towards interoperability**
  - Re-engineer existing sw components based on standards emerging within the Grid community
    - **E.g. Virtual Organization Membership Service (VOMS)**
- **JRA1 – Virtual Organization Membership (VOM)**
  - Provides new SAML-based VOMS server (prototype)
- **JRA1 – Job Submission and Management (JOBS)**
  - Provides OGSA-BES interfaces to CREAM & UNICORE & GT4
- **JRA3 – Infrastructure Integration (Interoperability)**
  - JRA3 – Task 1: Common Security
    - **VOMS as one part of the security profile**
  - JRA3 – Task 2: Infrastructure Integration
    - **Central VOMS server to enable Grid middleware interoperability in Authz.**

Production VOMS

- **Virtual Organization Membership**
  - VO level attributes that are used for authorization



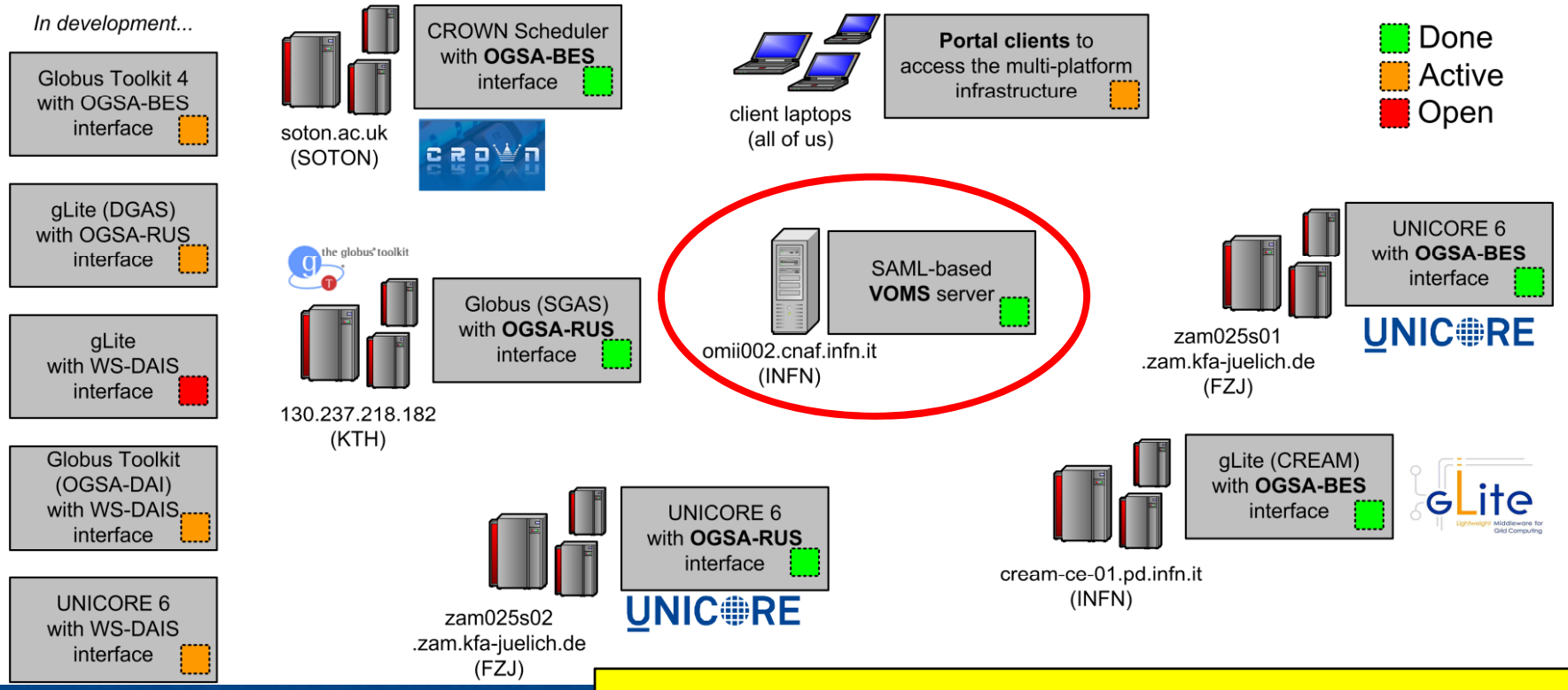
- **Virtual Organization Membership Service (VOMS)**
  - Attribute Authority releasing attributes holding their position in a VO
    - **Group/Project membership**
    - **Role possession**
- **Requires gLite components for build and running**
- **Format: RFC 3821 compliant Attribute Certficates (AC)**
  - ACs are inserted into an extension of proxy certificates
  - Adopted by gLite (EGEE), VDT (OSG), and GT4 (TeraGrid)
  - Limitation: End entity certificates based middleware (UNICORE)

New SAML-based VOMS

- **Developed in OMII – Europe JRA1 VOM activity**
  - Re-engineering VOMS to support standards, prototype available
  - OGF OGSA Authorization WG → Profile for attribute retrieval
  - OASIS Security Assertion Markup Language (SAML) V2.0
- **Web services-based VOMS server**
  - WS-Clients can use official SAML XSD schema to access VOMS
  - VOMS works without gLite within a standalone container (-admin!!!)
    - **(can be e.g. deployed within Tomcat, using AXIS 1.4, OpenSAML v2.0)**
- **Re-engineered component is not going to replace the current but to support more usage patterns**
  - E.g. homogenous cross-middleware VO management
  - New SAML-based VOMS as Attribute Authority (AA) for middleware
    - **In future maybe supported by gLite, UNICORE, GT4, and others**

Interoperability & SAML-based VOMS

- **New SAML-based VOMS is independent from gLite**
  - Gets a central role in JRA3 in terms of interoperability (authz)

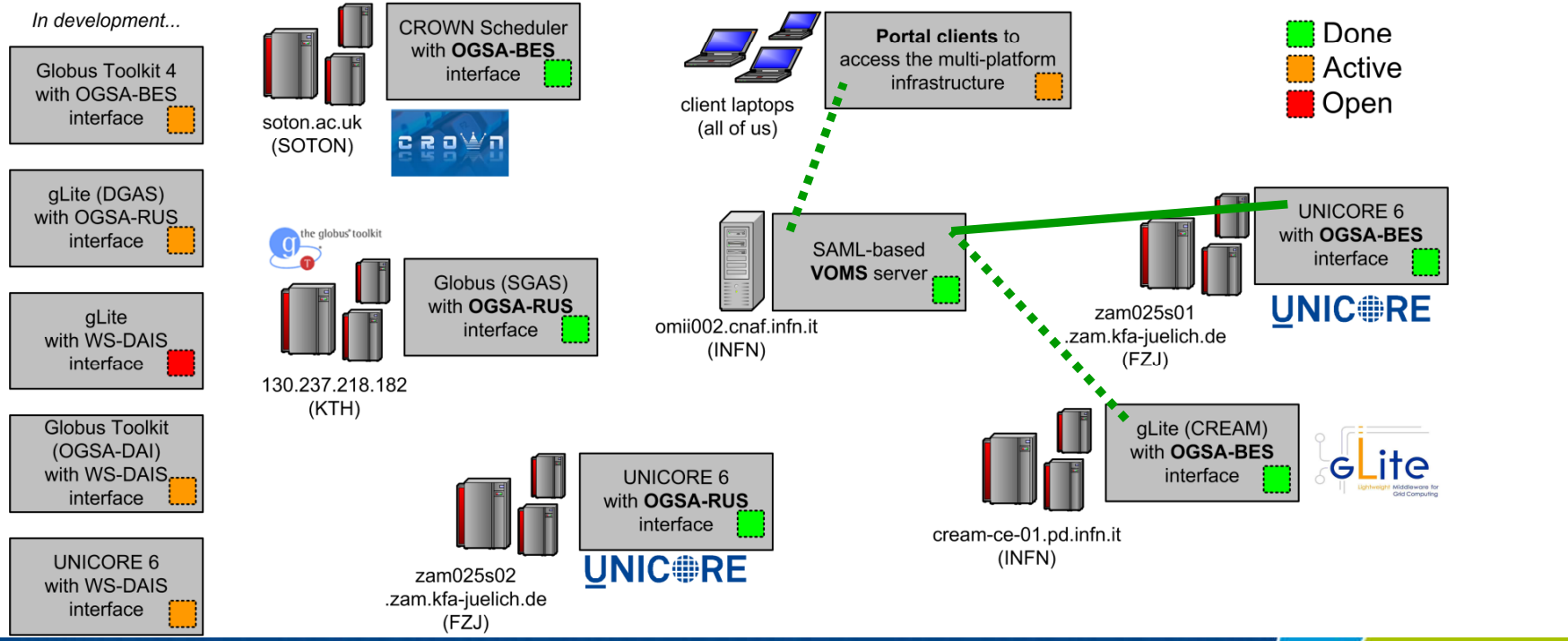


omii europe
open middleware infrastructure institute

EU project: RIO31844-OMII-EUROPE

Interoperability Scenario: VOMS-based Jobs

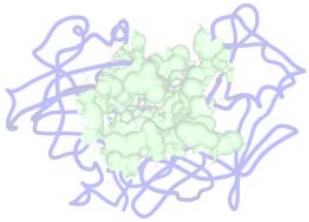
- **Using VOMS released SAML assertions**
  - UNICORE 6 service environment supports them (prototype)
  - CREAM (OGSA-BES gLite interface) supports them (development)



PDP Problem and Solutions

- **Policy Decision Point (PDP) Problem in OMII – Europe**
  - VOMS is ‘only’ a Policy Information Point (PIP)
  - There is no effort in OMII-Europe working on a PDP for a PEP
- **One solution are XACML-based PDPs**
  - OASIS Extensible Access Control Markup Language (XACML)
  - Fine-grained access control and policies
  - Can be used to make authz decisions based on VOMS SAML assertions (e.g. project membership, role possession)
- **E.g.: XACML used within UNICORE 6 (Sun XACML 1.2)**
  - WS-Security set of specifications are used to carry SAML attribute assertions in SOAP, no proxies needed (prototype available)
  - Using XACML policy in conjunction with UNICORE User Database (UUDB) to achieve attribute-based authz. via VOMS assertions

Cross-Grid use case example: WISDOM



- **WISDOM (Wide In Silicio Docking on Malaria)**
  - WISDOM aims at developing new drugs for Malaria
  - WISDOM uses EGEE for large scale in silicio docking
    - **A computational method for prediction of whether one molecule will bind to another using (using AutoDock and FlexX software)**
  - AutoDock and FlexX as software provided via gLite in EGEE
  - Output is a list of chemical compounds (potential drugs)
- **Refine best compound list via molecular dynamics (MD)**
  - Fast MD comp. use highly scalable AMBER via UNICORE in DEISA
    - **AMBER (Assisted Model Building with Energy Refinement)**
- **Future: Accelerate drug discovery with gLite&UNICORE**
  - SAML-based VOMS becomes useful, but e-Infrastructure policies…

Conclusion

- **Cross-Middleware authz. via new SAML-based VOMS**
  - Integrated with UNICORE 6 (beta version, final in Mid 2007)
  - Soon integrated with CREAM-BES (pre-production)
- **Benefits: WISDOM project use case**
  - More easier to use both UNICORE & gLite together in a scenario
- **Showstoppers: production e-Infrastructure policies**
  - Adoption of newly developed components slow
    - **DEISA uses UNICORE 5, code freeze in EGEE (no new VOMS in gLite now)**
  - Even if technical level interoperability is possible, politics remain..
- **Outlook: Using SAML for trust delegation (?)**
  - Works also with UNICORE full end entity certificates
- **MWSG: There is a public deliverable with more infos…**

Call for Paper: IGIIW @ e-Science 2007

International Grid Interoperability & Interoperation Workshop (IGIIW)

in conjunction with

e-Science 2007, Garuda, India

Call for paper published :
http://www.omii-europe.org/OMII-Europe/igiiw2007

omii europe
open middleware infrastructure institute

EU project: RIO31844-OMII-EUROPE

References

- **Int. Interoperability & Interoperation Workshop (IGIIW)**
  - http://www.omii-europe/OMII-Europe/IGIIW2007
- **JRA3 Internal Wiki with Monthly Reports, Deliverables&Milestones**
  - http://tjasse.pdc.kth.se/omii-europe/ (username, passwort)
- **JRA1 VOM Deliverable (for new SAML-based VOMS + UNICORE)**
  - http://www.omii-europe (Intranet)

Questions…

Morris Riedel
m.riedel@fz-juelich.de

Valerio Venturi
valerio.venturi@cnaf.infn.it

JRA 3 Team
jra3@omii-europe.com

SAML-based VOMS request example

```
<AttributeQuery ID="_qwertyuiopasdfghjklzxcvbnm" Version="2.0"
    xmlns="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:urn="urn:oasis:names:tc:SAML:2.0:assertion">

  <urn:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-
    format:x509SubjectName">CN=Morris Riedel,OU=ZAM,OU=Forschungszentrum
    Juelich GmbH,O=GridGermany,C=DE
  </urn:Issuer>

  <urn:Subject>
    <urn:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
      format:x509SubjectName">CN=Morris Riedel,OU=ZAM,OU=Forschungszentrum
      Juelich GmbH,O=GridGermany,C=DE
    </urn:NameID>
  </urn:Subject>
</AttributeQuery>
```

SAML-based VOMS response example (1)

```
<Response ID="_1234567890qwertyuiopasdfghjklzxcvbnm"
    InResponseTo="_qwertyuiopasdfghjklzxcvbnm" IssueInstant="2007-04-
    22T14:34:09.996Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:samlp…..“>
  <saml:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-
    format:x509SubjectName"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">CN=omii002.cnaf.infn.it,L=
    CNAF,OU=Host,O=INFN,C=IT
  </saml:Issuer>
  <Status>
    <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </Status>
...
```

SAML-based VOMS response example (2)

```
...
<saml:Assertion ID="_1234567890abcdefghilmnopqrstuvz" IssueInstant="2007-04-
    22T14:34:10.059Z" Version="2.0"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
 <saml:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-
    format:x509SubjectName">CN=omii002.cnaf.infn.it,L=CNAF,OU=Host,O=INFN,C=IT
 </saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
    c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#_1234567890abcdefghilmnopqrstuvz">
...
```

SAML-based VOMS response example (3)

```
...
<saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
      format:x509SubjectName">CN=Morris Riedel,OU=ZAM,OU=Forschungszentrum Juelich
      GmbH,O=GridGermany,C=DE</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
  <saml:SubjectConfirmationData>
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:X509Data>
  <ds:X509Certificate>xxxxxxx</ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>
</saml:SubjectConfirmationData>
</saml:SubjectConfirmation>    </saml:Subject>    <saml:Conditions NotBefore="2007-04-
      22T14:34:10.060Z" NotOnOrAfter="2007-04-23T02:34:10.060Z"/>    <saml:AttributeStatement>
      <saml:Attribute Name="group-membership-id"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:string"
      xmlns:xs="http://www.w3.org/2001/XMLSchema">/omiieurope</saml:AttributeValue>
      </saml:Attribute>    </saml:AttributeStatement>  </saml:Assertion></Response>
```

SAML-based VOMS response example (2)

```
...
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments">
         <ec:InclusiveNamespaces PrefixList="ds saml xs"
     xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue/>
    </ds:Reference>
    </ds:SignedInfo>
 <ds:KeyInfo>
 <ds:X509Data>
   <ds:X509Certificate>xxxxx</ds:X509Certificate>
     </ds:X509Data>
     </ds:KeyInfo>
</ds:Signature>
...
...
```