Attributes and VOs: Extending the UNICORE autorisation capabilities

Arash Faroughi
Roozbeh Faroughi
Wolfgang Ziegler
Fraunhofer Institute SCAI

Philipp Wieder
Research Center Jülich

UNICORE Summit 2007
August 28, 2007, Rennes, France

Acknowledgements

- Some of the work reported in this presentation is funded by the German Federal Ministry of Education and Research through the IVOM project under grant #01AK800A. This presentation also includes work carried out jointly within the CoreGRID Network of Excellence funded by the European Commission's IST programme under grant #004265.

Outline

- Background
- Shibboleth Integration
- VOMS Integration
- Outlook

Background

- D-Grid environment with three supported middleware systems: GT4, gLite, UNICORE
- Focus: Interoperability and Integration
- Development is part of the D-Grid IVOM project
- IVOM: Interoperability and Integration of VO Management in D-Grid
- UNICORE 5 as initial code base

Shibboleth basics

- Shibboleth is a federated identity management system (developed by Internet2)
- Supports authorisation decisions based on the attributes of the users
- It uses the Security Assertion Markup Language (SAML) to implement SSO across or within organizational boundaries.
- Shibboleth supports an Attribute Based Access Control

- The three major components:
  - Identity Provider
  - Service Provider
  - Where are you from Service

Goals of the UNICORE-Shibboleth Integration

- The goals of the UNICORE integration with Shibboleth are:
  - Extend UNICORE by providing attribute-based authorization based on Shibboleth
  - To keep the modification of the UNICORE Client as minimal as possible
  - Keep the UNICORE authentication mechanisms as much as possible.
  - Find a bridge between X.509 and SAML assertions (Shibboleth Identity to Grid Identity)
- The main tasks are:
  - UNICORE Authentication with a SLC
  - Attribute-Based UUDB mapping

UNICORE Authentication (SLC)

- The exchange in Shibboleth is based on assertions between an Identity Provider and a Service Provider.
- The AAI in UNICORE relies on the usage of X.509 certificates.

- To translate a Shibboleth Identity to a Grid Identity:
  - The GridShib CA issues a short lived X.509 Credential after a successful user authentication at a Shibboleth Identity Provider.
  - Assertion(s) bound to a SLC Certificate-Extension.
  - SLC have a maximum Lifetime of 1 million seconds.

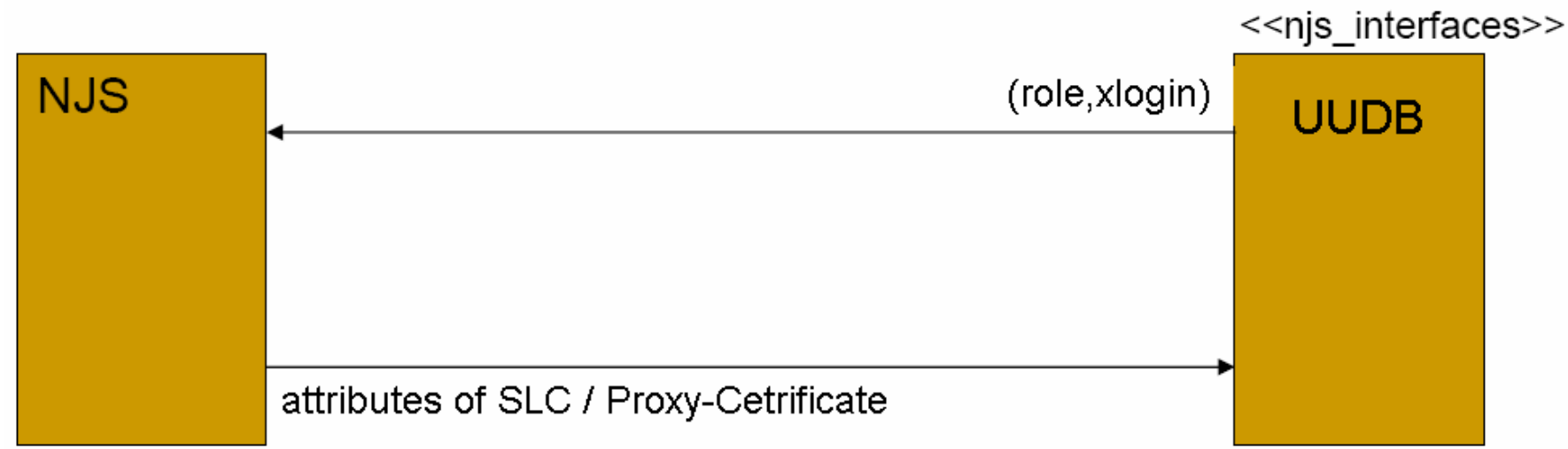
- Using SLC the authentication mechanisms in UNICORE are largely unchanged.

SLC with SAML assertion

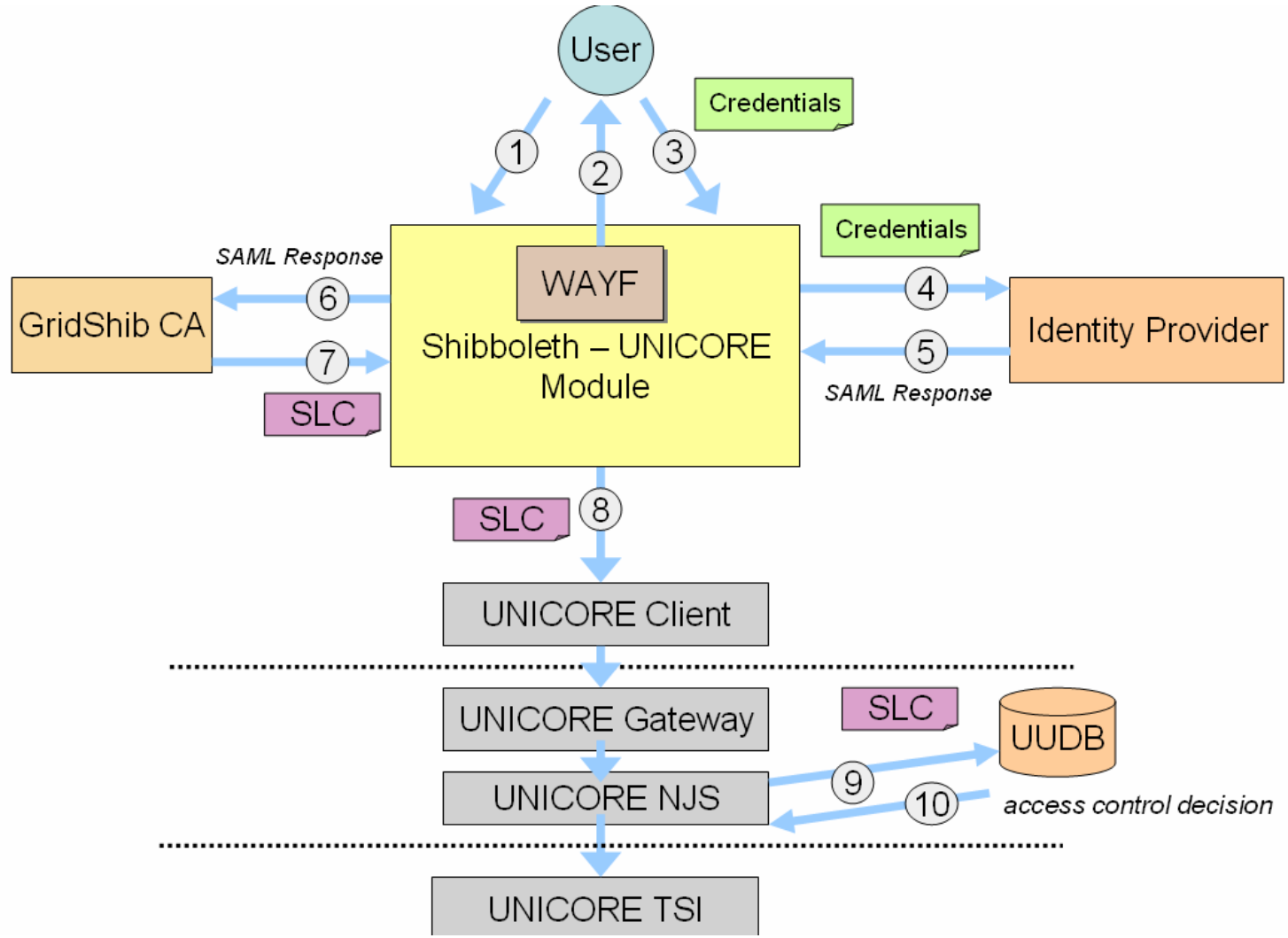
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 154 (0x9a)
Signature Algorithm:
Issuer:
Validity
Subject:
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
X509v3 extensions:
1.3.6.1.4.1.3536.1.1.1.10:
<Assertion>…….</Assertion>
Signature Algorithm: ….

Attribute based UUDB

- UNICORE maps the identity of the end-user to a local account using the information stored in the UUDB.
- To support ABAC-Authorisation, the UUDB authorisation mechanism must be extended.
- UUDB implementation is needed, which does the mapping to the permissions based on the attributes.



UNICORE – Shibboleth- Architecture



Fraunhofer SCAI Institut Algorithmen und Wissenschaftliches Rechnen

Forschungszentrum Jülich in der Helmholtz-Gemeinschaft

D-GRID

UNICORE Integration with VOMS

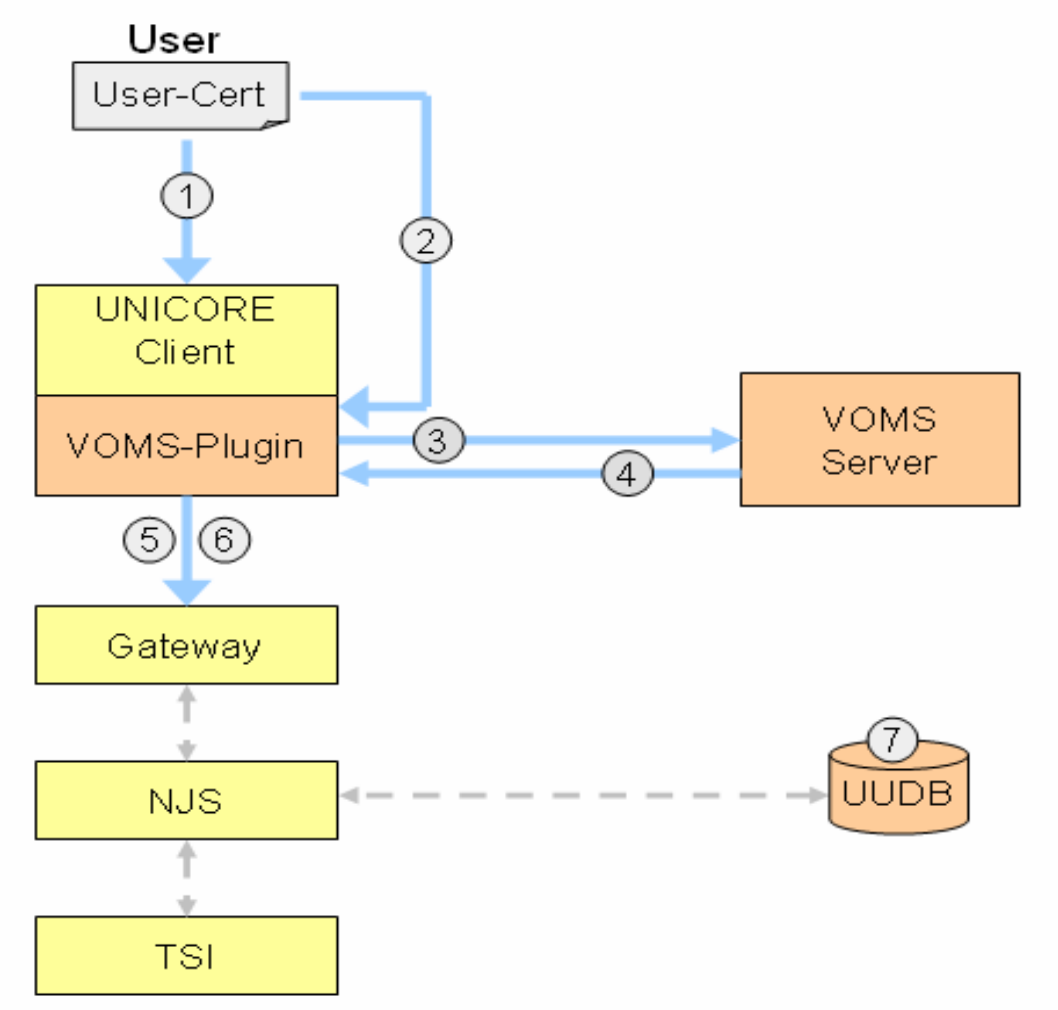
Virtual Organization Membership Service

- VOMS has been developed as part of the joint efforts of the European Data-Grid and DataTAG projects
- Classifies users that are participating in a VO based on a set of attributes.
  - VOMS-FQAN (Full Qualified Attribute Names)
- Attributes will be included into Globus-compatible proxy-certificates for supporting Single Sign-On (SSO) in Grid-environments

Integration UNICORE-VOMS (1)

- Two new Modules are needed:
  - **VOMS-Plugin:**
    - generates a proxy certificate (PC) with VOMS-specific extensions for the end-user (voms-proxy-init)
    - attaches the PC to the Abstract Job Object (AJO) encapsulated as a site-specific security object (SSO-Object)
  - **UUDB-VO:**
    - maps VOMS-FQANs (Full Qualified Attribute Names) to a local account

UNICORE – VOMS Architecture



Fraunhofer SCAI Institut Algorithmen und Wissenschaftliches Rechnen

Forschungszentrum Jülich in der Helmholtz-Gemeinschaft

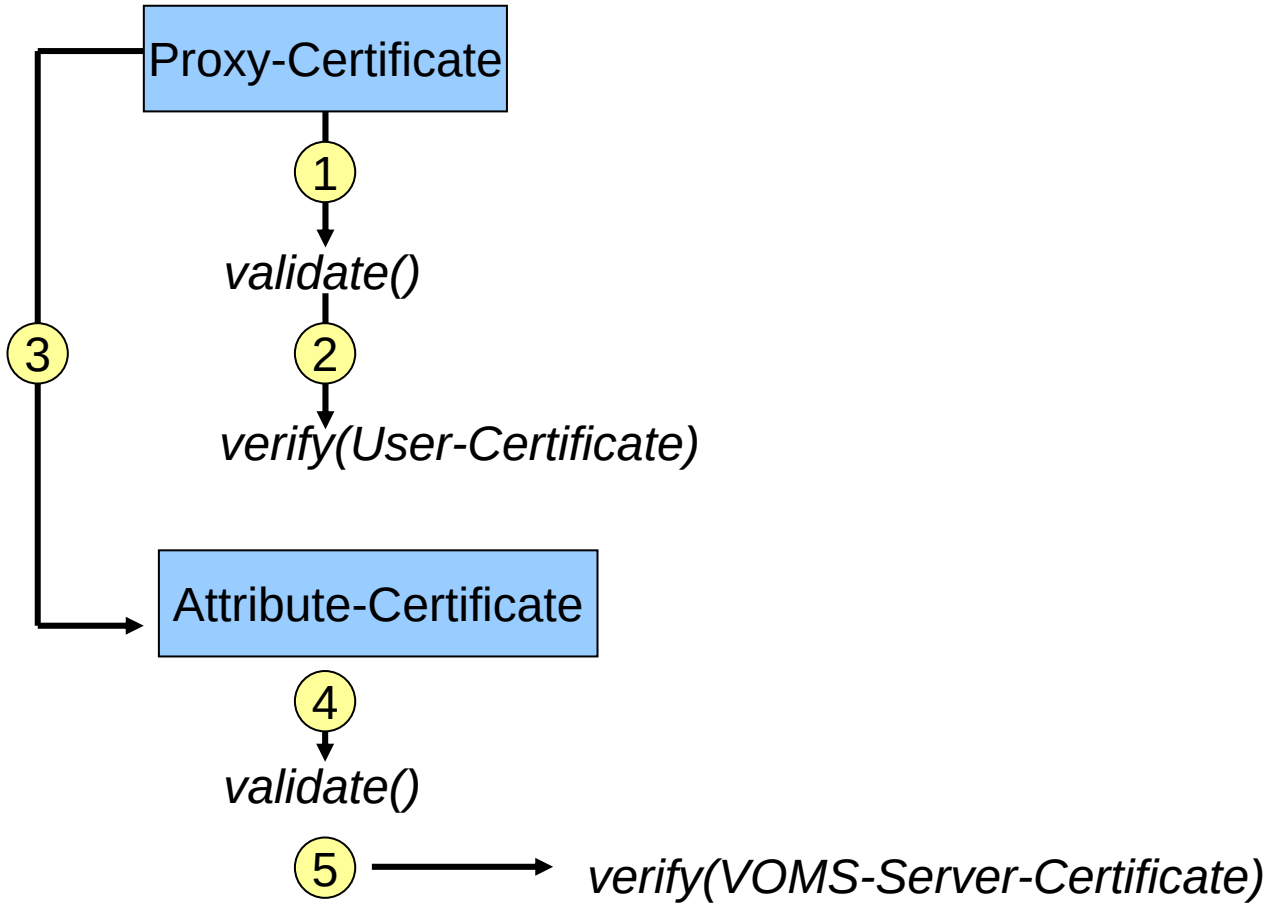
D-GRID

Integration UNICORE-VOMS (2)

- Required certificates:
  - **Authentication:**
    - User-Certificate (UC)
    - CA-Certificate of the UC
  - **Authorization:**
    - User-Certificate
    - Proxy-Certificate
    - Attribute-Certificate
    - VOMS-Server-Certificate

Integration UNICORE-VOMS (3)

- Security-model (Authorization):



Integration UNICORE-VOMS (4)

VOMS-Proxy-Certificate

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 14 (0xe)
        Signature Algorithm: md5WithRSAEncryption
        Issuer:
        Validity
        Subject:
Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.8005.100.100.5:
                0...0...0...0.....0X.V0Q.O0M1.0...U....DE1.0
..U....NRW1.0...U.
0...U....user....h0f.d0b1.0...U....DE1.0
..U....NRW1.0...U.
.....L:.0"..20070705092825Z..20070705212825Z0..0...
+.....Edd.1..0.....vo://kappes:150010h.
/vo/Role=Rechnend/Capability=NULL../vo/Role=NULL/Capability=NULL.%/vo/IVOM/Role=NULL/Capability=NULL0,0...U.8....0.....o....p.YJ..4O.&..[....._.&N..5..*.....h?5.....3Y..bnRtz..T.2.t
.s.....N).GX..|.....}..5..R.M{m.....f....0..C.._...q....._.....0..s.3.>....:9l.....1.#.....B.z....y..SR.[.....a?..].y..X.....-
|.....r..2X.+....*.....9....0....ihY....|
....

Integration UNICORE-VOMS (5)

VOMS-Attribute-Certificate

OID of the Attribute-Certificate: „**1.3.6.1.4.1.8005.100.100.4“**

```
AttributeCertificate ::= SEQUENCE {
      acinfo                          AttributeCertificateInfo,
      signature                       Algorithm AlgorithmIdentifier,
      signatureValue      BIT STRING}


AttributeCertificateInfo ::= SEQUENCE {
      verson                                  AttCertVersion,
      holder                                  Holder,
      issuer                                  AttCertIssuer,
      signature                               AlgorithmIdentifier,
      serialNumber                            CertificateSerialNumber,
      attrCertValidityPeriod                  AttCertValidityPeriod,
      attributes                              SEQUENCE OF Attribute,
      issuerUniqueID UniqueIdentifier         OPTIONAL,
      extensions Extensions                   OPTIONAL}
```

State & Outlook

- First implementations ready by end of August 2007
- IVOM to provide a D-Grid GridShib implementation later this year
- DFN is creating the (first) German Shib federation for education and science (legal & administrative issues)
- DFN-AAI project to provide the necessary infrastructure
- Looking for UNICORE 6 issues
- Sync with the VOMS/SAML OMII-Europe developments