

## UNICORE 6 security

Bernd Schuller and the UNICORE team  
Jülich Supercomputing Centre, Forschungszentrum Jülich GmbH  
March 17, 2010  
OGF28 Munich

## Outline

- UNICORE 6 security overview
- X.509, SSL
- Role of the Gateway
- SAML trust delegation assertions
- Authorisation process

## Security overview

Security based on open standards, XML-based where possible

- X.509 certificates for clients and servers
- Client-authenticated SSL for all client-server and inter-component interaction
- Signed SAML assertions (Security assertion markup language)
  - XML-DSig, Web-services security, SAML v2.0
- Open and flexible security system
  - Authorisation attribute sources: VO server, LDAP, ...
  - Optional, limited, proxy support
- Extensible clients

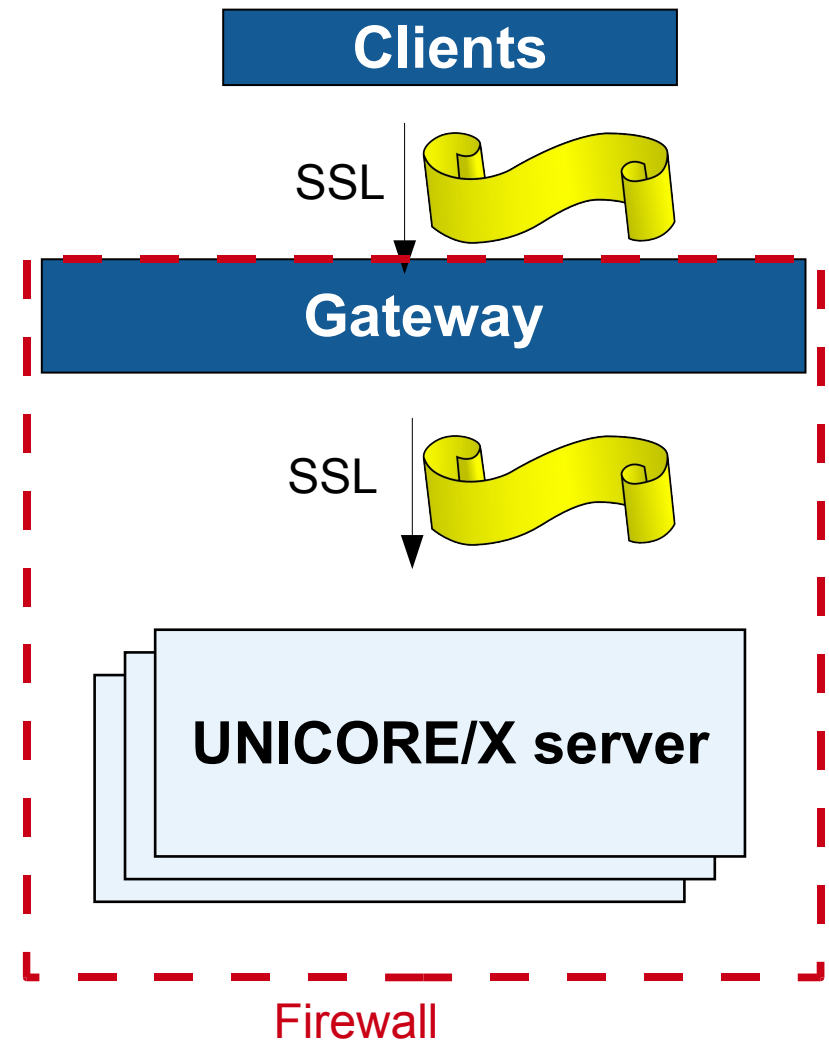
## Basic security: X.509 and SSL

- X.509
  - End-entity certificates issued by a trusted Certification Authority (CA)
  - Used for both clients and servers
- SSL
  - Client needs to trust server CA
  - Server needs to trust client CA (client authenticated SSL)
  - Off-the-shelf components (Jetty server, Apache HTTPClient)

## The Gateway - I


Sites are protected by firewalls.

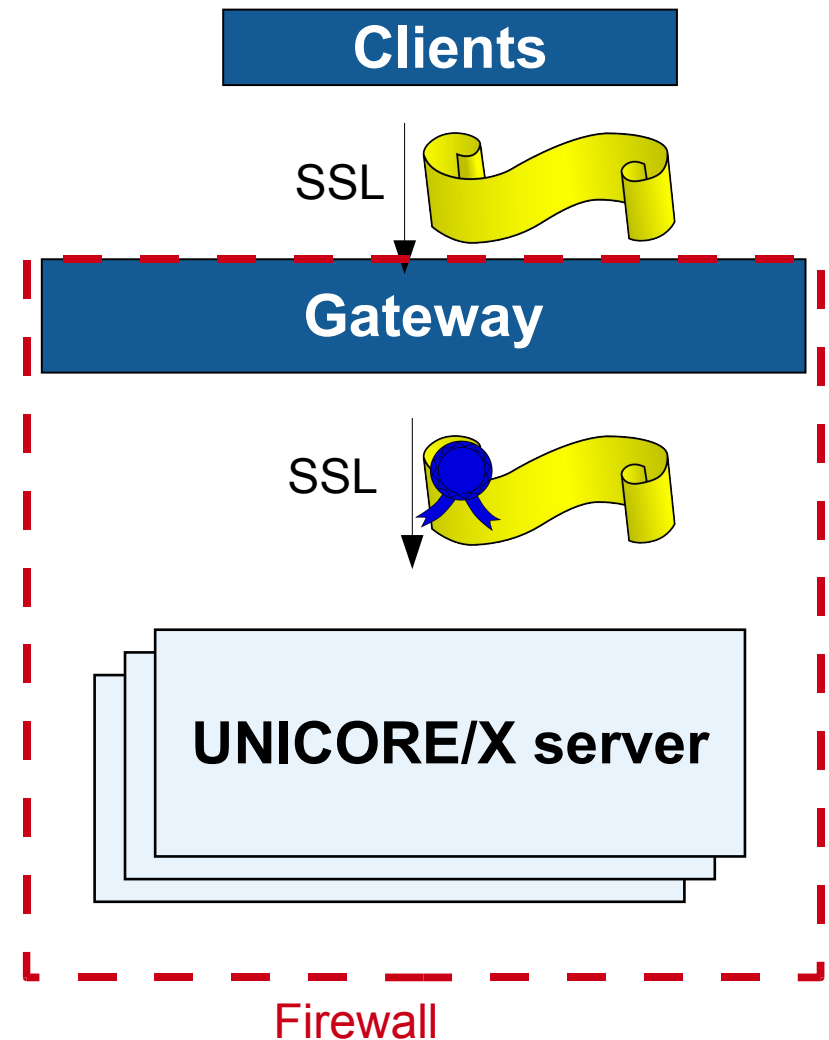
- Gateway provides single firewall entry point
- Client makes client-authenticated SSL connection to the gateway
- Gateway should forward request to the target site
- **How to preserve client certificate information?**
- Proxy based solution not acceptable



## The Gateway - II

Solution using SAML assertion

- Client makes client-authenticated SSL connection to the gateway
- Gateway issues a SAML assertion (optionally signed by the gateway) containing client certificate info  
→ **Consignor assertion** 
- Placed in SOAP header
- Gateway forwards request to target site, target site gets client information from the assertion



# Consignor assertion example

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soap:Header>
    <ns0:Assertion xmlns:ns0="urn:oasis:names:tc:SAML:2.0:assertion" ID="SAMLY2lib_assert_fb58d1eb1"
      IssueInstant="2010-03-16T08:49:14.829+01:00" Version="2.0">
      <ns0:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        C=DE,O=unicore.eu,OU=Testing,CN=UNICORE demo gateway
      </ns0:Issuer>
      <ns0:Subject>
        <ns0:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
          C=DE,O=unicore.eu,OU=Testing,CN=UNICORE demo user
        </ns0:NameID>
        <ns0:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
          <urn:SubjectConfirmationData xmlns:urn="urn:oasis:names:tc:SAML:2.0:assertion"
            xsi:type="urn:KeyInfoConfirmationDataType">
            <ns1:KeyInfo xmlns:ns1="http://www.w3.org/2000/09/xmldsig#">
              <ns1:X509Data>
                <ns1:X509Certificate>MIICS .... </ns1:X509Certificate>
                <ns1:X509Certificate>MIICeTC... </ns1:X509Certificate>
              </ns1:X509Data>
            </ns1:KeyInfo>
          </urn:SubjectConfirmationData>
        </ns0:SubjectConfirmation>
      </ns0:Subject>
      <ns0:AttributeStatement>
        <ns0:Attribute Name="CONSIGNOR" NameFormat="urn:unicore:subject-role"/>
      </ns0:AttributeStatement>
    </ns0:Assertion>
    <wsa:To xmlns:wsa="http://www.w3.org/2005/08/addressing"> ... </wsa:To>
    <wsa:Action xmlns:wsa="http://www.w3.org/2005/08/addressing"> ... </wsa:Action>
  </soap:Header>
  <soap:Body>
    <rp:GetResourcePropertyDocument xmlns:rp="http://docs.oasis-open.org/wsrf/rp-2"/>
  </soap:Body>
</soap:Envelope>

```

Gateway info

User info

Assertion type

Payload

## The Gateway - III

### Advantages

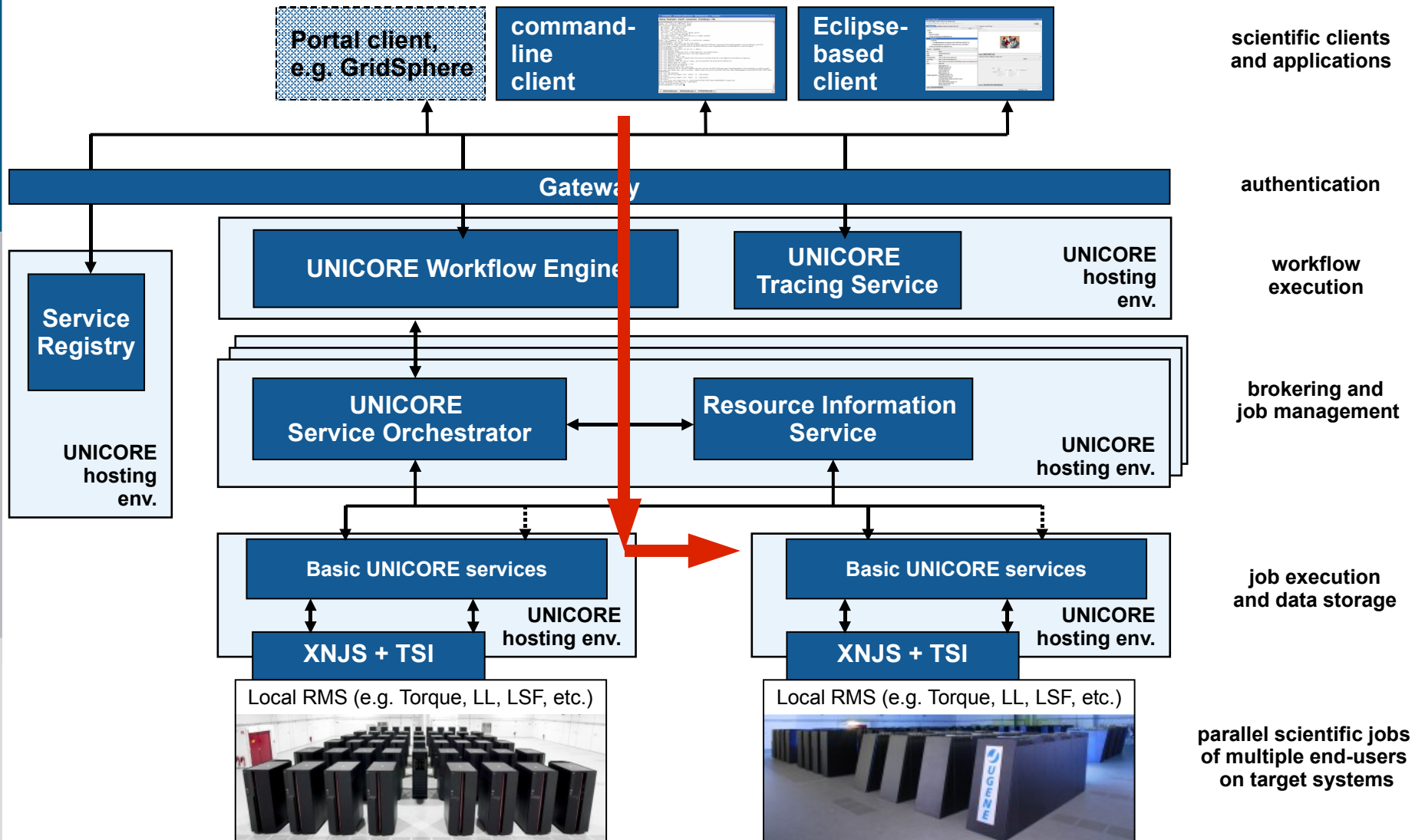
- Only single open firewall port needed for a Grid site
- Easier to perform security audits
- Authentication and management of trusted CAs only needed in one place

### Disadvantages

- Lots of traffic goes via a single server

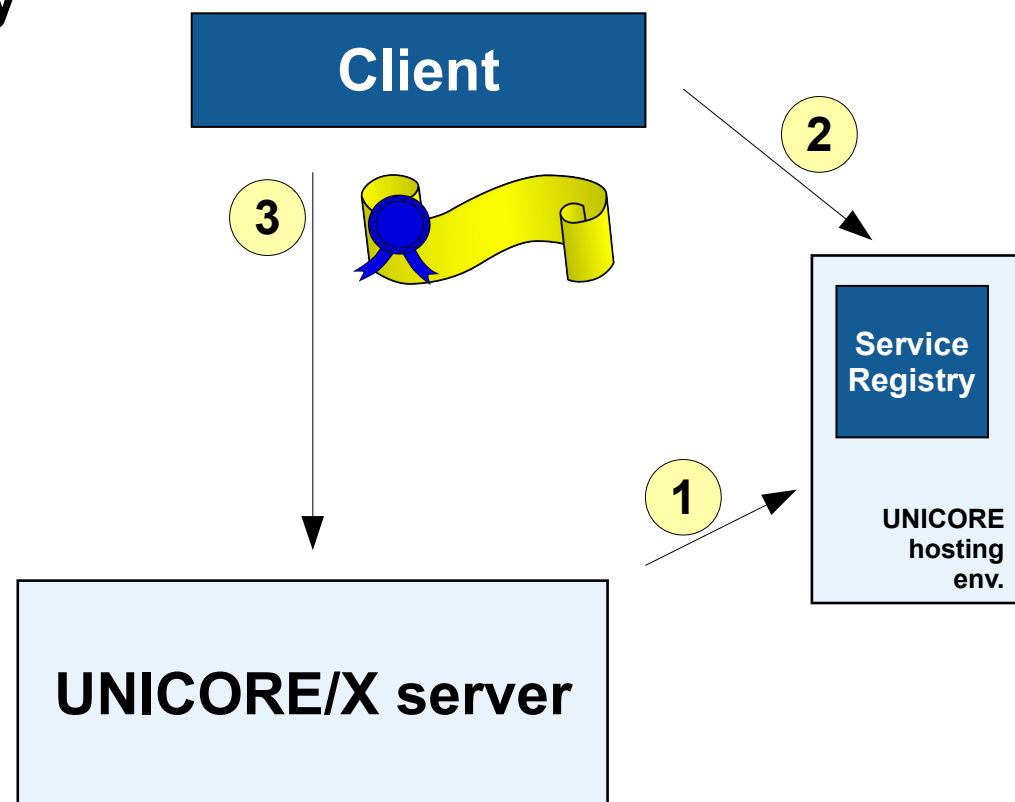
## Trust delegation

# Example: workflow system



## SAML assertions for trust delegation

- Server publishes identity information (DN) to the **registry**
- Client gets identity info from the registry
- Client issues **Trust delegation assertion**
- Client sends request, and adds the TD to the SOAP header






# Registry entry example

```

<sg:Entry xmlns:sg="http://docs.oasis-open.org/wsrf/sg-2">
  <sg:ServiceGroupEntryEPR>...</sg:ServiceGroupEntryEPR>
  <sg:MemberServiceEPR xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <add:Address xmlns:add="http://www.w3.org/2005/08/addressing">
      https://localhost:8080/DEMO-SITE/services/StorageFactory?res=...
    </add:Address>
    <add:Metadata xmlns:add="http://www.w3.org/2005/08/addressing">
      <met:InterfaceName xmlns:met="http://www.w3.org/2005/08/addressing/metadata"
        xmlns:x="http://unigrids.org/2006/04/services/smf">
        x:StorageFactory
      </met:InterfaceName>
      <unic:ServerIdentity xmlns:unic="http://www.unicore.eu/unicore6">
        C=DE, O=unicore.eu, OU=Testing, CN=UNICORE demo unicorex
      </unic:ServerIdentity>
    </add:Metadata>
  </sg:MemberServiceEPR>
  <sg:Content xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <sg:RPDoc>
      <wsrf:WSResourceInterfaces xmlns:bpri1="http://docs.oasis-open.org/wsrf/rlw-2"
        xmlns:bpri2="http://docs.oasis-open.org/wsrf/rpw-2"
        xmlns:wsrf="http://schemas.ggf.org/ogsa/2006/05/wsrf-bp">
        bpri1:ScheduledResourceTermination
        bpri2:GetResourceProperty bpri2:GetResourcePropertyDocument
        bpri1:ImmediateResourceTermination
        bpri2:QueryResourceProperties</wsrf:WSResourceInterfaces>
    </sg:RPDoc>
  </sg:Content>
</sg:Entry>

```

-  Service address
-  Service type
-  Identity

# Trust delegation assertion example

```

<urn:Assertion ID="SAML2lib_assert_6413" IssueInstant="2010-03-16T12:58:56.911+01:00" Version="2.0"
xmlns:urn="urn:oasis:names:tc:SAML:2.0:assertion">
  <urn:Issuer >C=DE,O=unicore.eu,OU=Testing,CN=UNICORE demo user</urn:Issuer>
  <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <dsig:SignedInfo><dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" /><dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" /><dsig:Reference
URI="#SAML2lib_assert_64133d2c292015b6ec4a6b3c43dab1a5ae241f1d0fec4175"><dsig:Transforms><dsi
g:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /><dsig:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /></dsig:Transforms><dsig:DigestMethod Algorithm="
http://www.w3.org/2000/09/xmldsig#sha1
"/><dsig:DigestValue>IUZTxdLLOX1Bappo0jE3MqLSY8=</dsig:DigestValue></dsig:Reference></dsig:Signed
Info>
  <dsig:SignatureValue>S2jNlb...</dsig:SignatureValue>
  <dsig:KeyInfo><dsig:X509Data>
  <dsig:X509Certificate>MIICSDCCAb...</dsig:X509Certificate>
  <dsig:X509Certificate>MIICeTCCAeK...</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo></dsig:Signatu
re>
  <urn:Subject><urn:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DE,O=unicore.eu,OU=Testing,CN=UNICORE demo unicorex</urn:NameID><
/urn:Subject>

  <urn:Conditions NotBefore="2010-03-16T12:58:56.910+01:00"
    NotOnOrAfter="2010-03-17T12:58:56.910+01:00">
    <urn:ProxyRestriction Count="10" />
  </urn:Conditions>

  <urn:AttributeStatement><urn:Attribute Name="TrustDelegationOfUser" NameFormat="urn:unicore:trust-
delegation:dn">
  <urn:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">C=DE,O=unicore.eu,OU=Testing,CN=UNICORE
demo user</urn:AttributeValue></urn:Attribute>
</urn:AttributeStatement>

</urn:Assertion>

```

Issuer +  
signature

Issuer key

Subject

Conditions

Assertion  
type

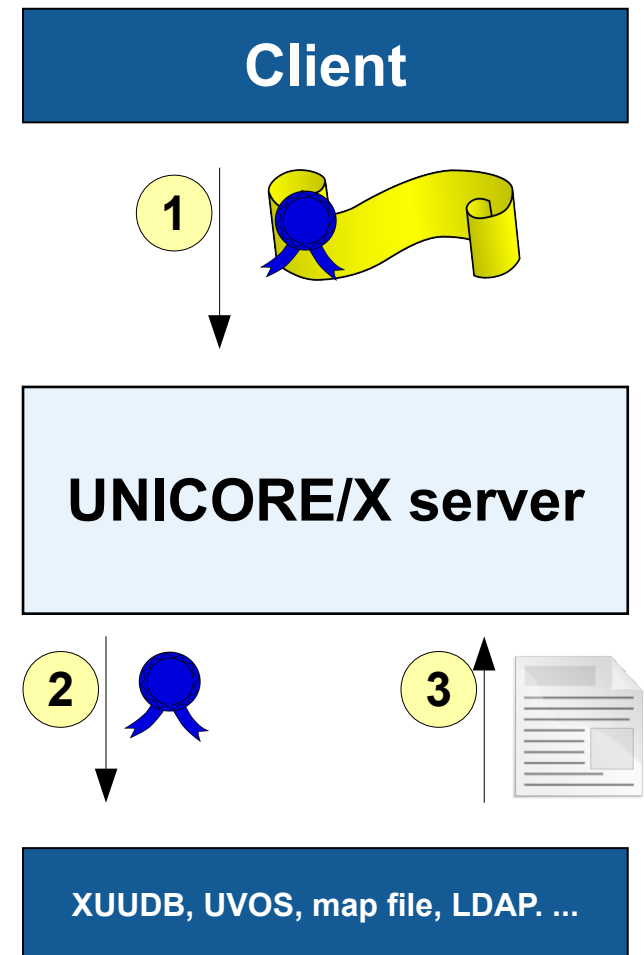
## Summary: SAML based trust delegation

- Delegations contain only public information
  - Identity of the target server, taken from the EPR entry in the registry
  - Issuer (user) certificate
- Trust chain is extensible
  - Fully auditable
  - Extension count can be restricted
- Currently: delegation to a DN
  - Subject to attacks using a weak (but trusted CA)
  - Better: delegate to a full certificate (→ Genesis II)

## Authorisation process

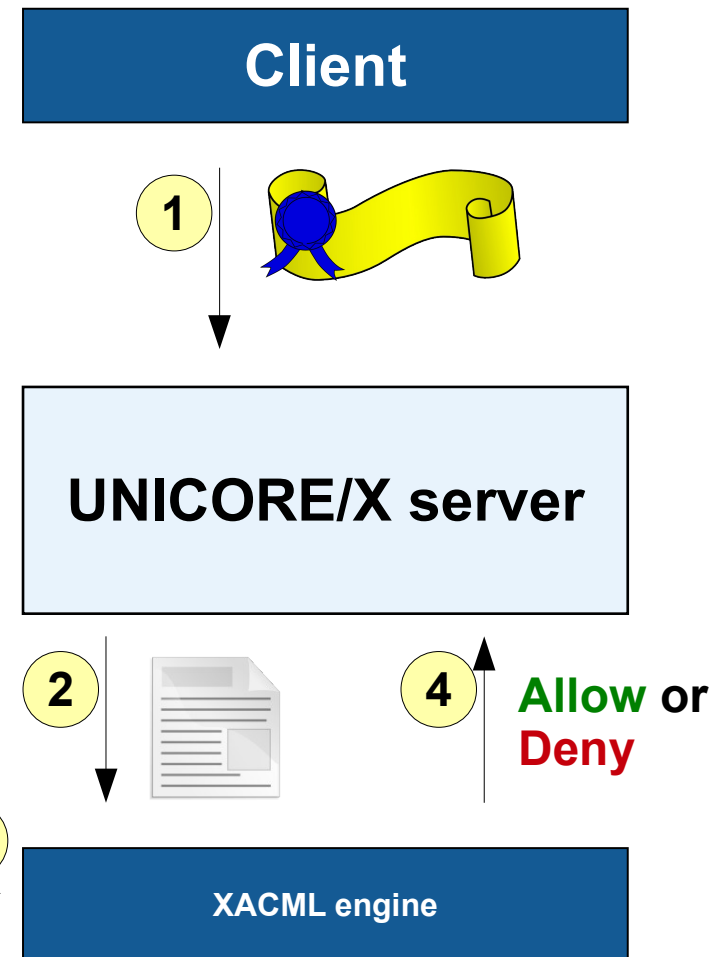
## Authorisation attributes

- Authorisation process occurs on the web-service level
- User identity (certificate or DN) is used by the UNICORE/X server to retrieve attributes
- Current sources:
  - XUADB (default)
  - UVOS (or SAML VOMS)
  - Local map file
- Typical attributes
  - Local Unix login (xlogin)
  - Role (user, admin, ...)



## Authorisation: XACML

- Attributes are used for an XACML callout  
(Default XACML 1.0 engine is built into UNICORE/X)
- XACML policies are checked
- Engine returns evaluation result
- UNICORE/X allows or denies the intended action (web service method invocation)



**Thank you!**