SAML – Create and Exchange Security Information in Grids

Morris Riedel, Forschungszentrum Juelich (FZJ), Juelich Supercomputing Centre (JSC), Germany

OMII – Europe, Leader Infrastructure Integration Task

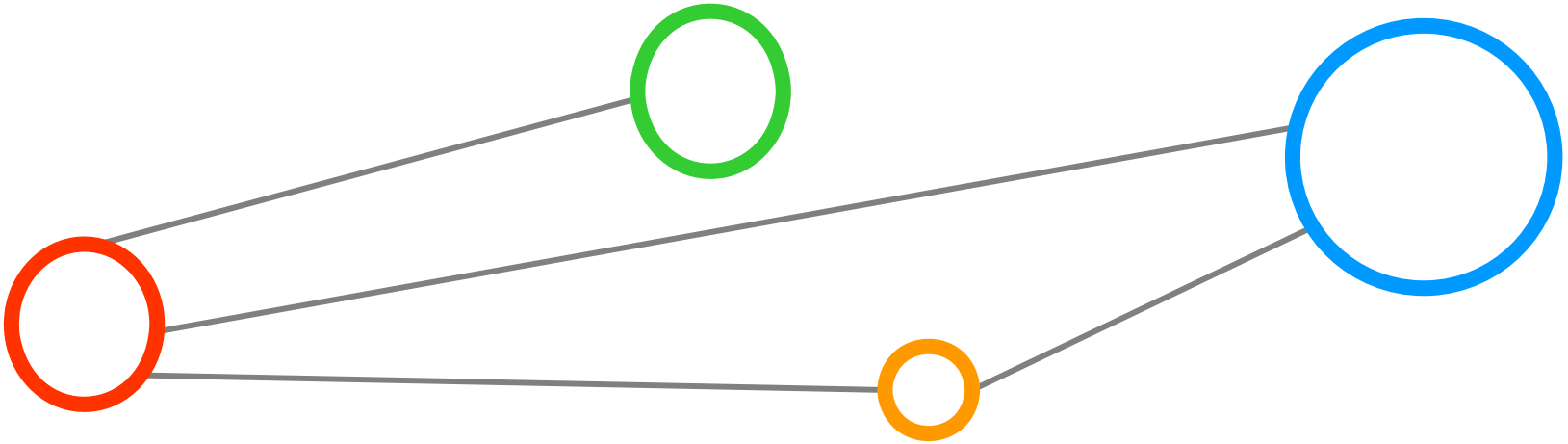
3. D-Grid Security Workshop, Göttingen, 1. – 2. April 2008

Inhalt

- **Security Assertion Markup Language (SAML)**
  - Kurze Übersicht des SAML Standard von OASIS
- **Anwendung von SAML im Kontext Grid: Autorisierung**
  - Fein-granulierte Autorisierung im Grid
  - Zur Erinnerung: „Classic VOMS“
  - SAML – basierter VOMS
  - Aufbau und Transport von SAML Assertions
- **SAML in einem Interoperabilitäts – Szenario**
- **Andere Anwendungen mit SAML im Grid**
  - Chemomentum, IVOM & Shibboleth, SAML Delegation, …
- **Schlussbemerkungen & Referenzen**

Gestern C. Grimm während Tutorial: “Zukünftige VOMSe sprechen SAML…”

Security Assertion Markup Language (SAML)



EU project: RIO31844-OMII-EUROPE

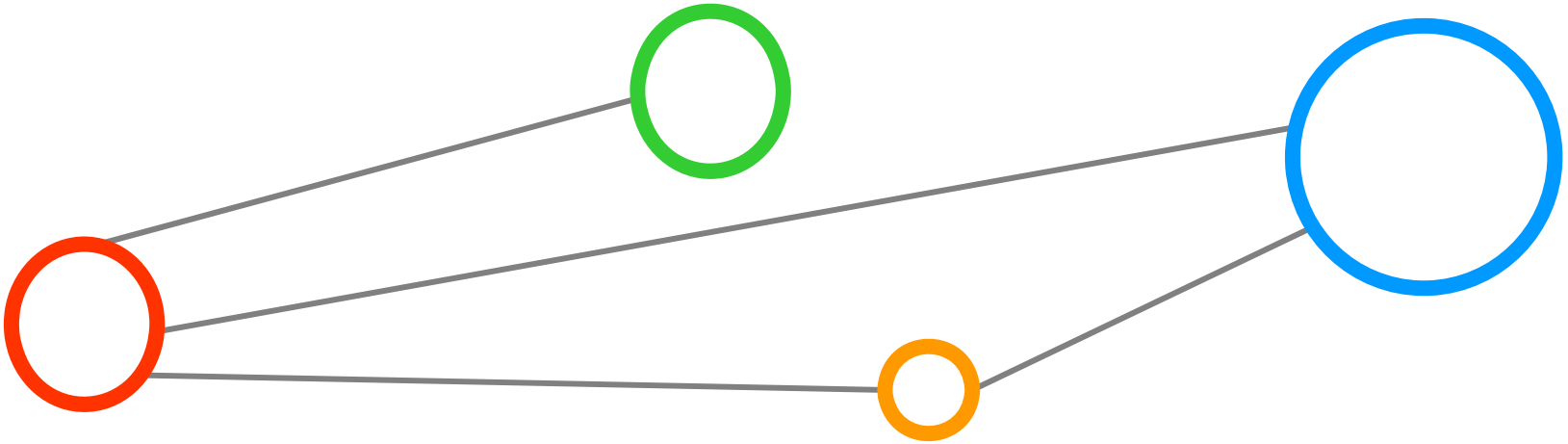
Kurze Übersicht SAML Standard von OASIS

- **OASIS = Organization for the Advancement of Structured Information Standards**
- **SAML V2.0**
  - Standardisiert seit 2005 von OASIS SAML TC
  - SAML definiert Syntax und Semantiken zur Verarbeitung von assertions über ein Subject ausgestellt von einer Systementität
  - SAML Assertions und Protokolle zum Austausch in XML kodiert
  - Viele Spezifikationen: core, bindings, profiles, metadata, Authentication Context, …
  - Viele XML Schemas: ~ 33 Stück (!)
  - Industriebeteiligung: Internet2, Nokia, Sun Microsystems, RSA Security, BEA Systems, Boeing, IBM, Atos Origin, AOL, HP, …

SAML TC [17]

J. Hughes et al. [17]
"SAML Technical Overview"

Anwendung von SAML im Kontext Grid: Autorisierung



EU project: RIO31844-OMII-EUROPE

Fein-granulierte Autorisierung im Grid

- **Das "Grid Problem"**
  - Dynamische Ansammlung von Personen, Organisationen und Resourcen
  - Flexibles, koordiniertes und sicheres Teilen von Resourcen
  - Idee: Bessere Problemlösungen durch zusammenschliessen von mehreren Organisationen/Personen/Resourcen

Foster et al. [1]
"Anatomy of the grid"

- **Autorisierung im Kontext**
  - Hochflexible Teilungsbeziehungen unter präziser Kontrolle
  - Kontrolle wie genau die geteilten Resourcen benutzt werden
  - Wer oder welches Gruppen-/Projektmitglied darf Resourcen nutzen
  - Anforderung: Dynamische fein-granulierte Autorisierung für die sichere Koordinierung und Kontrolle des Teilens im Grid

→ Grimm + Weisz,
"Grid Security Tutorial", ab S. 44

Zur Erinnerung: „Classic VOMS“ (1)

- **Virtual Organization Membership Service (VOMS)**
- **Beantwortet Anfragen mit signierten Assertions**
  - Proprietäres XML Protokoll, keine Web service Schnittstelle
- **Assertions (dt. Zusicherungen) beinhalten Attribute**
  - Sogenannte Fully Qualified Attribute Names (FQANs)
  - “Position des Benutzers in einer VO”
  - n x Aufbau: /VO/group/subgroup(s)
  - Arten von Attributen: Gruppen-/Projektteilnahme/Rollen
- **Assertions werden per “Attribute Certificate” (AC) zurückgegeben und benutzt**
  - Standard Format nach IETF RFC 3281

→ Grimm + Weisz, “Grid Security Tutorial”, ab S. 51

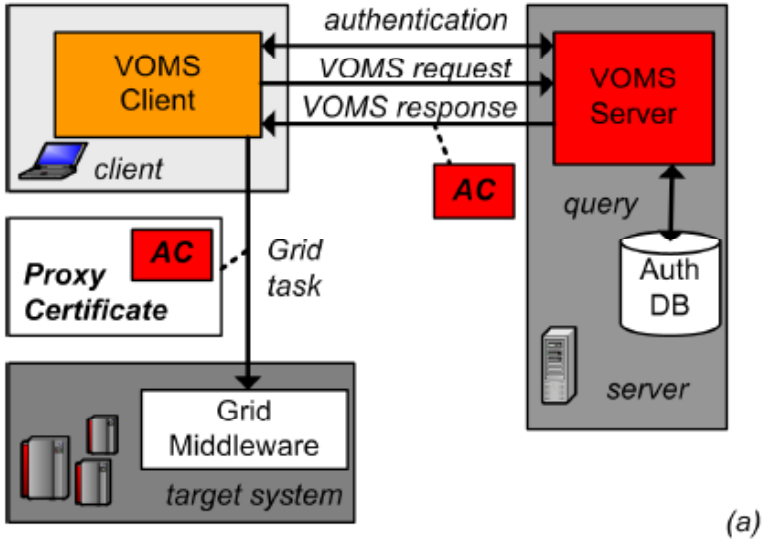
Farrell et al. [5]
IETF RFC3281

Zur Erinnerung: „Classic VOMS“ (2)

- **„Attribute Certificates“ sind eingebettet in den Proxy Zertifikaten der Benutzer**

Tuecke et al. [6]
IETF RFC3820

- **Bedeutet…**
  - Wenn Benutzer mit seinem Proxy eine Grid Middleware kontaktiert liefert er ein VOMS AC mit
  - Anhand dieser Information kann dann eine fein-granulierte Autorisierung vorgenommen werden



Alfieri et al. [8]
“From gridmapfile to voms: managing authorization in a grid environment”

„SAML – basierter VOMS“ (1)

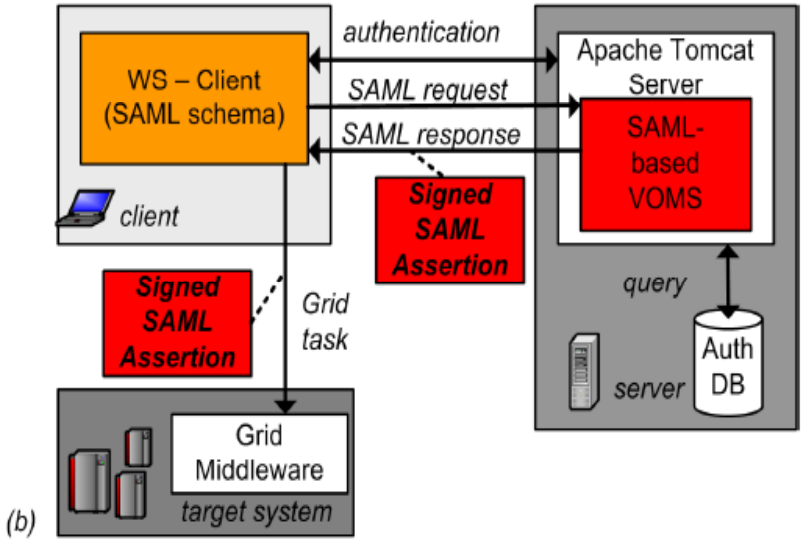
- **Beantwortet Anfragen mit signierten SAML Assertions**
  - Standardisiertes Protokoll, welches ein Standard Format zurückgibt
  - Web service Schnittstelle mit SAML Query/Response Operationen

Venturi et al. [7]
OGF AuthZ Attribute Exchange Profile

- **Entwickelt in OMII – Europe, geplant in gLite → EGEE-III**
  - “Neutraler” Web service → nicht fest in gLite mehr eingebunden
  - Web service ist “deployed” in einem typischen Apache Tomcat
  - Betrieb (erstmal) parallel zu der “Classic VOMS” Variante
- **Benutzt dasselbe Backend wie der “Classic VOMS”**
  - “Classic VOMS” parallel zu SAML-basiertem VOMS mit gleicher VOMS DB zur Speicherung der VO-Daten der Benutzer
  - VOMS DB Verwaltung weiterhin durch VOMS Admin Programm

„SAML – basierter VOMS“ (2)

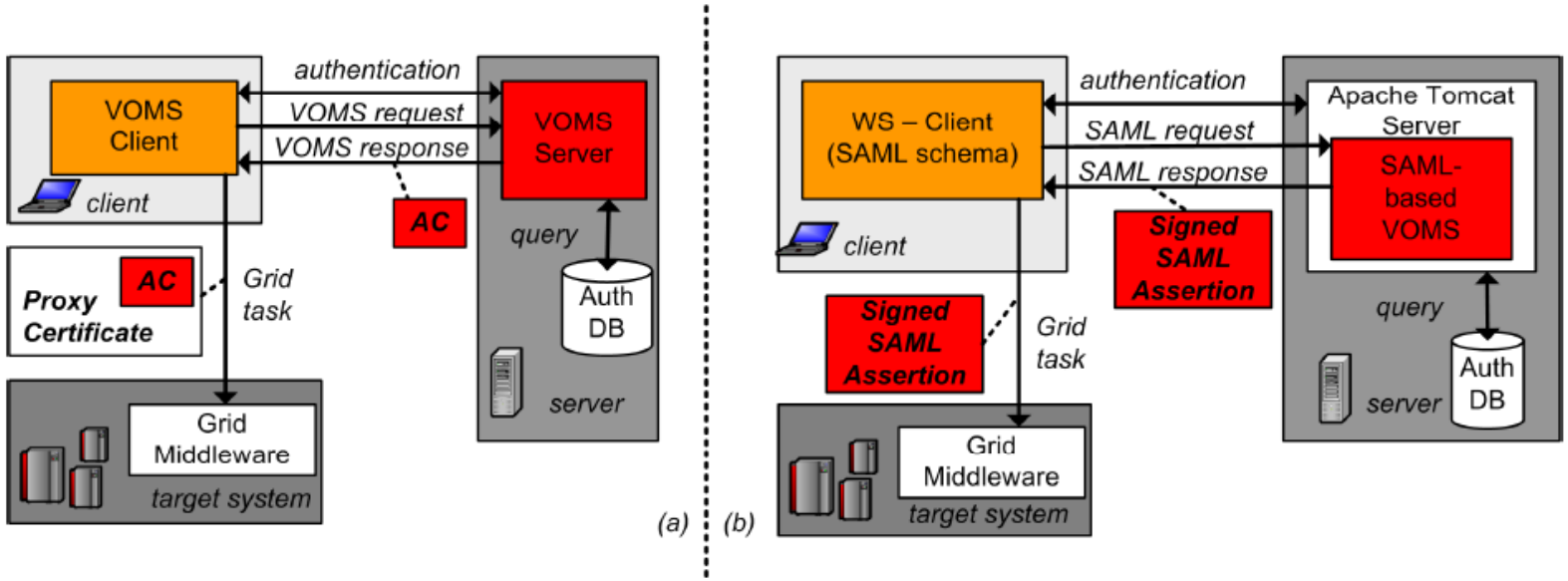
- **SAML Assertions beinhalten nun die VO Attribute**
- **Enthalten daneben aber auch “Conditions” ähnlich wie X.509 proxies**
  - Z.b. Gültigkeitszeiträume
  - Z.b. Maximale Anzahl der Weiterverwendung
- **Enthalten auch…**
  - …wer die SAML Assertion ausstellte (“Issuer”)
  - …über welche Person die SAML Assertion etwas aussagt (“Subject”)



Venturi et al. [9]
“Virtual Organization Management Across Middleware Boundaries”

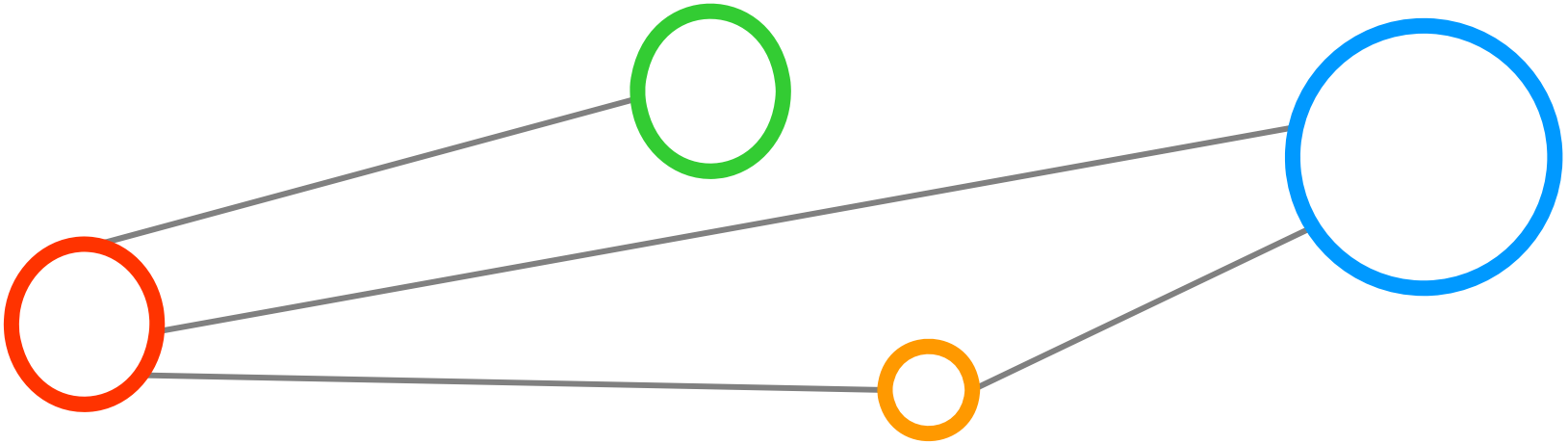
Beide Systeme auf einen Blick

- **Integration von offenen Standards erlauben nun mehrere Szenarien und Verwendung des VO Konzepts**



Venturi et al. [3]
„Using SAML-based VOMS for Authorization within Web Services-based UNICORE Grids“

Aufbau und Transport von SAML Assertions



omii europe
open middleware infrastructure institute

OpenGridForum
OPEN FORUM | OPEN STANDARDS

UNICORE

gLite

the globus alliance

CROWN

EU project: RIO31844-OMII-EUROPE

Issuer

- **SAML Assertion ist eine atomare Einheit**
  - Verbindet quasi Proxies mit Attribute Certificate VOMS Angaben

```
<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>
     ...
     <ds:KeyInfo>
         <ds:X509Data><ds:X509Certificate>CRYPTIC</ds:X509Certificate></ds:X509Data>
     </ds:KeyInfo>
   </ds:Signature>
   ...
</saml:Assertion>
```

Subject

- **Der Issuer sagt etwas über das Subject aus**
  - Subject konnte sich durch Schlüssel ausweisen

```
<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>…</saml:Issuer><ds:Signature>…</ds:Signature>
    …
   <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>CRYPTIC</ds:X509Certificate></ds:X509Data>
          </ds:KeyInfo>
        </saml:SubjectConfirmationData>
     </saml:SubjectConfirmation>
  <saml:Subject>
  …
</saml:Assertion>
```

AttributeStatement

- **Der Issuer sagt etwas genaues über das Subject aus**
  - VO/Gruppen/Rollen kodiert als Attribute (mit begrenzter Gültigkeit)

```
<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>…</saml:Issuer><ds:Signature>…</ds:Signature>
  …
  <saml:Subject>…<saml:Subject>
  …
  <saml:Conditions NotBefore="2007-04-22T14:34:10.060Z" NotOnOrAfter="2007-04-23T02:34:10.060Z" />
  …
  <saml:AttributeStatement>
    <saml:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                        Name="http://voms.forge.cnaf.infn.it/group"
                                        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/fzj/production
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Eine vollständige SAML Assertion

→ **Beispiel: Datei samlassertion.xml**

Transport von SAML Assertions

- **Möglich innerhalb von Proxies (als Extension)**
- **„Signiertes XML“ (assertion) kann prinzipiell überall hin**
- **Besser: Nutzung von WS-Security Security Extensions**

WS-Security Security Extensions [19]

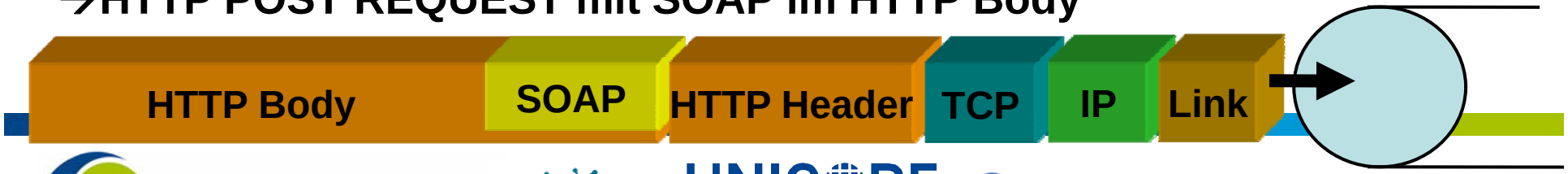
  – Assertions werden standardisiert in den SOAP header eingebracht
  – NameSpace xmlns:wsse = "docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
- **Grid Client kontaktiert VOMS und fügt die SAML Assertion in den SOAP:Header bei einem Grid Job**
- **Grid Middleware entnimmt die SAML assertion aus dem SOAP:Header und nutzt sie zur Autorisierung**

SAML Assertion im SOAP Header

→ Beispiel: Datei samlassertionAndSOAP.xml

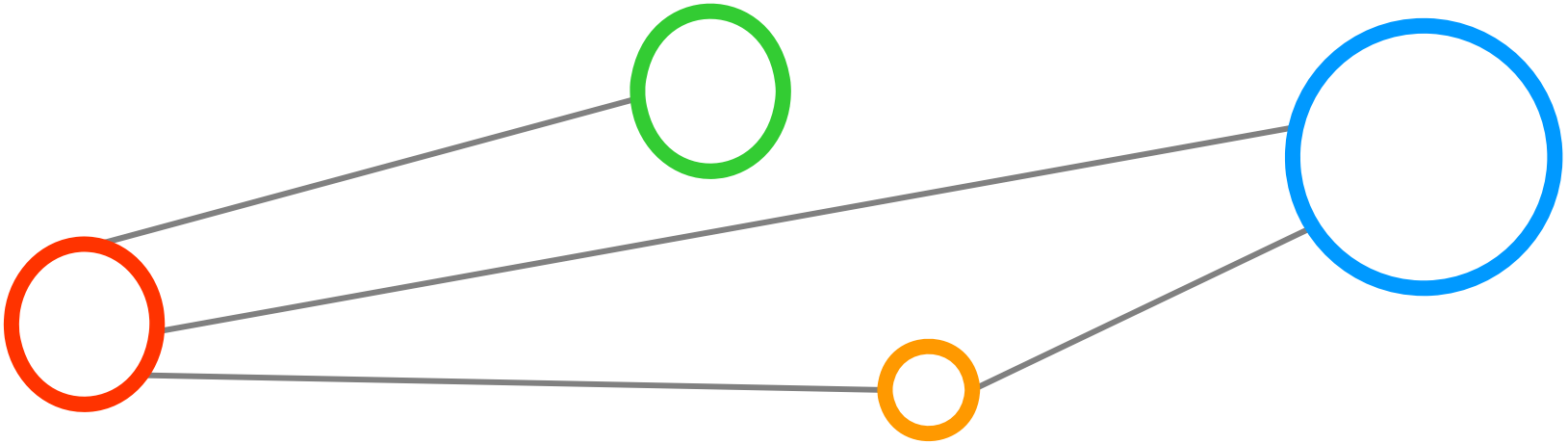
```
<soap:Envelope xmlns:soap="...„>
  <soap:Header>
     <wsse:Security wsse="...„>
        <saml:Assertion xmlns:saml="...">
        ....
        </saml:Assertion xmlns:saml="...">
     </wsse:Security>
   </soap:Header>
   <soap:Body>
   ... // Hier kommen
   </soap:Body>
</soap:Envelope>
```

→HTTP POST REQUEST mit SOAP im HTTP Body



EU project: RIO31844-OMII-EUROPE

SAML in einem Interoperabilitäts – Szenario



EU project: RIO31844-OMII-EUROPE

e-Infrastructure Inseln in Europa

DEISA [11]

- **DEISA Grid (Supercomputing/HPC community)**
  - Nicht WS-basiert UNICORE 5: Proprietäre Jobs (AJO/UPL)
  - Kein Virtual Organization Membership Service (VOMS), Volle X.509
  - Nützlich für massiv-parallele Jobs (MPI, viele Interaktionen)
- **EGEE Grid (hauptsächlich HEP community + andere)**
  - Nicht WS-basiert gLite: Proprietäre Jobs (JDL)
  - Proxy-basiert X.509 Sicherheit, aber "Classic VOMS" support EGEE [12]
  - Nützlich für "Farming Jobs" (wenig Interaktion zwischen cores)
- **Beide sind momentan nicht technisch interoperabel**
  - Anwender kann nicht (nur) eine Middleware nutzen als Zugang
  - **Middlewares hatten bislang nicht viele Standards integriert**

A guide to European flagship e-Infrastructure projects

OMII – Europe im Kontext

EC e-Infrastructures [10]

Knowledge is the **most valuable commodity in today's economy** and e-Infrastructures can be understood as the highways for creating and disseminating this k knowledge widely available throughout society. **So what exactly are eInfrastructures?**

'e-Infrastructure' is the short term for *Electronic Research Infrastructures*.

These are collections of ICT based resources and services used by the worldwide research and education community to conduct collaborative projects and generate

These ICT based resources consist of telecommunication links, computers, storage systems, instruments, software and related computer technology. Importantly organisations operating in different locations in the world.

European eInfrastructures are structured into the following elements:

- Connectivity (Géant2): high-speed internet backbone connecting research and education institutes.
- Cluster grids (EGEE-II): clusters of computers around the world that are connected on the above Géant network to maximse their full power.
- Supercomputer Grid (DEISA): Supercomputers linked together, also on the Geant2 network, to run groundbreaking applications not possible on just one.
- Middleware (OMII Europe): A 'software' that allows you to use and easily access these above distributed EGEE and DEISA grid infrastructures.

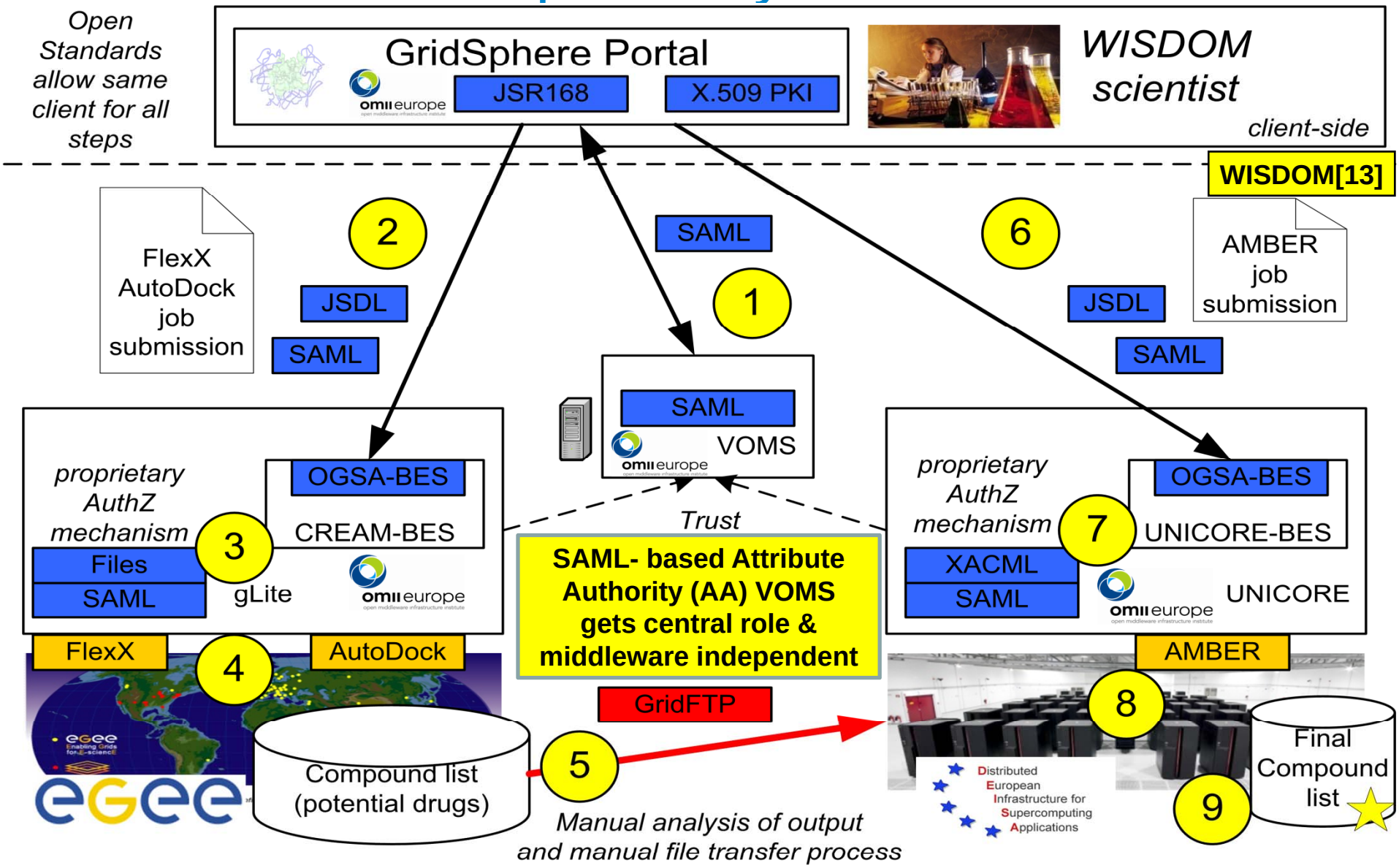
Together these elements form the eInfrastructures that create 'Global virtual research communities' that exchange and generate new knowledge.

Whereas 20 years ago the problems that researchers faced in just exchanging information led to the WWW, the need to exchange knowledge in powerful wa resources for collaborative research.

Just as the web led to new dramatic changes, so do these eInfrastructures allow new research, discoveries and working methods that were otherwise impossible.

Download the full version | Download the brief version

SAML in Interoperability Szenario WISDOM



Standards implemented by OMII-Europe I

Scientific Software

Manual usage of technologies by the scientists, no automation possible so far

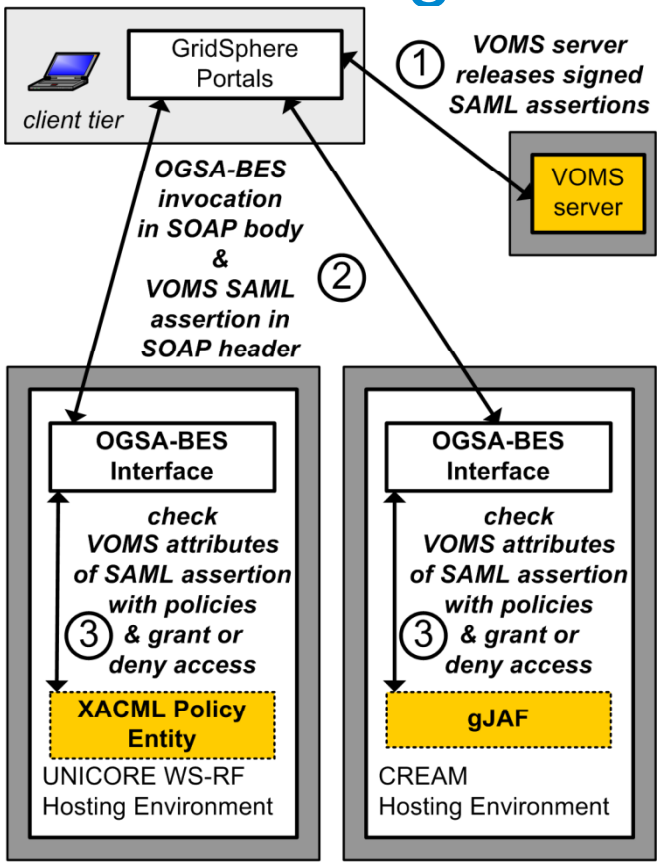
n Steps in the process

Unterstützung von SAML in UNICORE & gLite

- **Offene Standards des SAML-basierten VOMS sind Basis für Interoperabilität**
  - OASIS XACML bietet gute Funktionen zum prüfen der Assertions

XACML [21]

- **Funktioniert nicht nur in Verbindung mit OGSA – Basic Execution Services in Middleware!**
- **Grundidee dahinter funktioniert mit aller Web services**



Marzolla et al. [4], „*Open Standards-based Interoperability of Job Submission and Management Interfaces across the Grid Middleware Platforms gLite and UNICORE*„

Erhältliche Komponenten des Szenarios (1)

- **CREAM-BES (gLite) erhältlich im OMII – Europe Repository**
  - http://repository.omii-europe.org/projects/

omii europe
open middleware infrastructure institute

Repository Projects Sitemap

Enter keywords Search

Quick Links

Home
Help & Support

Login
Registration

All RSS Feed

Home

All Public Projects

Below is a list of the current projects registered with OMII-Europe. Having registered and logged into the website you can add your own project.

Browse by category:

All Public Projects Browse

Project	Status	Summary	Operations
CREAM-BES	PUBLIC	The Computing Resource Execution And Management (CREAM-BES) service is a Grid computing service. Its interface complies with the Basic Execution Service (BES) and Job Submission Description Language (JSDL) specifications.	View Project Summary View Project Details
Credential Management and Conversion Script	PUBLIC	A script for converting Security Credentials to [illegible]	View Project Summary View Project Details
Dgas Rus Client	PUBLIC	This project carried on by OMII-Europe in the field of grid accounting aim to augment the DGAS Accounting System (DGAS) with the OGSA Resource Usage Service (RUS) interface (draft-17). This components is the Web Service command line client to access Accounting Information stored in a RUS server	View Project Summary View Project Details

Erhältliche Komponenten des Szenarios (2)

- **SAML VOMS erhältlich im OMII – Europe Repository**
  - http://repository.omii-europe.org/projects/

			Details
Unicore 5 Gateway Proxy Acceptance Extensions	PUBLIC	Unicore 5 Gateway extensions to enable it to acceot X509 proxy certificates	View Project Summary View Project Details
UNICORE 6 OGSA-BES Adoption	PUBLIC	Implementation of the OGSA-BES and JSDL interface specification of the Open Grid Forum. In combination with some HPC-based extensions to JSDL, this version of UNICORE 6 is OGF HPC-Profile compliant.	View Project Summary View Project Details
UNICORE 6 OGSA-RUS Adoption	PUBLIC	Components and documents of the UNICORE 6 OGSA-Resource Usage Service (RUS) adoption, which implies the adoption of the Usage Record (UR) format standard. Both standards are emerging from the Open Grid Forum (OGF).	View Project Summary View Project Details
UNICORE 6 SAML-based VOMS Support	PUBLIC	Software to use UNICORE in conjunction with the SAML-based Virtual Organization Membership Service (VOMS)	View Project Summary View Project Details
Vine Toolkit	PUBLIC	A Java Grid application framework	View Project Summary View Project Details
VOMS SAML Service	PUBLIC	The Virtual Organization Membership Service is an Attribute Authority focused on Virtual Organization Management. This component provides an interface implementing recommendation and specifications from the OGF OGSA Authorization WG.	View Project Summary View Project Details

Erhältliche Komponenten des Szenarios (3)

- **SAML-basierte VOMS Unterstützung und OGSA-BES für UNICORE 6 erhältlich im OMII – Europe Repository**
  http://repository.omii-europe.org/projects/

UNICORE 6 SAML-based VOMS Support	PUBLIC	Software to use UNICORE in conjunction with the SAML-based Virtual Organization Membership Service (VOMS)	View Project Summary View Project Details

- **Auch erhältlich via UNICORE@SourceForge**
  - **http://www.unicore.eu**

UNICORE

UNICORE (Uniform Interface to Computing Resources) offers a ready-to-run Grid system including client and server software. UNICORE makes distributed computing and data resources available in a seamless and secure way in intranets and the internet.

- Home
- UNICORE
- Testgrid
- Download
- Documentation
- Community
- UNICORE Forum e.V.
- UNICORE Summit

News

Latest Archive

Chemomentum and UNICORE OpenDay in Tartu (Estonia) 10 Mar 2008

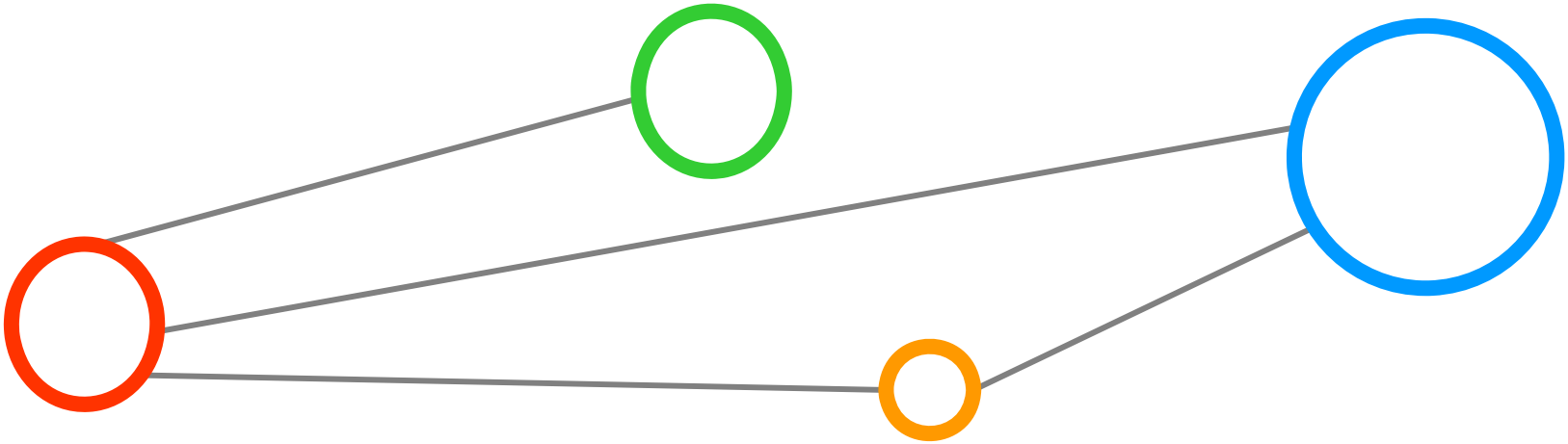
The Chemomentum project is organising a tutorial on UNICORE 6 and the Chemomentum system in Tartu (Estonia) on April 3, 2008. Detailed information can be obtained from

http://www.chemomentum.org/open_day_1 (0 comments)

Latest Releases

- Unicore6-OGSA-BES 1.0.0, 03 Mar 2008
- Unicore6-SAMLVOMS 1.0.0, 03 Mar 2008
- Unicore6-CommandlineClient 6.1.0-rc, 22 Feb 2008
- Unicore6-WorkflowSystem 6.1.0-rc, 22 Feb 2008

Andere Anwendungen von SAML im Grid



EU project: RIO31844-OMII-EUROPE

UAS-VO Service von Chemomentum

- **SAML-basierter VO service welcher die gleichen Standards integriert wie der SAML-basierte VOMS**
- **Zusammen mit VOMS teilgenommen in OGSA-AuthZ working group interop beim OGF22 in Boston**
- **Initiale Entwicklung von ICM in Polen**
- **Nun offene Community Entwicklung bei UNICORE@SourceForge:**
  - http://unicore.svn.sourceforge.net/viewvc/unicore/unicorex/uas-vo/

Chemomentum [2]

IVOM Projekt

IVOM [16]

- **IVOM → „Interoperability and Integration of VO management Technologies in D-Grid“**

Grimm et al. [14]
„ Trust Issues in Shibboleth-Enabled Federated Grid Authentication and Authorization Infrastructures Supporting Multiple Grid Middleware“

- **SAML Standard wird auch in Shibboleth verwendet**
  - (Wie gesehen gestern in der DEMO von Ralf Groeper et al.)
- **Shibboleth ist SAML-basierte Attribute Authority (AA)**
  - (In diesem Talk lernten wir das VOMS eine SAML-basierte AA ist)
  - GridShib: SAML assertions können direkt in ein „Short Lived Credential (SLC)“ integriert werden
  - GridShib: Optional SAML Assertions an X.509 Proxies gebunden

GridShib [15]

SAML als Lösung zu Proxy Problemen?

→ Anknüpfung an Diskussionen von gestern: Proxy nicht in Industrie für reale Szenarien sinnvoll!?

- **Es gab einen guter Grund warum UNICORE nie Proxies unterstütze**
  - Industriepartner wie Intel, Fujitsu, T-Systems… seit Beginn dabei
- **Industrie ist von Proxies nur eingeschränkt überzeugt**
  - Beispiel gestern von D.Rubin im Rahmen von ProGrid: *„Industriepartner sagte…gehen wir Richtung echter Produktion ist ein Einsatz von Proxies nicht realistisch…“*
  - Weitere Diskussionen ergaben sich dadurch, generelles Fazit: *„Proxies nicht zweckgebunden an eine Operation unerwünscht…“*
- **Probleme an vielen anderen Ecken und Enden…**
  - Bottom line: Volle Inpersonifikation (man darf kurzzeitig alles)
  - VOMS-Attribute beschränken grob für was – „schränkt Macht ein“

SAML Delegation (1)

- **Problem der Delegation (und Proxies) ist nicht neu…**
  - Keine anderen Lösungen für Delegation? (doch, ggf. nicht perfekt)
  - Nur ein Beispiel aus dem Internet zur Delegation (in der Industrie)

http://www.identityblog.com/?p=703#comments

Scott Cantor March 25, 2007 | 11:09 am

I hate to do this again, but I feel compelled to comment. Everything you say here about the SAML protocol is wrong.

It is not a single token design, never has been. A lot of the changes in SAML 2.0 were designed by me explicitly to better support delegation scenarios, and it does support them (usually by using multiple SAML tokens or with a token exchange model). And on top of all that, it supports non-SAML tokens exactly like WS-Trust does, it just requires a SAML token around them.

You've noted problems with the use of SAML assertions, and some of them are quite valid. These issues are not. On the contrary, it is WS-Trust which lacks interoperable profiles around performing delegation in conjunction with SSO. SAML and Liberty have them. That's the reality of things.

Bei Weiterlesen zu dem Thema würde man folgende Konsequenzen im Beispiel für MediGrid sehen: „Zugriffe auf Patientendaten können im Grid delegiert werden, ABER mit der Einschränkung <u>welche</u> Ärzte (oder Arzttypen) <u>was</u> genau damit machen dürfen und für <u>wie lange</u>… → Ticket?! (Link zu Pattloch: Problem wird tatsächlich auf einer anderen Ebene gelöst → man darf halt nicht alles)

SAML Delegation (2)

- **SAML 2.0 Single Sign-On with Constrained Delegation**
  - SAML „Delegation Profiles“ wäre ein eigener Vortrag, daher nur kurz
- **Jeder Delegierende muss ein eindeutiges <saml:SubjectConfirmation> Element beifügen**
  - Darin enthalten sind Name, KeyInfo, etc. des Delegierenden
- **Dazu kommt ein <saml:AudienceRestriction> Element**
  - Wird benutzt um anzugeben mit wem/was der Delegierende die Assertion zur AuthN oder AuthZ benutzen darf (WICHTIG!)
  - Also eingeschränkte Delegation im Auftrag des Subjects
- **Attribute erlauben das fine-tuning <u>wofür</u> die Assertion benutzt wird**

Cantor et al. [20]
„SAML 2.0 Single Sign-On with Contrained Delegation“

SAML Delegation (3)

- **Anstelle von Proxies echte X.509 Zertifikate**
- **Dazu gibt man eine beliebige Anzahl von SAML Assertions mit Rechten die man delegieren will**
  - Initial signiert von Attribute Authority (AA), dann von Delegierenden
  - Beispiel im Grid: UNICORE 6 nutzt SAML Delegation statt Proxies
- **Löst Proxy Problem der vollen „Inpersonifikation“**
  - Industrie sagt kontextbezogene Inpersonifikation ist ja ok
  - SAML Assertion erlaubt Identität der AA zu prüfen
  - Kontextbezogene Attribute können benutzt werden
  - SAML Assertion ist atomar!

Cantor et al. [20]
„SAML 2.0 Single Sign-On with Contrained Delegation“

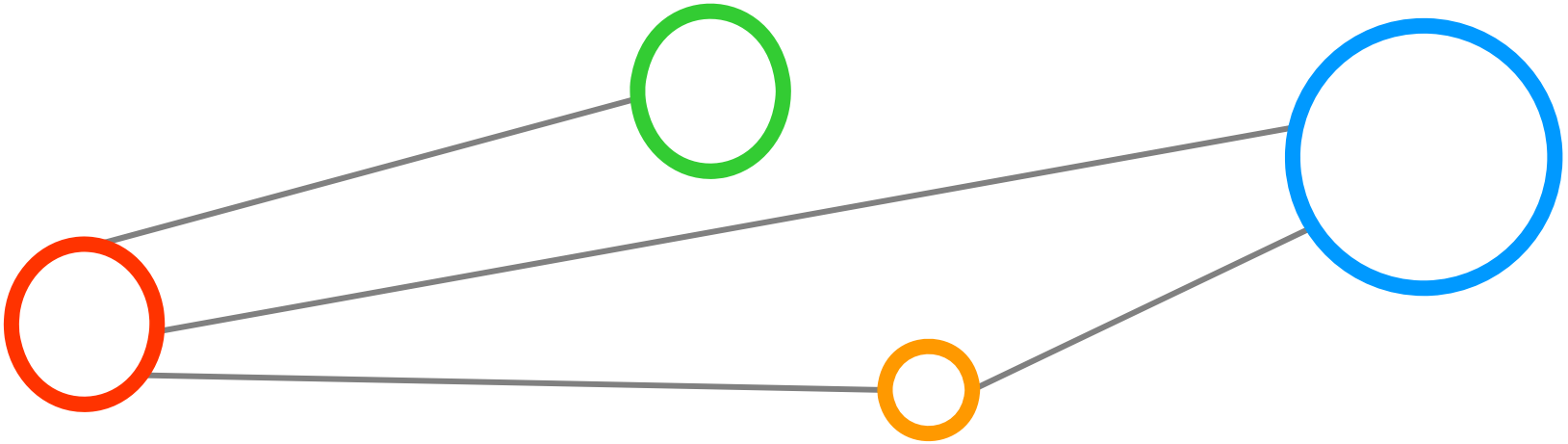
→ Chance die Proxy Problematik von Industrievertretern für die „Grid-Industrie“ zu lösen

SAML Delegation (4)

- **Ein paar Vorteile…**
  - Im Sinne der Informatik lose gekoppelt mit Transport Level (SAML Assertions unabhängig von SSL Verbindung, gut da einige Web Server keine Proxy-chain checken→ Bsp.: Jetty server)
  - SAML Assertions kann man flexibel überall benutzen (im SOAP Header oder innerhalb von Dokumenten, etc.)
  - Proxy delegation erzeugt neue Proxy credentials per Delegierenden (Zeitgewinn: Assertions werden nur erweitert per Delegierenden)
- **Nachteile?**
  - Zwar Möglichkeit zu definieren wer was wofür machen darf…. →
  - Jedoch etwas weniger flexibel als Proxy → Aber: so will die Industrie das (oft) nun mal! Fakt den GSI-Vertreter nicht bestreiten können…

Wieder Link zu Diskussion gestern: SAML Assertion ist ähnlich wie ein „Ticket“ was von mehreren abgestempelt wird…

Schlussbemerkungen



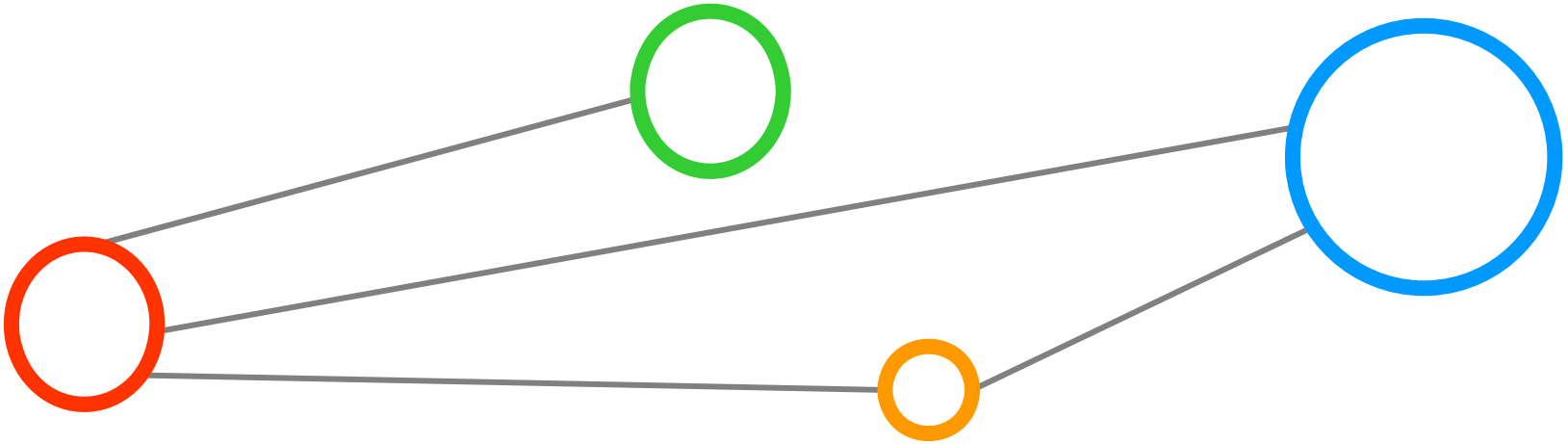
Schlussbemerkungen

- **Industrie macht viel mit dem SAML Standard und entwickelt ihn dementsprechend immer weiter**
  - SAML ist seit mehreren Jahren ein etablierter Standard von OASIS
  - SAML Version 2.0 erlaubt unglaublich viele Möglichkeiten
- **SAML findet sich auch im Open Grid Forum (OGF)**
  - OGF OGSA – Authorization Arbeitsgruppe arbeitet mit SAML
- **SAML wird in zwei wichtigen Komponenten benutzt**
  - Als Attribute Authority in VOMS UND Shibboleth
- **SAML „überbrückt“ die Grid Middleware „Inseln“**
  - Unterstützung von SAML in gLite, UNICORE und Globus Toolkits

→ SAML als Chance in D-Grid als einheitliche Technologie

Sax: SAML und XACML auch im Gesundheitsbereich etabliert

Referenzen



Referenzen (1)

[1] Foster, Kesselman, Tuecke, Anatomy of the grid, International J. Supercomputer Applications, 15(3), 2001

[2] Chemomentum Project, http://www.chemomentum.org/

[3] *Using SAML-based VOMS for Authorization within Web Services-based UNICORE Grids, Venturi et al., UNICORE Summit 2007 @ EuroPar 2007*

[4] M. Marzolla, P. Andreetto, V. Venturi, A. Ferraro, A.S. Memon, M.S. Memon, B. Twedell, M. Riedel, D. Mallmann, A. Streit, S. van de Berghe, V., Li, D. Snelling, K. Stamou, Z.A. Shah, F. Hedman
Open Standards-based Interoperability of Job Submission and Management Interfaces across the Grid Middleware Platforms gLite and UNICORE
Proceedings of International Interoperability and Interoperation Workshop (IGIIW) 2007 at 3rd IEEE International Conference on e-Science and Grid Computing, Bangalore, India, December, 2007, IEEE Computer Society, ISBN 0-7695-3064-8, pp. 592 - 599

[5] IETF RFC3281, Farrell et al., http://www.faqs.org/rfcs/rfc3281.html

[6] IETF RFC3820, Tuecke et al., http://www.faqs.org/rfcs/rfc3820.html

[7] OGF AuthZ Attribute Exchange Profile, Venturi et al., https://forge.gridforum.org/projects/ogsa-authz

[8] „From gridmapfile to voms: managing authorization in a grid environment", Alfieri, Cecchini, Ciaschini, dell'Agnello, Frohner, Lörentey, und Spataro. *Future Generation Comp. Syst., 21(4):549–558, 2005.*

Referenzen (2)

[9] *„Virtual Organization Management Across Middleware Boundaries"* , Venturi et al., Int. Grid Interoperation and Interoperability Workshop (IGIIW) 2007 @ e-Science 2007, Bangalore, India

[10] European e-Infrastructures, http://www.beliefproject.org/cookbook/cookbook-intro/view

[11] DEISA Project, http://www.deisa.org

[12] EGEE Project, http://public.eu-egee.org/

[13] WISDOM Project, http://wisdom.eu-egee.fr/

[14] Grimm et al., *"Trust Issues in Shibboleth-Enabled Federated Grid Authentication and Authorization Infrastructures Supporting Multiple Grid Middleware"*, International Grid Interoperation and Interoperability Workshop (IGIIW) 2007 @ e-Science 2007, Bangalore, India

[15] GridShib, http://gridshib.globus.org/

[16] IVOM Project, http://www.dgrid.de/index.php?id=314

[17] SAML Technical Committee, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

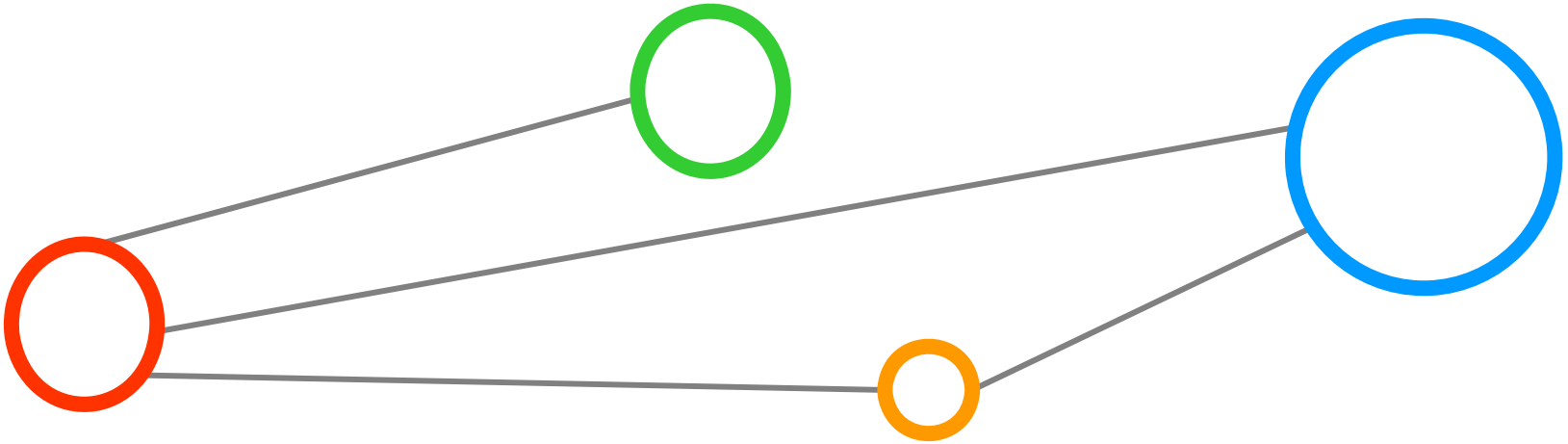
[18] SAML Technical Overview, J. Hughes et al., OASIS, February 2005. Document ID: sstc-saml-tech-overview-2.0-draft-03, see http://www.oasisopen. org/committees/security/

[19] WS-Security Security Extension, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

[20] „SAML 2.0 Single Sign-On with Contrained Delegation", Cantor et al., 2005, OASIS SAML TC, http://shibboleth.internet2.edu/docs/draft-cantor-saml-sso-delegation-01.pdf

[21] „Extensible Acces Control Markup Language (XACML), OASIS XACML TC

Danksagungen



EU project: RIO31844-OMII-EUROPE

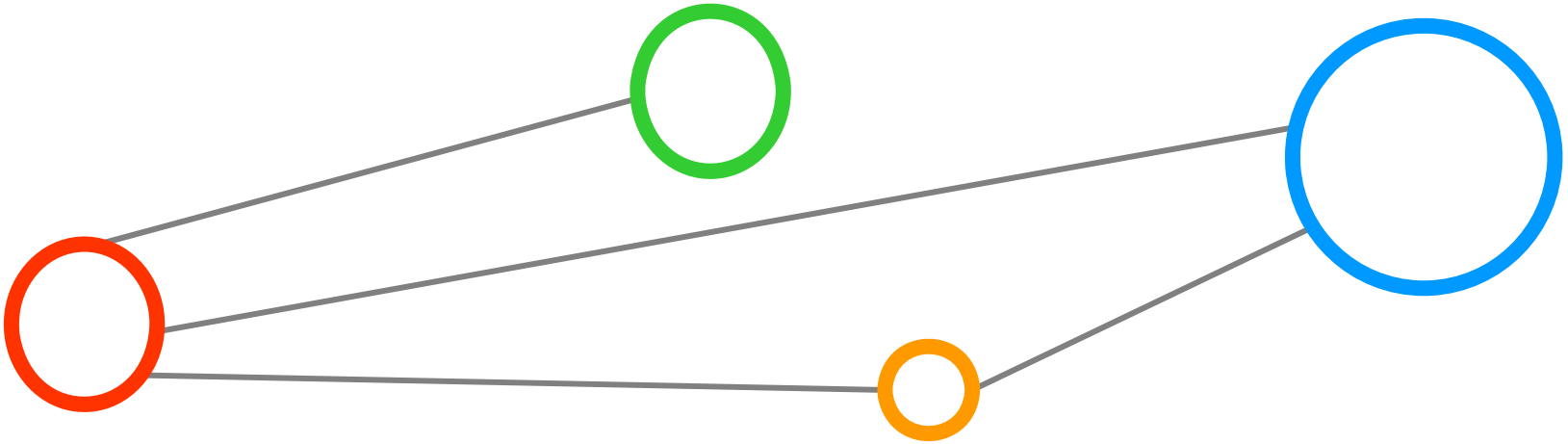
Danksagungen

- **Open Middleware Infrastructure Institute for Europe**

  – OMII – Europe project under EC grant RIO31844-OMII-EUROPE, duration May 2006 - April 2008

- **Jülich Supercomputing Centre (JSC) of Forschungszentrum Jülich (FZJ) in the HELMHOLTZ association, Germany**

Ankündigungen



OGF 23 @ Barcolona

The 23rd Open Grid Forum

June 2 - 6, 2008

Barcelona, Spain

OpenGridForum
OPEN FORUM | OPEN STANDARDS

OpenGridForum
OPEN FORUM | OPEN STANDARDS

For more Information please visit:

http://www.ogf.org/OGF23/

omii europe
open middleware infrastructure institute

OpenGridForum
OPEN FORUM | OPEN STANDARDS

UNICORE

gLite

the globus alliance

CROWN

EU project: RIO31844-OMII-EUROPE

Grid Interoperation Now (GIN)

D-Grid → Interessiert an Interoperation/Interoperability:

Besucht die GIN Community Group beim 23rd Open Grid Forum

June 2 - 6, 2008

Barcelona, Spain

http://www.ogf.org/OGF23/

EU project: RIO31844-OMII-EUROPE