Security (JRA3)

Åke Edlund, JRA3 Manager, KTH
David Groep, Security Expert, NIKHEF
EGEE 1st EU Review
9-11/02/2005

Introduction - JRA3 Objectives

- **Enable secure operation of a European Grid infrastructure.**
  - Develop security architectures frameworks and policies.
  - Includes requirements cycle,
  - definition of incident response methods and
  - authentication policies.
- **Consistent design of security mechanisms for all core Grid services.**
  - Meet production needs of resource providers with regard to identity integrity and protection.
- **Provide robust, supportable security components**
  - Select, re-engineer, integrate identified Grid Services
- **Selection of security components based on requirements of**
  - The Middleware developer's
  - The Applications
  - The Operations
- **Support and evolve the middleware components (as part of JRA1)**

Introduction - Achievements, Issues and Mitigation

Major achievements for this past period

Producing a **Global Security Architecture** document (DJRA3.1), well received from the community and a **Site Access Control Architecture** document (DJRA3.2). A number of **security modules**, of which four will be added to the first release candidate.

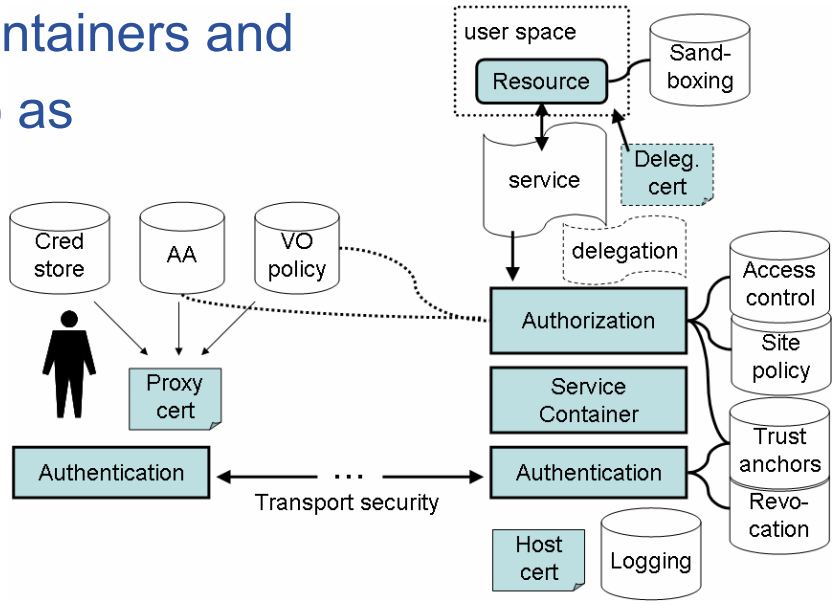
Major issues and mitigation

- **Geographically distributed teams:**
  - Need to improve the handing over of security modules to the middleware developers. More traveling for the JRA3 members.
  - Improve further contact with NA4, applications: The Middleware Security Group (MWSG, chaired by JRA3) has been the meeting point so far. Need more.
- **Conflicting/challenging security requirements from applications**
  - Connectivity. *Mitigation: Dynamic Connectivity Service*
    Sites: 'worker nodes' shall have no global connectivity
    Apps: 'worker nodes' must have full connectivity
  - Identity anonymity vs. identity traceability. *Mitigation: Pseudonymity Service*

Architecture - Baseline assumptions

Security Architecture - Modular, Agnostic, Standard, Interoperable

- Modular – add new modules later
- Agnostic – modules will evolve
- Standard – start with transport-level security but intend to move to message-lever security when it matures
- Interoperable - at least for AuthN & AuthZ
- Applied to Web-services hosted in containers and applications (Apache Axis & Tomcat) as additional modules



Architecture - Baseline assumptions

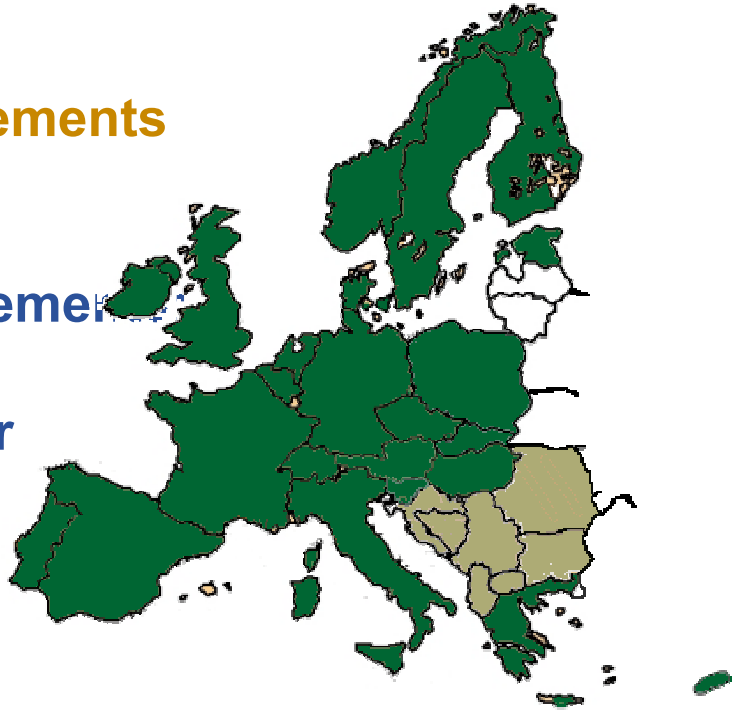
Security Requirements - Horizontal activity, managed through central groups

- Lesson learned: reused and updated requirements from earlier projects
- Collecting (continuous process) the requirements from the activities - Middleware, Sites, Applications.
- Share the requirements with other grid activities and get feedback, e.g. in the US
- Prioritization set in the security groups, with representatives from all involved activities.
- Defining what security modules to deliver when.

EUGridPMA

European Grid Authentication Policy Management Authority for e-Science

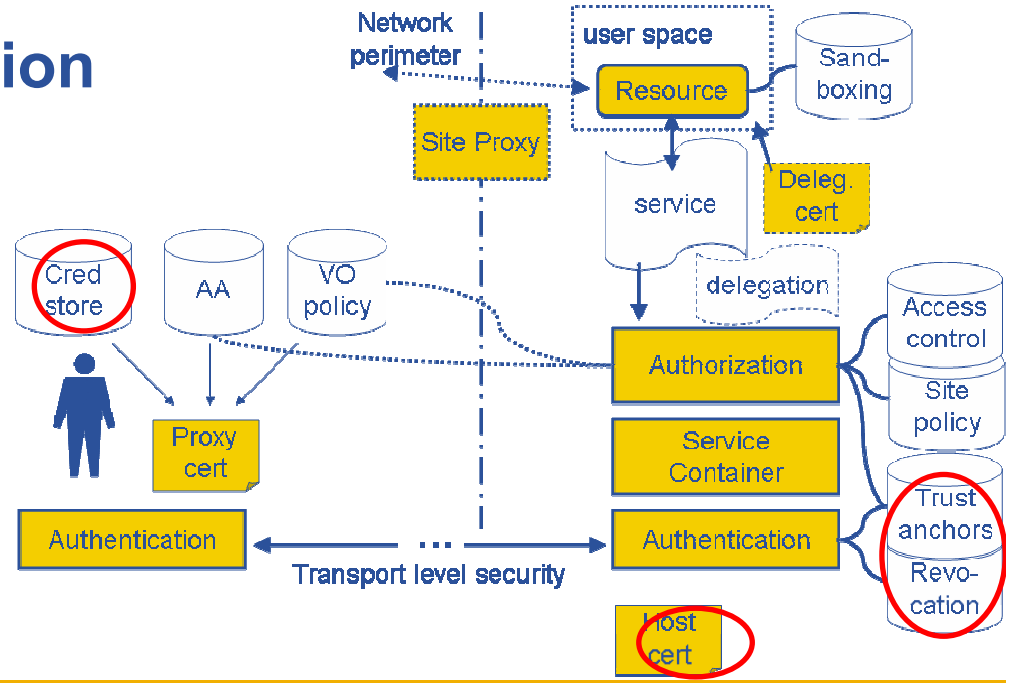
- **Setting guidelines and minimum requirements for Grid authentication for e-Science**
- **Now a Global federation of grid identity providers, based on EUGridPMA requirements and the *International Grid Federation* (IGF)**
- **EUGridPMA was the driving example for similar groups in Asian-Pacific and the Americas**
- **Coverage of Europe almost complete**
  - 30 accredited members
  - 7 non-EU countries + 1 treaty organization
- ***Initiative strongly encouraged by e-IRG***



Architecture - Authentication

- ***Managed* credential storage**
  - i.e., where access policy can be enforced
  - "Active" Certificate stores (smart cards, MyProxy)
  - Organizationally rooted trust (KCA, SIPS)
  - Password-scrambled files should go away

- **Better certificate revocation technologies needed**



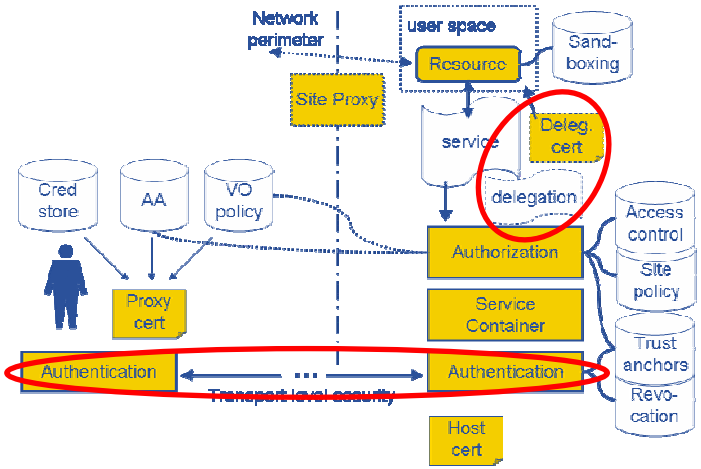
Architecture - TLS vs MLS

- **Transport Level Security**
  - Uses widely deployed TLS/SSL protocol
  - However provide security between communicating host only

- **Message Level Security**
  - Uses Web Services or SOAP messages security technology
  - Recommended by WS-I Consortium as preferable WS-Security solution
  - Performance and support issues

- **So, TLS for now**
  - SOAP over HTTPS with proxy cert supported path validation
  - WS interface for delegation

- **Integrate MLS as we go along**
  - Use cases for MLS exist already (DM)



Overview of the security architecture services (1/3)

Service	Description	Time frame
Logging and Auditing	**Ensures monitoring of system activities, and accountability in case of a security event**	**Now**
Authentication	Credential storage **ensures proper security of (user-held) credentials**	**Now**
	Proxy certificates **enable single sign-on** TLS, GSI, WS-Security **and possibly other X.509 based transport or message-level security protocols ensure integrity, authenticity and (optionally) confidentiality**	**Now** **Now**
	EU GridPMA **establishes a common set of trust anchor for the authentication infrastructure**	**Now**
	Pseudonymity **services addresses anonymity and privacy concerns**	**Mid-term**

Overview of the security architecture services (2/3)

Service	Description	Time frame
Authorization	Attribute authorities **enable VO managed access control** Policy assertion services **enable the consolidation and central administration of common policy** Authorization framework **enables for local collection, arbitration, customisation and reasoning of policies from different administrative domains, as well as integration with service containers and legacy services**	**Now** **Future** **Now**
Delegation	**Allows for an entity (user or resource) to empower another entity (local or remote) with the necessary permissions to act on its behalf**	**Now**

Overview of the security architecture services (3/3)

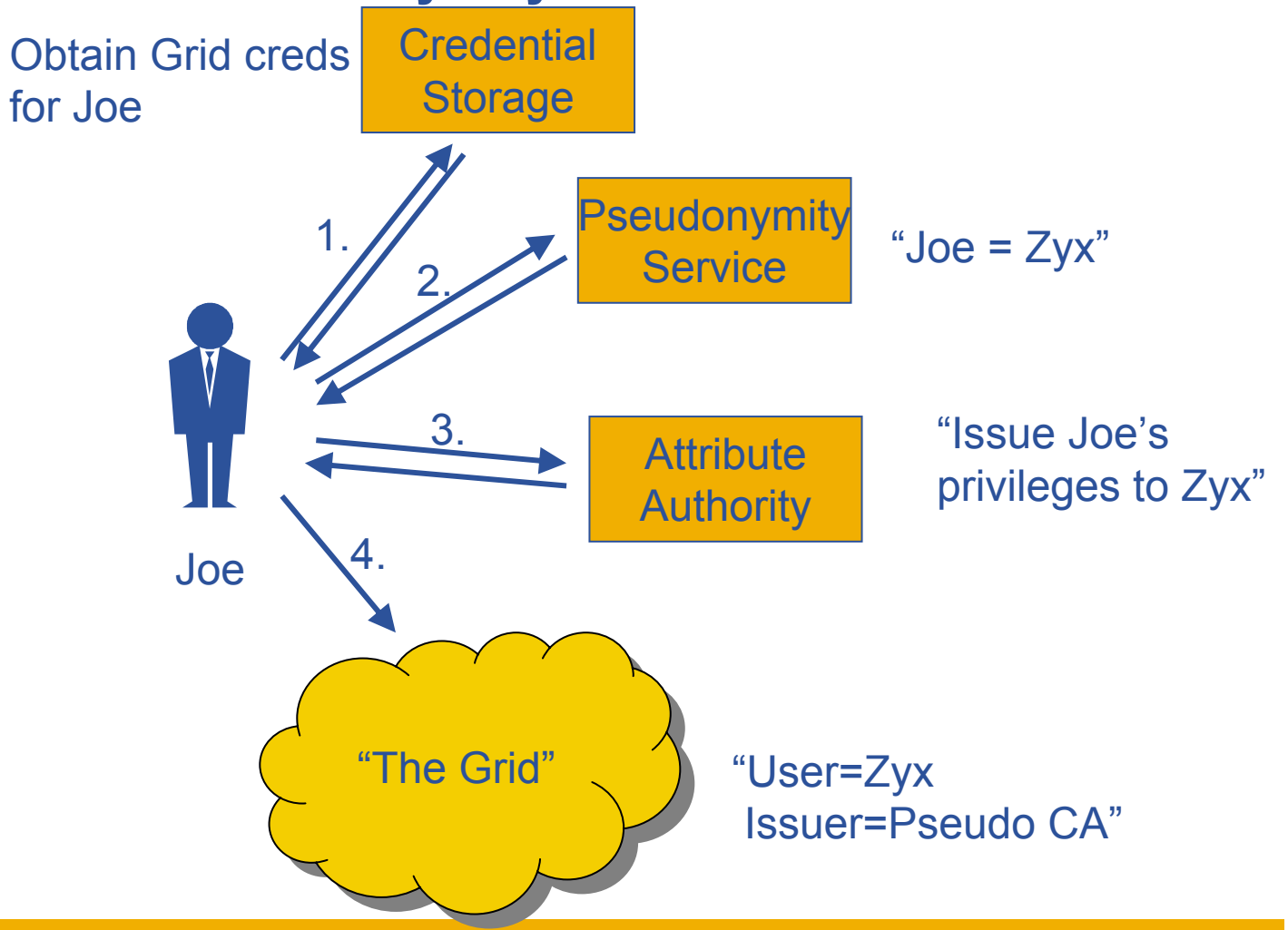
Service	Description	Time frame
Data key management	**Enables long-term distributed storage of data for applications with privacy or confidentiality concerns**	**Mid-term**
Sandboxing	**Isolates a resource from the local site infrastructure hosting the resource, mitigating attacks and malicious/wrongful use**	**Mid-term**
Dynamic Connectivity Service	**Enables applications to communicate despite heterogenous and non-transparent network access**	**Mid-term**

High-level requirements and how the architecture address them

Requirement	Fulfilled	Solution/Technology/Service	Time frame
Single sign-on	Yes	Proxy certificates and a global authentication infrastructure	Now
User Privacy	Partially	Pseudonymity services	Mid-term
Data Privacy	Partially	Encrypted data storage	Mid-term
Audit ability	Partially	Meaningful log information	Now
Accountability	Yes	All system interactions can be traced back to a user	Now
VO managed access control	Yes	VOMS	Now
Support for legacy and non- WS based software components	Yes	Modular authentication and authorization software suitable for integration	Now
Timely revocation delays	Yes	Gradual transition from CRL based revocation to OCSP based revocation	Mid-term
Non-homogenous network access	Yes	Dynamic Connectivity Service	Future

Business Applications - "Anonymity"

- **Issue: Identity anonymity vs. identity traceability**
- **Proposed solution: Pseudonymity**

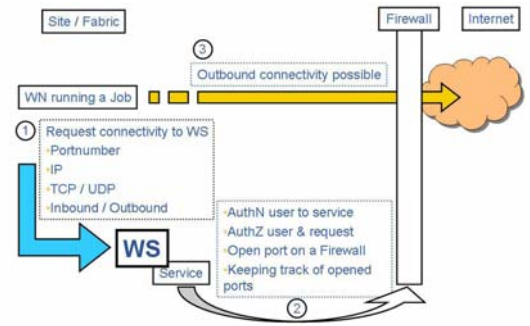


Issue: Conflicting requirements

- Sites: 'worker nodes' shall have no global connectivity
- Apps: 'worker nodes' must have full connectivity

Proposed solution, security-wise (JRA3):

- 'Dynamic Connectivity Service' (DCS)
- Policy-controlled connections to the outside world
- Same fine-grained access control via VOMS
- Grid service interface
- Compliant to work in JRA4



Integration and development

- **JRA3 is, from start of the project, part of the JRA1 development - *as the Nordic Cluster*.**
- **All software development at JRA3 follows the processes of JRA1.**
- **See previous presentation from JRA1.**

Module candidates for Release candidate 1 (RC1):

- **SOAP over HTTPS**
  - This implements transport layer security for web services.
- **Authorization framework**
  - A java rendering of the pluggable authorization framework
- **VOMS support for authorization**
  - The Virtual Organization Membership Service (VOMS) is used for managing the membership to VOs and as attribute authority.
- **Resource Access Control (LCAS, LCMAPS, gatekeeper)**
  - Resource access control is based on LCAS and LCMAPS. The globus WorkSpace Service (WSS) is used for account management.

Plans and status - RC1.x, RC2

- **Ready for later releases of RC1:**
  - Message level security
  - Delegation
  - Grid enhancements for OpenSSL (part of 097/098, i.e. the Feb/March release of OpenSSL)
  - Dynamic Connectivity Service (work ongoing)

- **New release plan to be presented at next MWSG, Feb 23-24**

- **JRA3 has also contributed in:**
  - WorkSpace Service (WSS) - **a EGEE and Globus collaboration**
  - Coordinating and collaborating with JRA1 security work (VOMS)
  - LCG security work (VOMS Admin)

Plans and status - Next 9 months

- PM10-12 **gLite Release 1**
- PM12 **First revision of the Security operational procedures document**
- PM12 **Document describing the framework for policy evalutation expected to be accepted in GridPMA policies and determination of the CA service authorities for EGEE**.
- By PM12 **all EU memberstates active in Grid projects will have a national accredited Authority**.
- PM16 **Global Security Architecture document is revised**, with input from operations, applications, and external collaborating infrastructure projects. The revised architecture will be used to help drive the work on security **software modules that will be included in the 2nd major release of gLite.**
- PM18 **Second revision of the Security operational procedures document**.
- PM18 **A documented assessment** of the work and experience gathered with the basic **accounting infrastructure** already deployed and will highlight what remains to be done to provide a secure, deployable quota allocations and enforcement mechanism.

Plans and status - A word on collaboration

Next period:

- JRA3 will work with **GGF** to define and **prototype a WS proposals and standards based delegation method**.
- All general security aspects will be performed in **collaboration with other grid initiatives** such as **DEISA, OSG, Diligent, NextGrid, CoreGrid, eIRG, TC-EMC2, TF-CSIRT, the Baltic states and Asian collaborators.**

Summary

Top 3 achievements so far:

- **Security architecture in place,** minor revisions expected during the following 9 months.
- **Significant contribution to EUGridPMA (chair) and standardization work (co-chair of GGF Security).**
- **Security components to gLite: continuous work. 4 modules in release candidate 1.0.**

Major Issues:

- **Geographically distributed teams**
- **Conflicting/challenging security requirements from applications**

Questions and answers

Questions about the activity: Ake Edlund

Technical questions: David Groep