Enabling Grids for E-science in Europe

www.eu-egee.org

PEB All-Activity Meeting, September 13, 2004

JRA3 Security

Åke Edlund
Security Head

EGEE is a project funded by the European Union under contract IST-2003-508833

Contents

- Summary of work accomplished since last AA meeting
- Relationship between JRA3 and JRA1 work and deliverables
- Hiring status and manpower levels
- State of deliverables and milestones for PM4-PM6
  - MJRA3.3 - OGSA SEC service initial recommendations for reengineering
  - DJRA3.1 - Global security architecture
  - MJRA3.4 - Security operational procedures and incident handling, definition of a common Grid incident format
- Risk analysis
- Issues related to other activities
- Highest priority steps to take between now and th conference in Den Haag

Summary of work accomplished since last AA meeting

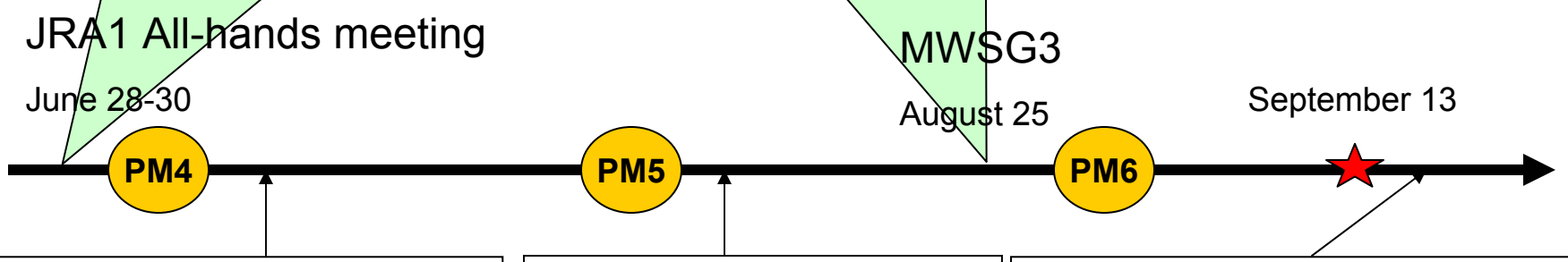
Enabling Grids for E-science in Europe

TR7: Software maintenance and development

PM5: **SOAP over HTTPS** 80%
PM6: **Delegation** 45%, **AuthZ framework** 70%, **Mutual AuthZ** 10%, **VOMS admin & parser** (ongoing)
PM7: **Message level security** 70%
PM9: **Resource access control** 10%, **Grid enhancements for OpenSSL** Started
PM11: **Site Proxy for GRID cluster** Started

-Productive meeting, kick-off for the s/w maintenance/development at JRA3.

- Global Security Architecture
- Security requirements
- Incident response capability



Task 1: Security requirement doc MJRA3.1 (PM3) completed

Task 3: Phase1 OGSA doc MJRA3.3 (PM4) completed

Task 4: DJRA3.1 Security Architecture doc (PM5) delivery date: Sept. 17

Recurrent tasks:
- JRA1 design team, integration, testing
- EUGridPMA, QAG
- Software maintenance and development

Task 5: Taxonomy document on Incident handling and Security operational procedures; definition of a common Grid incident format. (PM6+) In cooperation with JSG and OSG

Relationship between JRA3 and JRA1 work and deliverables

Enabling Grids for E-science in Europe

Requirements on gLite: collected and prioritized by MWSG

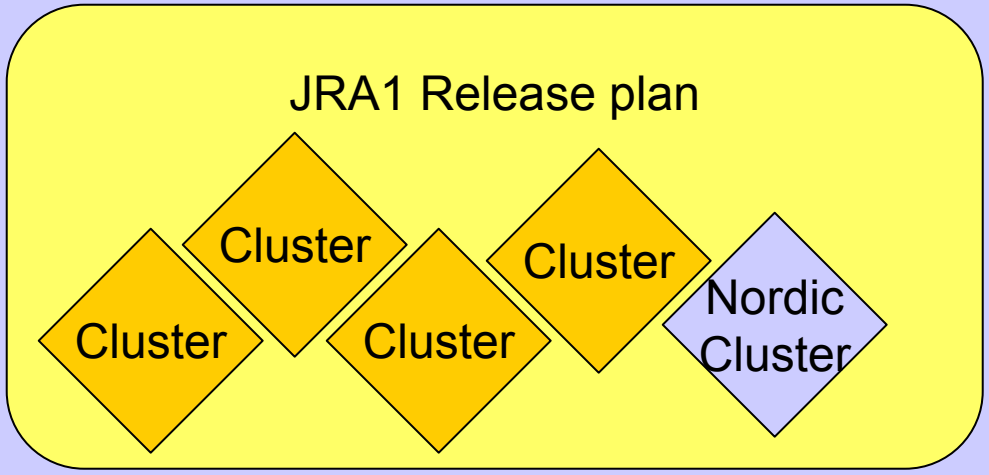
Architecture and design: Security architect and senior developers from JRA3 involved in the gLite architecture and design, from start.

DJRA1.1 gLite Architecture

DJRA1.2 gLite Design

DJRA3.1 gLite Security Architecture

Implementation:
Security modules needed in gLite are developed in the Nordic (JRA3) cluster.



Relationship between JRA3 and other activites

Enabling Grids for E-science in Europe

MWSG in collaboration with JSG ensures the horizontal function of JRA3 at this stage. Further developed the working channels to :

JRA1:

- Design Team (David Groep, and Olle Mulmo from JRA3)
- EMT (Åke Edlund from JRA3)
- MWSG (All in JRA3, cluster mgrs from JRA1)
- Cluster-by-cluster - Integration, testing, data mgmt, ... (one member per cluster from JRA3)

JRA2:

- QAG (Gerben Venekamp/Martijn Steenbakkers from JRA3)

SA1:

- MWSG (All in JRA3, members from the JSG from SA1)
- JSG (Joni Hakala, Åke Edlund from JRA3)

NA4:

- MWSG (All in JRA3, NA4 representing application-by-application)

OSG security:

- MWSG (Bob Cowles, Dane Skow)

Hiring Status & Manpower level

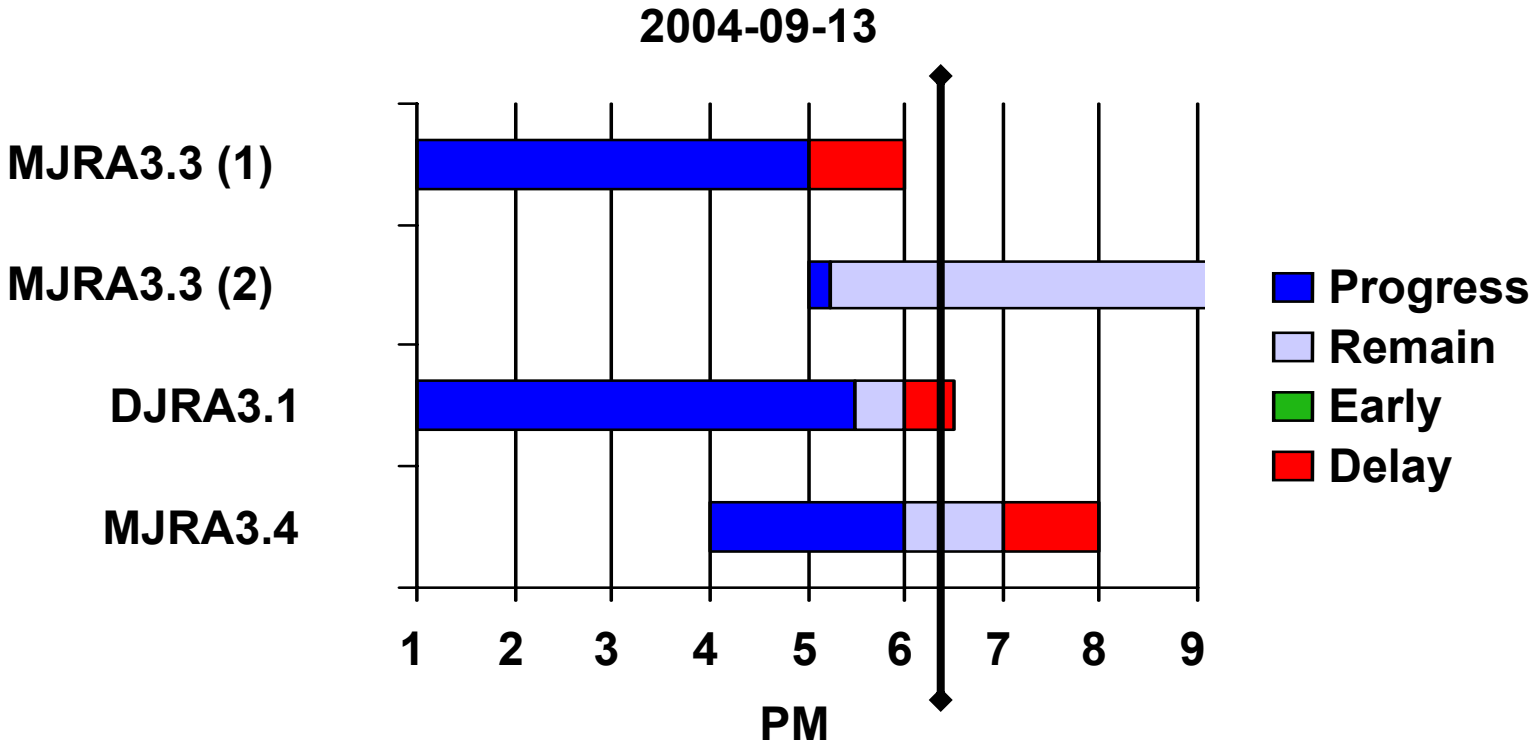
Enabling Grids for E-science in Europe

Partner	FTE[1]	MM	Assigned[2]	To Hire[2]	FTE from TA[2]	Deviation
UiB	2,0	24	2,0	0,0	2	0%
UvA	2,0	24	2	0,0	2	0%
FOM	2,0	24	2	0,0	2	0%
UH-HIP	2,0	24	2	0,0	2	0%
KTH	4,0	48	4	0,0	4	0%
Total effort	12,0	144	12,0	0,0	12	0%

Resource Plan indicator	
Hired or assignated up now	12,0
Total FTE from TA	12,0
Recruitment indicator	100%
Still to hire	0,0

1: People planned & assigned
2: Head count

State of deliverables and milestones for PM4-PM6



MJRA3.3 OGSA security reengineering recommendations

DJRA3.1 Global Security Architecture

MJRA3.4 Security operational procedures

Scope, objectives and status of M5/M6 deliverables

Enabling Grids for E-science in Europe

MJRA3.3

OGSA SEC service initial recommendations for reengineering

DJRA3.1

Global security architecture

MJRA3.4

Security operational procedures and incident handling, definition of a common Grid incident format

Enabling Grids for E-science in Europe

MJRA3.3

OGSA SEC service initial recommendations for reengineering

DJRA3.1

Global security architecture

MJRA3.4

Security operational procedures and incident handling, definition of a common Grid incident format

Scope, objectives and status of M5/M6 deliverables: MJRA3.3 - OGSA SEC service initial recommendations for reengineering (1/4)

Enabling Grids for E-science in Europe

Reason for the reformulation of this task:

Currently available security standards supporting the creation of security components for the Open Grid Services Architecture (OGSA) too scarce.

Due to the lack of standards against which to implement, JRA3 decided to focus first (PM4) on security for ordinary web services and postpone the OGSA specific activities to a later stage (PM9).

Advantages with the reformulation of the task:

- Implementation of modules can start at an earlier stage of the project,
- Early implementation allows us to join other EGEE activities' iterative software development processes and thus eases future integration of components,
- The lack of OGSA security standards is no longer an immediate obstacle, and,
- The experience acquired from the web services security work can be fed in into future OGSA security work: e.g. when implementing and contributing to standardisation efforts etc.

Scope, objectives and status of M5/M6 deliverables: MJRA3.3 - OGSA SEC service initial recommendations for reengineering (2/4)

Enabling Grids for E-science in Europe

Goal of this task:

Identify a set of security modules that can be implemented before the 2nd EGEE conference to address some of the most immediate EGEE security needs, namely those of JRA1.

The focus is to work on security modules that serve to improve the security of existing Web Services software components of EGEE middleware. As such, this document serves as input to the overall JRA3 release plan.

Longer term security objectives and modules that require more time to implement will only be identified and they serve as place holders to be elaborated on in future versions of this document.

Scope, objectives and status of M5/M6 deliverables: MJRA3.3 - OGSA SEC service initial recommendations for reengineering (3/4)

Enabling Grids for E-science in Europe

Phase 1 completed, see https://edms.cern.ch/document/488169/1.0

Phase1 (PM4)	**3.1.1**	Select and study standards relevant to OGSA security, test GTK 3.2 sec implementation
	3.1.2	Collect and categorize EGEE security requirements wrt first release of JRA1 modules
	3.1.3	Analyse requirements wrt first release of JRA1 modules
	3.1.4	Write first release of doc: OGSA security initial recommendations for reengineering
	3.1.5	Plan reengineering work based on feedback to recommendation doc from 3.1.4 (was 3.1.5)
Phase2 (PM9)	**3.1.6**	Start reengineering chosen modules according to set priorities (was 3.1.6)
	3.3.1	Collect and categorize EGEE security requirements wrt OGSA security
	3.3.2	Analyse requirements wrt OGSA sec & EGEE sec infra
	3.3.3	Write final release of doc: OGSA security initial recommendations for reengineering

Scope, objectives and status of M5/M6 deliverables: MJRA3.3 - OGSA SEC service initial recommendations for reengineering (4/4)

Enabling Grids for E-science in Europe

Conclusion at this stage:

The main conclusion is that **the standards and available tools are not mature enough to use**. Currently the only viable solution to do authentication and message security is to use transport layer security.

The delegation portType is the only actual WS level item chosen to be implemented. The development of message level security standards and tools has to be followed and checked for viability periodically.

When the standards and tools mature the recommendations in this document will need to be updated.

Scope, objectives and status of M5/M6 deliverables

Enabling Grids for E-science in Europe

MJRA3.3

OGSA SEC service initial recommendations for reengineering

DJRA3.1

Global security architecture

MJRA3.4

Security operational procedures and incident handling, definition of a common Grid incident format

Scope, objectives and status of M5/M6 deliverables

Enabling Grids for E-science in Europe

MJRA3.3

OGSA SEC service initial recommendations for reengineering

DJRA3.1

Global security architecture

MJRA3.4

Security operational procedures and incident handling, definition of a common Grid incident format

Scope, objectives and status of M5/M6 deliverables: DJRA3.1 - Global security architecture (1/5)

Enabling Grids for E-science in Europe

Where to find the document:

https://edms.cern.ch/document/487004/

Some of the requirements inputs to the document:

- JRA3: Gap analysis - reviewed at the first MWSG
- JRA1: gLite architecture document
- JRA3: User requirements collection
- NA4: Application requirements database

Next step:

Final release of the document: September 17.

Still missing: Use cases (We define a security architecture as *A set of features and services that tackles a set of security requirements and can handle a set of use cases*.)

Scope, objectives and status of M5/M6 deliverables: DJRA3.1 - Global security architecture (2/5)

Enabling Grids for E-science in Europe

Overview of the security architecture services.

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

Scope, objectives and status of M5/M6 deliverables: DJRA3.1 - Global security architecture (3/5)

Enabling Grids for E-science in Europe

Overview of the security architecture services.

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

Scope, objectives and status of M5/M6 deliverables: DJRA3.1 - Global security architecture (4/5)

Enabling Grids for E-science in Europe

Overview of the security architecture services.

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
Site proxy	Enables applications to communicate despite heterogenous and non-transparent network access	Mid-term

Scope, objectives and status of M5/M6 deliverables: DJRA3.1 - Global security architecture (5/5)

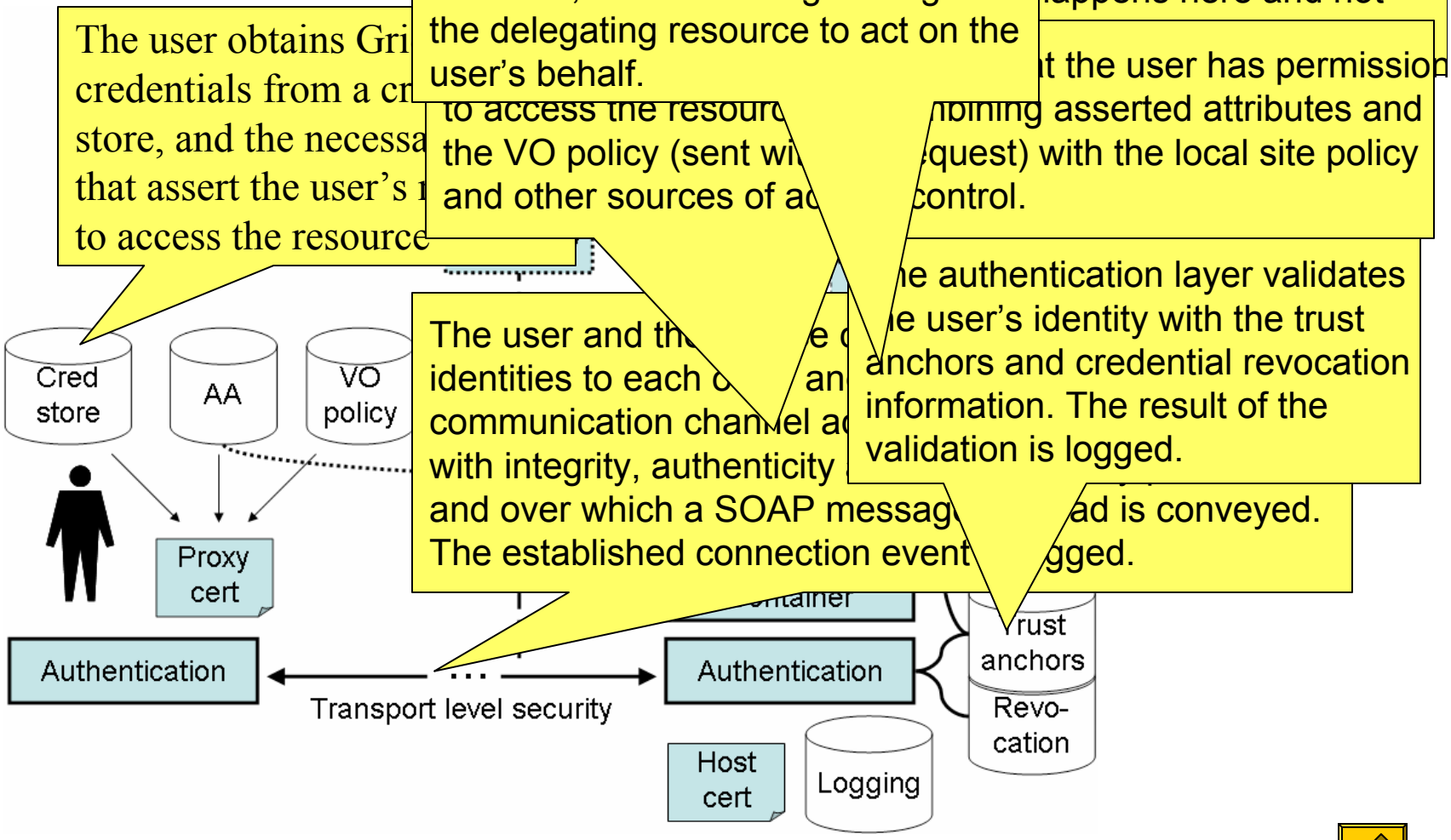
Enabling Grids for E-science in Europe

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	Site Proxy	Future

Scope, objectives and status of M5/M6 deliverables: DJRA3.1 - Global security architecture (

Overview on how the components in the security architecture interact



Scope, objectives and status of M5/M6 deliverables

Enabling Grids for E-science in Europe

MJRA3.3

OGSA SEC service initial recommendations for reengineering

DJRA3.1

Global security architecture

MJRA3.4

Security operational procedures and incident handling, definition of a common Grid incident format

Scope, objectives and status of M5/M6 deliverables

Enabling Grids for E-science in Europe

MJRA3.3

OGSA SEC service initial recommendations for reengineering

DJRA3.1

Global security architecture

MJRA3.4

Security operational procedures and incident handling, definition of a common Grid incident format

Scope, objectives and status of M5/M6 deliverables: MJRA3.4 Security operational procedures and incident handling, definition of a common Grid incident format.

Enabling Grids for E-science in Europe

This task is completed together with JSG and OSG

PM6:

- Inventory of security and incident handling procedures and requirements from GOC and ROCs (internal doc)
- Definition of characteristics for a common reporting format (public document)

PM7, Den Haag, 2nd EGEE Conf.:

- Draft of ”Joint OSG and EGEE incident policies and procedures”. Together with Bob Cowles, Ian Bird, and Dave Kelsey.

Risk analysis (incomplete)

Enabling Grids for E-science in Europe

Risk title	Description
Security Architecture	**Performance vs security**, E.g. Whether authentication can be turned into and run as an independent credential validation web service is subject to the performance constraint stated by JRA1 (200 ms/message).
Security Architecture	**Security not prioritized** : How this could evolve: Security requirements are not a central point in developing/solving security problems between different activities complicating the coordination of efforts. E.g. developers are not referring to Sec Reqs in developing security solutions
Requirement handling	Not making the proper **priorities**, meeting the application needs. Esp. regarding the biomed applications' needs.

Issues related to other activities

1. Not delivering security modules fast enough to JRA1. This is JRA3's problem to solve. Still an issue to JRA1.

2. Clarification regarding horizontal security work - responsibilities, mandates (MWSG catches most of these issues. Ongoing).

Highest priority steps to take between nowand the 2nd project conference in Den Haag

Enabling Grids for E-science in Europe

- To support JRA1 need of security software, re-engineering, development
- Finalize task 4, and 5 (task 1, 2, 3 (phase 1) already delivered).
- MWSG, to prioritize and handle requirements, next meeting October 15.
- Key Management for Biomed applications. Phase 1: scope, limitations and plan - might need to be speeded up.

Thank you!

Enabling Grids for E-science in Europe

http://egee-jra3.web.cern.ch/egee-jra3/index.html