Enabling Grids for
E-science in Europe

www.eu-egee.org

PEB All-Activity Meeting, June 18, 2004

JRA3 Security

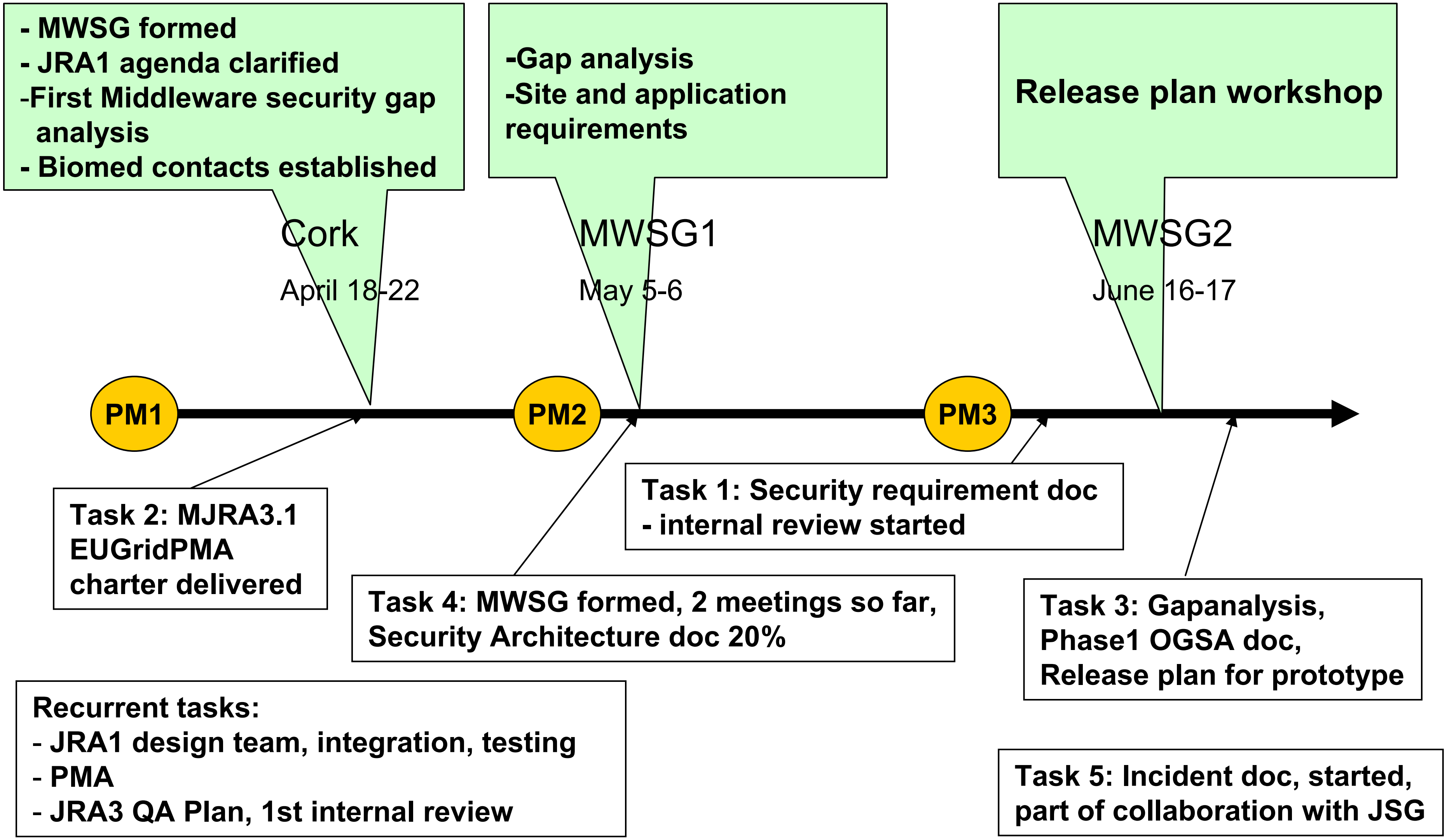
Åke Edlund
Security Head

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

Contents

- Summary of work accomplished since First EGEE Conference in Cork
- State of deliverables and milestones for M3 (as well as indication on deliverables and milestones for M4 and M5)
- State of Execution Plan
- Overview of current and planned WBSs
- Risk analysis
- Issues related to other activities
- Highest priority steps to take between no
  the 2nd project conference in Den Haag
- Planning for DJRA3.1:
  Global security architecture (document)

Summary of work accomplished since First EGEE Conference in Cork



- MWSG formed
- JRA1 agenda clarified
-First Middleware security gap analysis
- Biomed contacts established

-Gap analysis
-Site and application requirements

Release plan workshop

Task 2: MJRA3.1 EUGridPMA charter delivered

Task 4: MWSG formed, 2 meetings so far, Security Architecture doc 20%

Task 1: Security requirement doc
- internal review started

Task 3: Gapanalysis, Phase1 OGSA doc, Release plan for prototype

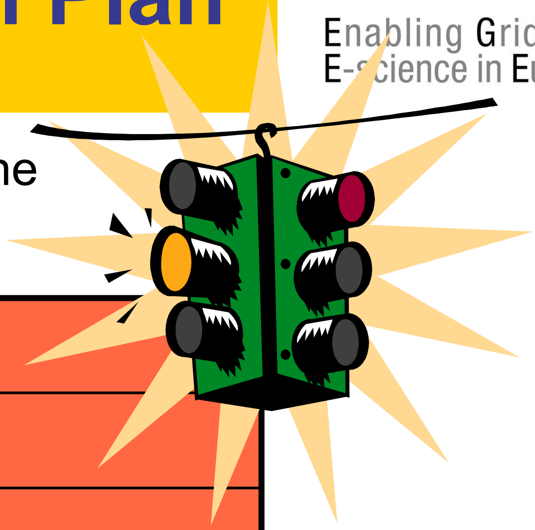
Recurrent tasks:
- JRA1 design team, integration, testing
- PMA
- JRA3 QA Plan, 1st internal review

Task 5: Incident doc, started, part of collaboration with JSG

State of deliverables and milestones

Project Month	Deliverables & Milestones	Item	Lead Partner	Status
M03	MJRA3.1	Completed user requirements survey defines effort redistribution over action lines.	KTH/PDC, FOM	80%
M03	MJRA3.2	Set-up of the PMA for European CAs and liaison with the corresponding extra European ones (document + standing committee)	FOM	Done
M04	MJRA3.3	OGSA SEC service initial recommendations for reengineering	UH-HIP	50%
M05	DJRA3.1	Global security architecture (document)	KTH	20%

State of Execution Plan



Execution plan v2.3: still need for updates, esp. when the release plan is set

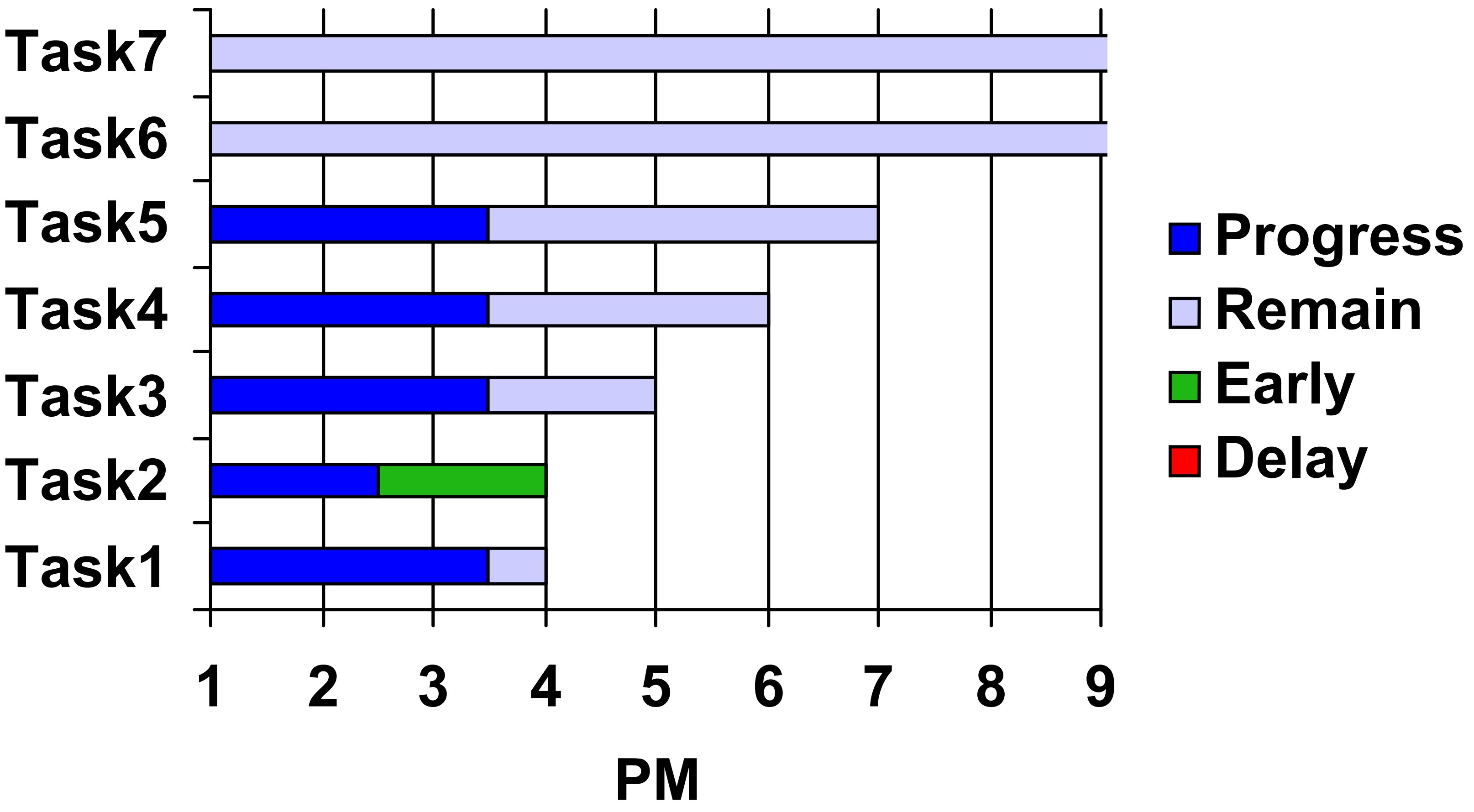
	TA planned effort	
	Resource Plan	
	MRP	
	WBS	
TasksDesc		
	GANTT	
		InitialRisks
Training Plan		

Overview of current and planned WBSs

Task 1	User requirements survey
Task 2	Setup of the PMA for European CAs
Task 3	OGSA security reengineering recommendations
Task 4	Global Security Architecture
Task 5	Security operational procedures
Task 6	Secure Credential Storage procedures
Task 7	Site access control architecture

Overview of current and planned WBSs

2004-06-18



Task 3 has been modified, to meet the this year’s prototype’s need

Enabling Grids for E-science in Europe

New

Previous version

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)
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

Task 3 has been modified

3.1.1	Select and study standards relevant to OGSA security, test GTK 3.2 sec implementation	Select standards for study. Group them based on if they are of relevance for current EGEE software, OGSA compatible EGEE software or future, namely WSRF related ones and focus on the two first groups.
3.1.2	Collect and categorize EGEE security requirements wrt first release of JRA1 modules	Identify requirements that are specific to JRA1 middleware security. Liaison with other activities, esp. JRA1, SA1, Arch. Team to have an as complete a set of requirements as possible. Note a bunch of novel requirements from TA: advance reservation, complex policy enforcement, establish configuration conventions.
3.1.3	Analyse requirements wrt first release of JRA1 modules	Analyse the requirements identified and evaluate each in terms of what the implications are when they are to be fulfilled within the context of JRA1 middleware. Evaluate what current EGEE sec components and third-party components can be migrated or used to create an OGSA security/Web Services security compatible solution, give initial estimate of effort.
3.1.4	Write first release of doc: OGSA security initial recommendations for reengineering	Write the milestone document MJRA3.3 based on requirements collection + analysis and feedback from us and other activities. Focus: plain web services security.
3.1.5	Plan reengineering work based on feedback to recommendation doc from 3.1.4 (was 3.1.5)	Plan and prioritize work on those EGEE sec components that are to have an OGSA sec enabled version. Take into consideration input from other activities.
3.1.6	Start reengineering chosen modules according to set priorities (was 3.1.6)	Based on the prioritization of 3.1.5, start the design of the chosen security modules. Before proceeding with implementation, circulate design for comments with the established liaison partners in order to nail down problems, inconsistencies etc

Execution plan - Tasks

- **Task 1: User requirements survey**
  - Liaise with European bodies for authentication and PKI
  - Identify user communities and contact people
  - Acquire background information on EDG security architecture
  - Collect and sort security requirements
  - Perform user survey
  - Identify authorization requirements
- **Task 2: Setup of the PMA for European CAs**
  - Liaise with European bodies for authentication and PKI
  - Write and adopt the EUGridPMA Charter
  - Operating and sustaining the EUGridPMA
- **Task 3: OGSA security reengineering recommendations**
  - Liaise with other activities of EGEE such as the Architecture
  - Requirements collection and categorization
  - AuthZ and AuthN infrastructure
  - GGF connection (OASIS+WS)

Execution plan - Tasks (cont.)

- **Task 4: Global Security Architecture**
  - Security Architecture workshop
  - Participate in work on Global Architecture
  - Security Architecture document
- **Task 5: Security operational procedures**
  - Inventory of incident reporting practices and report formats
  - Definition of a common incident report format
- **Task 6: Secure Credential Storage procedures**
- **Task 7: Site access control architecture**
  - Prototyping and refactoring of site access tools for architecture development
  - Describe site access control architecture in documentation

Overview of current and planned WBSs

T1	User requirements survey	Artifact	Month Start	Month End	Estimated effort	Estimated-Allocated
1.1	Achieve MJRA3.1		M01	M03	**8**	**8**
1.1.1	Identify user communities and contact people		0	0	0,2	Collaboration with JRA1, SA1, NA4, Architecture Team
1.1.2	Acquire background information about EDG security architecture		0	1	1,75	
1.1.3	Provide a document that collects security requirements	First draft of Milestone MJRA3.1	1	2	2,5	
1.1.4	Collect and categorize security requirements	internal document	1	2	1	
1.1.5	Review and update the document	Final draft of Milestone MJRA3.1	3	3	1,75	
1.1.6	Perform user survey	User survey	9	11	0	Gather new user requirements after the first project review (month 9)
1.2.0	Task delivery					Subtasks with explicit dates for internal and external reviews
1.2.1	Ready for internal review					date: 2004-05-28
1.2.2	Task finalized					date: 2004-06-25

Overview of current and planned WBSs

Enabling Grids for E-science in Europe

T2	European PMA set-up	Artifact	Month Start	Month End	Estimated effort	Estimated-Allocated
2.1	Achieve MJRA3.2		M01	M03	**0,5**	**0,5**
2.1.1	Establish connection with European authentication and PKI bodies.	joint statement	0	0	0,5	In particular TERENA and eIRG
2.1.2	Write EUGridPMA charter.	charter document	0	0	0	
2.2.0	Task delivery					Subtasks with explicit dates for internal and external reviews
2.2.1	Ready for internal review					date: 2004-04
2.2.2	Task finalized					date: 2004-05

Overview of current and planned WBSs

T3	OGSA security reengineering recommendations	Artifact	Month Start	Month End	Estimated effort	Estimated-Allocated
3.1	Achieve MJRA3.3		M01	M04	**7,6**	**7,6**
3.1.1	Select and study standards relevant to OGSA security, test GTK 3.2 sec implementation		0	0	0,6	Partially a recurrent task
3.1.2	Collect and categorize EGEE security requirements wrt first release of JRA1 modules		1	1	1	
3.1.3	Analyse requirements wrt first release of JRA1 modules	internal document	2	4	3,5	Circulate within JRA3, JRA1,SA1, A team through the MWSG
3.1.4	Write first release of doc: OGSA security initial recommendations for reengineering	First release of MJRA3.3 document	3	4	2,5	Circulate within JRA3, JRA1,SA1, A team through the MWSG
3.1.5	Plan reengineering work based on feedback to recommendation doc from 3.1.4 (was 3.1.5)					
3.1.6	Start reengineering chosen modules according to set priorities (was 3.1.6)					
3.2.0	Task delivery					Subtasks with explicit dates for internal and external reviews
3.2.1	Ready for internal review					date: 2004-06-23
3.2.2	Task finalized					date: 2004-07-14
3.3.1	Collect and categorize EGEE security requirements wrt OGSA security		1	7	1	Overlap with MJRA3.1, see task 1.1.4
3.3.2	Analyse requirements wrt OGSA sec & EGEE sec infra	internal document	4	9	3,5	Circulate within JRA3, JRA1,SA1, A team through the MWSG, and with GGF
3.3.3	Write final release of doc: OGSA security initial recommendations for reengineering	Final release of MJRA3.3 document	8	9	2,5	Circulate within JRA3, JRA1,SA1, A team through the MWSG, and with GGF
3.4.1	Task delivery					Subtasks with explicit dates for internal and external reviews
3.4.2	Ready for internal review					date: 2004-12-31
3.4.3	Task finalized					date: 2004-12-31

Overview of current and planned WBSs

T4	Global security architecture	Artifact	Month Start	Month End	Estimated effort	Estimated-Allocated
4.1	Achieve DJRA3.1		M01	M05	**7,5**	**7,5**
4.1.1	Organize workshop	workshop	1	2	2	
4.1.2	First release of Global Security Architecture document	public document	1	5	5,5	
4.2.0	Task delivery					Subtasks with explicit dates for internal and external reviews
4.2.1	Ready for internal review					date: 2004-08-27
4.2.2	Task finalized					date: 2004-09-17

Overview of current and planned WBSs

Enabling Grids for E-science in Europe

T5	Security operational procedures and incident handling	Artifact	Month Start	Month End	Estimated effort	Estimated-Allocated
5.1	Achieve MJRA3.4		M01	M06	**4**	**4**
5.1.1	inventory of security and incident handling procedures and requirements from GOC and ROCs	internal document	1	4	2	GOC?
5.1.2	definition of characteristics for a common reporting format	public document	3	4	2	
5.2.0	Task delivery					Subtasks with explicit dates for internal and external reviews
5.2.1	Ready for internal review					date: 2004-mm-dd?
5.2.2	Task finalized					date: 2004-mm-dd + 21 days?

Overview of current and planned WBSs

T6	Secure Credential Storage procedures	Artifact	Month Start	Month End	Estimated effort	Estimated-Allocated
6.1	Achieve MJRA3.5		M01	M09	**8**	**8**
6.1.1	Evaluate online credential repositories		3	5	1,5	
6.1.2	Evaluate portable credential repositories				3	USB, smartcard, OpenLab?
6.1.3	Evalutate integration with organizational authentication methods		3	5	1,5	
6.1.4	Report				2	
6.2.0	Task delivery					Subtasks with explicit dates for internal and external reviews
6.2.1	Ready for internal review					date: 2004-11-15
6.2.2	Task finalized					date: 2004-12-10

Overview of current and planned WBSs

Enabling Grids for
E-science in Europe

T7	Resource access control architecture	Artifact	Month Start	Month End	Estimated effort	Estimated-Allocated
7.1	Achieve DJRA3.2		M01	M09	**7**	**7**
7.1.1	Prototyping and refactoring of site access tools for architecture development	software	1	9	5	
7.1.1.1	Ready for internal review					date: 2004-11-15
7.1.1.2	Task finalized					date: 2004-12-15
7.1.2	Describe site access control architecture in documentation	Public document	6	8	2	
7.1.2.1	Ready for internal review					date: 2004-10-15
7.1.2.2	Task finalized					date: 2004-11-15

Overview of current and planned WBSs

Enabling Grids for E-science in Europe

TR	Recurrent tasks	Artifact	Month Start	Month End	Estimated effort	Estimated-Allocated
TR1	JRA3 management		M01	M09	9	**9**
TR2	Security Group		M01	M09	11,25	**0**
TR3	Misc overhead (admin, conference)		M01	M06	4,5	**4,5**
TR3.1	First EGGE conf		M01	M01	4,5	**4,5**
TR3.2	Second EGGE conf		M07	M07	4,5	**4,5**
TR4	Global architecture discussions		M01	M09	3,6	Continuous and ongoing discussions will take place online in mailing lists and in the regularly scheduled Architecture and Security group meetings and phone conferences.
TR5	Operate the EUGridPMA		M01	M09	1,6	
TR6	Software maintenance and development old		M01	M09	4,5	LCAS, LCMAPS
TR6.0	External development effort liason		M01	M09	1,125	VOMS
TR7	Software maintenance and development new		M01	M09	0	
TR7.1	Plan reengineering work based on feedback to recommendation doc from 3.1.4 (was 3.1.5)		5	6	2	Post PM6?
TR7.2	Start reengineering chosen modules according to set priorities (was 3.1.6)		7	9	4	Participation & duration to be discussed

Risk analysis

Risk classification (M=Management/Organisation, P=Product, S= Service, T=technical)

Risk level (1 to 4: 1=low, 2=medium, 3=high, 4=critical)

Initial risk analysis - before April 1st

Enabling Grids for E-science in Europe

Risk title	Class	Level	Description	Status today
Part-time project personnel	M	3	Too many part-time people currently listed. Sort out what this means in practice	Still valid
Security Architecture	T		Dependent on overall architecture, which may be unclear at the start of the project (or rapidly change)	Better, but still valid.
Security Architecture	M		Inadequate support/response time from non-JRA3 members	Not valid at this stage
Security Architecture	M		Cross-activity Architecture and Security groups not quickly formed or consists of the "wrong" members	MWSG has the right set of members
Security Architecture	M/T		EGEE arch initially non-OGSA delaying reqs collection/analysis wrt OGSA sec	Happened already.
Security Architecture	T	1	Consensus on the concepts defined within GGF	MWSG and JRA3 architect channel to GGF
Interaction with other activity	M	3	We need to create as soon as possible a network of contact people within other activities, in particular JRA1, SA1, NA4 and Architecture Team	MWSG up and running.
User survey	P	2	2 concerns, to be addressed.	Still valid

Risk analysis - new titles

Risk title	Class	Level	Description
Prototype becoming final product	T	1	Short time solutions to be able to deliver prototype, remains in the final product.
Requirement handling	P	1	Not making the proper priorities, meeting the application needs. Esp. regarding the biomed applications' needs.

Issues related to other activities

No Issues. MWSG ensures the horizontal function of JRA3 at this stage. Established 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, datamgmt, ... (one member per cluster from JRA3)

JRA2:

- QAG (Martijn Steenbakkers from JRA3)

SA1:

- MWSG (All in JRA3, members from the Joint Security Group from SA1)

NA4:

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

OSG security:

- MWSG (Bob Cowles, Dane Skow)

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

- Release plan: to support JRA1 need of security software, re-engineering, development
- Key Management for Biomed applications. Phase 1: scope, limitations and plan
- Finalize task 1, 3, and 4 (task 2 already delivered)
- MWSG, to catch, prioritize and handle requirements, next meeting August 25.

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

Enabling Grids for E-science in Europe

	Java	C/C++	Python	Overall responsible	Deliverable date
SOAP over HTTPS	UH-HIP	UH-HIP		UH-HIP Joni Hahkala	PM5
Message level security	KTH			KTH Thomas Sandholm	PM7
Delegation	KTH			FOM David Groep	PM6
AuthZ framework	KTH			UvA Martijn Steenbakkers	PM6
Workload Management, "LCAS"	FOM			UvA Martijn Steenbakkers	PM7
Mutual AuthZ				UiB Jeremy Cook	PM6
VOMS GUI	UH-HIP			UH-HIP Joni Hahkala	PM6
Key Management for Biomed applications				KTH Olle Mulmo	Phase 1, PM8

Planning for DJRA3.1: Global security architecture (document)

Task owner: Olle Mulmo

June:	Release of internal DRAFT, 2004-06-25 - *Ongoing, on time*
July:	JRA3 responds to DRAFT - *David Groep, responsible*
August:	Ready for internal review, 2004-08-27
September:	Task finalized, 2004-09-17