EGEE

JRA3 EXECUTION PLAN
FOR THE FIRST 9 MONTHS

Document identifier:	**JRA3-ExecPlan-v1.98**
Date:	**2004-03-16**
Activity:	**JRA3: Security**
Document status:	**DRAFT**
Document link:	**https://edms.cern.ch/document/xxxxxx**

Abstract: This document describes the execution plan for **JRA3** Security Activity for the first nine months of the EGEE project.

Document Log

Issue	Date	Comment	Author
0-0	2003-12-16	First draft	F. Hedman
0-1	2004-01-08	Second draft (new format)	F. Hedman
0-2	2004-01-15	Added some names	F. Hedman
0-3	2004-02-23	Clean-up	F. Hedman
0-4	2004-02-24	Added text from others	F. Hedman
0-5	2004-02-25	Added text from Olle and Joni.	F. Hedman
0-6	2004-02-27	Merge text from others	F. Hedman
0-7	2004-03-03	Yet another merge	F: HedmanS

Document Change Record

Issue	Item	Reason for Change

CONTENT

1. INTRODUCTION

1.1. PURPOSE

This document describes the execution plan for JRA3 Security Activity for the first nine months.

The main items described are the following:

- JRA3 overview
- Recall the scope of the work (from TA)
- Table of milestones and EU deliverables
- Organisation, role & responsibility (from TA + refinements)
- JRA3 Management monitoring
- Product Breakdown Structure (PBS)
- Work Breakdown Structure (WBS)
- Staffing and resource plan
- Training
- Initial risk assessment
- Initial quality target indicators
- Major links with other activities
- Timeline with GANTT chart
- Technical Main Processes
- Tools & Methodology

1.2. APPLICATION AREA

The execution plan refines JRA3 activities defined in the technical annex. The work on the execution plan may lead to minor changes to the Technical Annex.

1.3. REFERENCES

[R1] https://edms.cern.ch/document/400278	Technical Annex
[R2] https://edms.cern.ch/document/422807	Execution Plan Guidelines

1.4. DOCUMENT EVOLUTION PROCEDURE

This document will be updated incrementally as the JRA3 Activity knowledge increases.

Comments should be sent to the author(s).

1.5. TERMINOLOGY

Glossary

JRA3	EGEE Security activity
TA	Technical Annex
PBS	Product breakdown structure
WBS	Work breakdown structure
MRP	Monthly Resource Plan

Definitions

2. JRA3 OVERVIEW

EGEE will construct an integrated and scalable infrastructure that will facilitate various types of applications and access patterns, ranging from single transactions to long-lived batch jobs. Security must be included in the architecture *from the start*, and not inserted

at a later point. Moreover, security considerations must be present in all activities. The JRA3 security group will define a Security Framework and Architecture and a set of high-level policies that will act as guidance to the other activities. This will ensure consistency and provides one of the more visible value-adding services of the Grid: transparent security and single sign-on.
The security architecture will be based on requirements from both Grid users and suppliers. JRA3 will will assist in defining and validating the EGEE security architecture in line with these requirements. It is perceived that a number of security related tasks are especially challenging when implemented to work across national boundaries and over a wide-ranging geographic area. Many of those tasks need immediate attention, although none are blocking the initial deployment of a Grid at open scientific organisations. To date, the following areas have been identified as being on the critical path for large-scale deployment:

- Basic Security Policy and Incident Response;
- CA Trust Establishment and Policy Management;
- VO Definition, Rights Delegation, and Scalability;
- OGSA Web Services Security and site service access, control and auditing;
- Site Usage Control and Budgeting;
- Secure Credential Storage.

2.1. SCOPE OF THE WORK

The tasks of this activity have one common goal: enabling the deployment of production-quality Grid that includes resources and applications that are security-conscious and handle sensitive information. The execution plan detailed below covers only the initial period of 9 months:

- **Project start:** The detailed planning of the management structures and functions described in this document will allow the project to become quickly established. To ensure a quick start-up phase, we intend to have all staffing in place by the start of the project. We will also make sure that our initial plans are well advanced at the start of the project.
- **PM3:** the first two milestones are at the end of project month 3: first, a completed users requirements survey will help to further refine the distribution of effort over action lines; and second, the set up of the Policy Management Authority (PMA) for European CAs. The PMA will also liaison with non-European CAs as necessary.
- **PM6:** at the end of project month 6, two more milestones have been met and the first deliverable is completed. The first milestone is a manual with initial recommendations for OGSA SEC services reengineering. The second is a document for security operational procedures and incident handling and a common Grid incident format. The deliverable is the initial Global security architecture document.

2.2. TABLE OF JRA3 MILESTONES AND EU DELIVERABLES

3. ORGANISATION

The purpose of the JRA3 activity is to "propose, implement and monitor the project's security architecture." The overall software development process described by JRA1 is also adopted by JRA3 (see Figure 1). The security head leads the whole activity and is a member of the PEB as well as the architecture team. In the other clusters of JRA1 there is a role dedicated to "security" which parallels the arrangement with a dedicated "unit tester" role. This is called the "Security Group". The security head animates this group; thus the security head works horizontally among the other JRA activities, while the cluster manager works more vertically within JRA3.

The security group will hold weekly conference calls at least twice a week and also meet 2-3 times per year. ### describe security group here ###

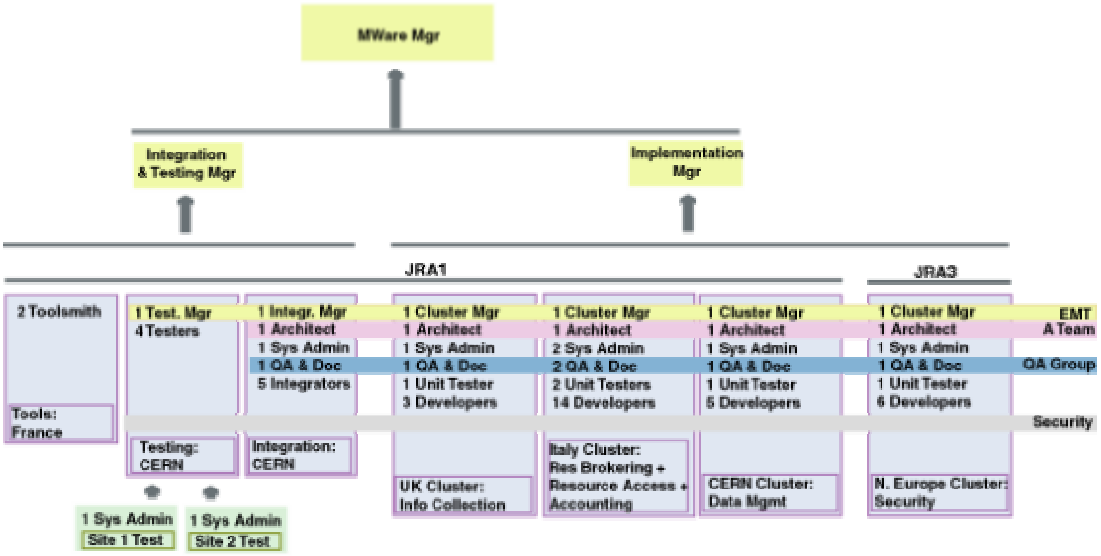

Figure 1: JRA3 relation to JRA1

3.1. IMPLEMENTATION

Table A *Manpower and geographical focal points for security activities*

Security Head	Fredrik Hedman, Stockholm

Software Development Cycle Team	4 software engineers:	
	Cluster Manager and Architecture	Olle Mulmo, Stockholm
	Sys Admin	1 person, Bergen
	QA and doc	Martijn Steenbakkers, Amsterdam
	Unit Tester	Joni Hakhala, UH-HIP
Security Architecture and Design Team	7 software engineers:	
	Basic Security Policy and Incident Response; CA Trust Establishment and Policy Management;	1 person, Amsterdam
	VO Definition, Rights Delegation, and Scalability	2 persons, Amsterdam
	OGSA Web services security and site service access, control and auditing	1 person, Stockholm Mika Silander, UH-HIP
	Site Usage Control and Budgeting; Secure Credential Storage.	2 persons, Stockholm and Bergen

3.2. INTEGRATION AND TESTING

3.3. MANAGEMENT

3.4. ARCHITECTURE TEAM

4. ACTIVITY MANAGEMENT MONITORING

4.1. PRODUCT BREAKDOWN STRUCTURE

The Product Breakdown Structure (PBS) serves as a logical decomposition of the system in order to identify smaller and smaller subsets until the lowest level, which could be new component, external software or material.
The PBS refers only to the products not services.

Relevant for JRA3?

4.2. TA EFFORT ESTIMATE

The effort expressed in FTE in the TA, are converted into Person month (PM). One FTE=24PM for the duration of the project. The distribution of the resources between the first and the second year of the project is added. Total effort=Funded+Unfunded.

4.3. WORK BREAKDOWN STRUCTURE FOR THE FIRST NINE MONTHS

As more details has been added
to the WBS, the table has become rather large. For full details see the MRP and WBS tables jra3-tables-1.98.xls.

4.4. STAFFING AND RESOURCE PLAN FOR THE FIRST NINE MONTHS

Collaborator name	Partner	Function	Available from Month	FTE	F | UF	Total PM
Cook Jeremy	UiB		1	0,5	F	*6*
NN1 (select)	UiB		1	0,5	F	*6*
NN2(hire)	UiB		1	1	UF	*12*
Demchenko Yuri	UvA		1	0,5	UF	*6*
Gommans Leon	UvA		1	0,2	UF	*2,4*
Steenbakkers Martijn	UvA		1	1	F	*12*
van Oudenaarde Bas	UvA		1	0,3	UF	3,6
Groep David	FOM		1	0,6		*7,2*
Koeroo Oscar	FOM		1	1		*12*
Venekamp Gerben	FOM		1	0,4		*4,8*
Hahkala Joni	UH-HIP		1	1	UF	*12*
Silander Mika	UH-HIP		1	1	F	*12*
Ahsant Mehran	KTH		1	0,25	UF	3
Danielsson Johan	KTH		1	0,5	UF	6
Hedman Fredrik	KTH	Security Head	1	1	F	12
Mulmo Olle	KTH	Architecture	1	1	UF	12
Sandholm Thomas	KTH		1	0,25	UF	3
Volpato Gian-Luca	KTH		1	1	F	12
Total effort				12		144
Total from the TA				12		144
Deviation				0		0

4.5. TRAINING PLAN

This section will present the training planned for the member of each activity.

No training needs identified yet.

4.6. INITIAL RISKS ASSESSMENT

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

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

Risk title	Class	Level	Description	Actions, responsibilit deadline
Part-time projet personnel	M	3	Too many part-time people currently listed. Sort out what this means in practice	04-03-31
Security Architecture	T		Dependent on overall architecture, which may be unclear at the start of th project (or rapidly change)	
Security Architecture	M		Inadequate support/response time from non-JRA3 members	
Security Architecture	M		Cross-activity Architecture and Security groups not quickly formed or cons of the "wrong" members	
Security Architecture	M/T		EGEE arch initially non-OGSA delaying reqs collection/analysis OGSA sec	

4.7. INITIAL QUALITY TARGET INDICATORS

To be completed later.

4.8. TIMELINE WITH GANTT CHART

To be completed later.

5. TECHNICAL PROCESSES

5.1. BACKGROUND AND COMMENT

The task descriptions of each task has been moved to the JRA3 spreadshhet tables. The descriptions below will be pruned once the tables have stabilized.

5.2. TASK 1: USER REQUIREMENTS SURVEY

Scope: MJRA3.1
Task: Identify user communities and contact people
Artifact: List of contact people within other activities
Effort:
Description: Collaboration and interaction with other activities is required in order to share and exchange as much information as possible. The TA indicates High Energy Physics and Biology/Health as the pilot application groups. User communities deal mostly with activity NA4 (Application Identification and Support) and SA1 (European Grid Support, Operation and Management). Identifying contact people within these activities, as well as with JRA1 and the Architecture Team, is required at the very beginning of the project.

Scope: MJRA3.1
Task: Acquire background information on EDG security architecture
Artifact:
Effort:
Description: The EDG Security Coordination Group prepared a set of documents that describe the security architecture and its implementation within EDG. Reading and understanding these documents is a starting point to create a solid background of information. The most relevant documents are deliverable D7.5, D7.6 and D7.7.

Scope: MJRA3.1
Task: Collect and sort security requirements
Artifact: Security requirements document
Effort:
Description: The identification of security requirements starts with collecting existing documents produced by the user communities within EDG, LCG and other projects.

From these documents we extract all security-related issues and sort them into homogenous groups, like authentication, authorization, policy enforcement, privacy (storage and transfer), integrity, logging, accountability, trace-ability, etc. Each requirement is described according to a template structure that illustrates the category, the middleware affected, the priority level, the degree of fulfillment in the present release of EDG/LCG software.

Each requirement is assigned a priority level; keep in mind we may not be able to satisfy/implement all requirements in the first EGEE software release.

Once the document is ready in its first draft it is circulated within JRA3 to receive feedback and comments. In a similar way, the draft is submitted to JRA1, SA1 and NA4 to receive feedback and comments.

The document is updated in order to integrate the comments and feedback.

Final version is delivered.

Scope: MJRA3.1
Task: Perform user survey
Artifact: Updated security requirements document
Effort:
Description: The requirements identified at the beginning of the project may be updated according to the assessment of the user communities. After the first project review (scheduled for month 9) it may be fruitful to perform a short user survey.

The survey is published on the web; responses are collected and analysed.

The security requirements document is updated in order to integrate the results of the survey.

```
  According to the Technical Annex the pilot application
groups are High Energy
  Physics and Biology/Health.
  Starting from the list of documents I sent some week ago I
would like to get
  some help from UiB and organize the work in the following
way:
  - PDC and UiB acquire initial background information about
security in EDG,
  by reading D7.5, D7.6, D7.7
  - PDC prepares a template document where requirements are
collected, sorted
  and given a priority
  - PDC analyzes HEP documents D8.1, D8.4 and fills the
template
  - UiB analyzes Bio documents D10.1, D10.2, D10.4 and fills
the template
  - PDC collects the requirements and writes a first
document draft
  - UiB analyzes Earth Observation documents D9.1, D9.4 (+
Technical Note),
  D9.5 and fills the template
  - PDC adds requirements from EO
  - PDC submits first draft to JRA3

Scope: MJRA3.1
Task:  Identify authorization requirements.
Description: Considering the overall set of security
requirements, describe where authorization applies in
various middleware area's according to the AuthZ framework
developed in GGF
```

5.3. TASK 2: SETUP OF THE PMA FOR EUROPEAN CAS

It is important that a single common trust domain for Grid authentication is Europe is established. The Technical Annex describes a "policy management authority" that is to operate in the EGEE context, but it is most beneficial to the European researchers if this trust domain extends to other areas and projects as well. In particular two other initiatives need to be considered to encompass the European *e*-Infrastructure: the sister project DEISA and the TERENA Academic CA Repository (TACAR) that includes the national roots of trust organized by the NRENs and academia also for non-Grid purposes.
This results in two incidental and one continuous task.

5.3.1. Task 2.1.1: Liase with European bodies for authentication and PKI

Artifacts: Joint Statement of the PMA and TERENA, endorsement by the eIRG
Start: PM –3 End: PM 1

This task in particular focusses on the TERENA TACAR organisation and the *e*-Infrastructure Reflection Group. Between the Grid Authentication PMA and TERENA a joint statement must clarify the interrelationship and collaboration.
Grid authentication uses techniques (like PKI) that could have wider applicability. In particular, PKIs have been deployed at the national scale by many NRENs and in some cases national governments. For the academic community, the TERENA task force on authentication and authorisation (TF-AACE) has recommended the establishment of an Academic CA Repository (TACAR).
The EUGridPMA group can leverage the work by TERENA in this area of mediating certified roots of trust for the EGEE Grid CAs. Links with the TF-AACE group and the TACAR coordinators (TERENA project officers) should be established and a mutual understanding reached. Moreover, it would be beneficial for all researchers in the European Research and Innovation Area to avail over a single common identity providers for Grid Authentication. This objective may be reached by building a common trust domain between EGEE, SEE-GRID and DEISA for Grid authentication for e-Science. Endorsement of such a development by a relevant European Community body in the e-Infrastructure area will be beneficial in reaching this common trust domain.

5.3.2. Task 2.1.3: Write and adopt the EUGridPMA Charter

Artefacts: An adopted Charter document for the EUGridPMA during a startup meeting in PM1
Start: PM-2 End: PM1
The European Grid PMA for authentication for e-Science needs a group structure and a charter for continued operation. With the Increase in community size, and extension of the scope with new countries in Europe and beyond, a more formal structure for the group's operation is required. The group will be managing its own charter, and the objective for

MJRA3.2 is a consensus agreement by the group on this charter in a plenary meeting on PM0.
Within the charter's mandate, the group will subsequently establish the baseline document on which the PMA operations are based (minimum requirements for CP/CPSs and the peer-review criteria). This document will be based on the Minimum Requirements v2 document as amended by the minutes of the EDG CACG since.

5.3.3. Operating and sustaining the EUGridPMA

Artefacts: Periodic meetings and continued existence of the trust domain as demonstrated by updated guideline documents
Start: PM1 End: PM24

The EUGridPMA is an on-going activity that will foster inter-organisational trust in e-Science through a Grid AuthN PKI. New CAs will be accredited, and documents updated. Periodic meetings (3-4 per year) are foreseen for management of the EUGridPMA.

5.4. TASK 3: OGSA SECURITY REENGINEERING RECOMMENDATIONS

```
As EGEE middleware security is likely to use many of EDG's
security
components and the problem field and requirements are
similar to those
of EDG, general security requirements and design criteria
and
constraints can be taken from the EDG Security Coordination
Group's
Deliverables D7.5, D7.6 and D7.7.
```

As EGEE middleware security is likely to use many of EDG's security components and the problem field and requirements are similar to those of EDG, general security requirements and design criteria and constraints can be taken from the EDG Security Coordination Group's Deliverables D7.5, D7.6 and D7.7.

```
Standards relevant to OGSA security reengineering
```

There is a great number of standards, both established and emerging related to OGSA security, e.g. XACML, SAML, X.509, XML-Encryption, XML-Signature, WS-SecureConversation, WS-Policy, WS-Trust, WS-Security, WS-Routing etc. Albeit we know many of these to varying degree of detail, selecting the most important ones for closer scrutiny and studying them is a prerequisite for working with OGSA Security. This will probably convert into a continuing activity for the whole duration of EGEE and so will the following of efforts of a number of standardisation bodies e.g. OASIS, GGF etc.

The recently released GTK 3.2 from Globus needs to be tried out to get familiar with the nitty-gritty details of its OGSA SEC implementation. This serves as background for evaluating the requirements collected. See task TJRA3.1.1.

5.4.1. Liaisoning

Liaisoning with other activities of EGEE such as the Architecture Team, JRA1, JRA4 and SA1, is important to make sure that the reengineering recommendations are backward compatible with existing middleware. This way we provide for a smooth transition towards an OGSI/WSRF based architecture.

5.4.2. Requirements collection and categorization

The requirements collected for MJRA3.1 are applicable as is for OGSA security work, i.e. the OGSA security reengineering efforts all aim at fulfilling the same identified requirements but within an OGSA framework. The evaluation of these requirements with respect to the OGSA security architecture will form the basis of the recommendations for reengineering.

The first step is to take as input the overall security requirements described in EDG deliverables D7.5, D7.6 and D7.7 and the categorisation in MJRA3.1. All requirements need to be evaluated in terms

```
 of the OGSA SEC architecture, e.g. apart from a
requirement's generic
 security implications does this requirement have any
characteristic
 why it must be treated differently when it is to be
fulfilled by an
 OGSA compliant security architecture? These and the
OGSA security requirements identified as specific to
OGSA are collected to an
 internal document to be later on analysed in task
TJRA3.1.3. See task TJRA3.1.2.

Requirements analysis with respect to OGSA security
and existing EGEE security infrastructure
```

Based on the requirements collection and categorization and in order to ease the migration from a non-OGSA architecture to an OGSI/WSRF based architecture we should attempt to maintain backward compatibility. This in turn translates into trying to keep existing security components of EGEE interoperable with the ones that are/will be OGSA sec enabled. In practise this includes components such as VOMS, LCAS, LCMAPS, edg-java-authN/authZ etc and issues like unifying current authN/authZ infrastructure for both hosted (Java) and native (Linux/Solaris/...) environments. This allows for a single implementation for authN/authZ, that can evolve together with the WS-* standards, and a thin interface (setuid root) to actually run "legacy" (i.e. UNIX-style) programs from a java environment.

To this end, the features of each should be documented to the extent that we can a) maintain interoperability, b) create an OGSA sec enabled version of each of them as identified in the requirements analysis phase. The features of interest are as always authentication, authorization, policy enforcement and auditing (goals described in Technical Annex). Overall, emphasis should be given to identifying those features of existing

components that need adaptation/re-engineering to fit into the OGSI/WSRF framework. Third-party components that can be used for implementing missing functionality should be identified, e.g. Permis for RBAC systems.

Building on the document from task TJRA3.1.2. an analysis of the security
requirements relevant to OGSA security work can be conducted. This work
is to provide a document that analyses each requirement with respect to the following characteristics and the current EGEE middleware setup:

-is there an OGSA SEC compatible implementation fulfilling this requirement fully or
partially.

-if no OGSA SEC compatible implementation is available, are there others
fulfilling this requirement fully or partially and thus are candidates
for migration.

-if none of the above is applicable, what are the other options for creating
a component fulfilling the requirement, e.g. by using third-party modules or
writing everything from scratch.

-are there backward compatibility issues? if yes, can these be solved by
deploying both a non-OGSA SEC compliant and an OGSA SEC compliant
software module?

In addition, there are three requests in the Technical Annex of more novel and until now either partially or completely unsupported security functionality; advance reservation of resources, complex policy enforcement and accounting. The security implications of all these should be analysed. Liaisoning with JRA4 is foreseen as it is also evaluating the implications of advance reservation.

The analysis should state for all requirements the required steps
that need to be taken to fulfill the requirement and the solution
candidates for this. It should also make an estimate on the best solution candidate and the effort needed for implementing it.

The output document of this task is to be first circulated internally and among necessary parties (JRA1, JRA4, SA1, Architecture Team) for comments and feedback. Based on feedback a final revision of the milestone document is written , see task TJRA3.1.4. This final revision is later on used for setting the priorities forthe priorities for each implementation

the re-engineering work, what security components of EGEE software is to have its OGSA SEC compatible implementation and when.

5.4.3. Risks for OGSA SEC work

First version of EGEE middleware is likely to have rather few OGSA compatible features and thus it is probable that during the beginning if not whole of EGEE we are in a constant transition from EGEE based services to OGSI/WSRF enabled ones and there's no guarantee in terms of how far this transition will be able proceed during the EGEE project.

The currently available assumption of the EGEE middleware setup is that it will be built of components from EDG and Griphyn. The outcome of ARDA is another factor likely to affect the setup. This requires taking into account backward compatibility issues when OGSA security solutions are designed and implemented. This translates into securing backward compatibility with security modules like VOMS, LCAS, GACL, edg-java-security-authN/authZ etc. To stay informed about this transition, liaisoning with the Architecture Team, Operations Activity (SA1) and JRA1 is needed.

The inherent risks here are that the OGSA SEC work cannot acquire a complete enough set of requirements early enough in the project and that the requirements acquired at the start get modified later on, thus effectively nullifying some of the effort spent.

5.4.4. AuthZ and AuthN infrastrcture

Describe a unified infrastructure for authZ (and authN) common to hosted and native environments (part of EGEE & OGSA security software analysis task ??)

Artifact: Internal document
Start: PM1 End: PM3
Make a unified design of the authZ/authN infrastructure for both hosted (Java) and native (Linux/Solaris/...) environments. This first requires a completely new design of the Gatekeeper/jobmanager system for which the "factory" concept seems quite suited. This allows for a single implementation for authN/authZ, that can evolve together with the WS-*

standards, and a thin interface (setuid root) to actually run "legacy" (==UNIX-style) programs from the java environment.

5.4.5. GGF connection (OASIS+WS)

GGF is currently heavely debating the position of OASIS standards within the grid middleware. The latest approach towards managing the statefullness of resources is called the WS resource framework. The evolution of the approaches need to be understood and their influence on the security arcitecture evaluated.

5.5. TASK 4: GLOBAL SECURITY ARCHITECTURE

The Global Security Architecture document will develop continually throughout the EGEE project lifetime.

When choosing/architecting a suitable security model, it will be heavily influenced of the chosen overall architecture and messaging model. Thus, this is not a standalone artefact but deeply nested into the work of SA1, JRA1 and the architecture group.

Since so many people need to contribute input to this document, a workshop will be held early on in order to gather all the parties, and understand/agree on scope and process followed by topic-by-topic discussions. In addition, continuous and ongoing discussions will take place online in mailing lists and in the regularly scheduled Architecture and Security group meetings and phone conferences.

All in all, this makes it really hard to make reasonable effort estimates. The efforts given are for the organization of the workshop and for writing the initial revision of the global security architecture document.

5.5.1. T 4.1.1

Task	Security Architecture workshop
Artefact	Workshop
Start	PM0
End	PM2
Effort	???

5.5.2. T 4.1.2

Task	Participate in work on Global Architecture
Artefact	Regular meetings, phone conferences, online discussions
Start	PM0
End	PM24
Effort	???

5.5.3. T 4.1.3

Task	Security Architecture document
Artefact	Document
Start	PM0

End PM5
Effort ???

5.6. TASK 5: SECURITY OPERATIONAL PROCEDURES

```
Task    Inventory of current incident handling procedures
         collection of requirements from OMC and CICs
         review CSIRT reporting forms
Artif.  internal document
```
Start: PM1 End: PM4

```
Descr.  A large body of work is already available in
incident response.
         This document will give an overview of available
procedures and
         reporting forms and how they are applicable to
grid. An extensive
         overview in the context of GGF has already been
done. See, e.g.,
         http://www-
unix.gridforum.org/mail_archive/security-
wg/2003/01/msg00022.html
         This document forms the basis for negociation with
the OMC and
         CICs on the common reporting format and recommended
actions.
```

5.6.1. Task 5.1.1 Inventory of incident reporting practices and report formats

Artefact Inventory of current incident handling procedures and requirements from OMC and CICs, codified as an internal document
Start: PM1 End: PM4

A large body of work is already available in incident response. This document will give an overview of available procedures and reporting forms and how they are applicable to grid. An extensive overview in the context of GGF has already been done. See, e.g., http://www-unix.gridforum.org/mail_archive/security-wg/2003/01/msg00022.html This document forms the basis for negociation with the OMC and CICs on the common reporting format and recommended actions.

5.6.2. Task 5.1.2 Definition of a common incident report format

Artefact: Document describing the common incident report format, accepted by SA1
Start: PM3 End: PM4
Incident reporting templates distributed to the sites, with detailed explanation on how to describe incodents so that the information is most useful to the operations centres and the people doing incident assessment.

5.7. TASK 6: SECURE CREDENTIAL STORAGE PROCEDURES

The site access control architecture should be an integral part of and compatible with the overall security architecture, but deals with the specifics of accessing resources under the contgrol of the various resource providers. It deals with both access to hosted services (web services in containers) as well as access to native operating systems services on the host systems (execution of legacy programmes in a *nix environment).

It is foreseen that commonalities between hosted and native environments are maximally exploited, whilst at the same time improving the current set of tools to best fit into existing site access use models.

5.8. TASK 7: SITE ACCESS CONTROL ARCHITECTURE

The site access control architecture should be an integral part of and compatible with the overall security architecture, but deals with the specifics of accessing resources under the control of the various resource providers. It deals with both access to hosted services (web services in containers) as well as access to native operating systems services on the host systems (execution of legacy programs in a *nix environment).

It is foreseen that commonalities between hosted and native environments are maximally exploited, whilst at the same time improving the current set of tools to best fit into existing site access use models.

5.8.1. Task 7.1.1: Prototyping and refactoring of site access tools for architecture development

Artifact: Software based on the current code base but providing easier integration with existing and legacy system management environments
Start: PM1 End: PM9
[PS: THIS TASK NEEDS INPUT FROM VINCENZO AND INFN FOR VOMS]

Interface of LCAS/LCMAPS/JR with the PAM/NSS system. This will allow better system integration for those sites that are not willing to adopt the poolaccount lease mechanism and that do not want to migrate to centrally managed user directories like LDAP. It will be more light-weight than the poolaccount/poolgroup mechanism and thus more easily adopted by smaller sites). Probably similar optimizations are to be foreseen for the Java-side of things.

Development of VOMS will remain a INFN responsibility, that will nonetheless work in tight communication with JRA3 to make sure that JRA3 requirements will be taken into account and will be respected in new releases of the software. In particular this will mean allowing VOMS to become a more "lightweight" service that can be instantiated by "normal" users. Lightweight VOs are a prerequisite for EGEE even in the first year of the project.

The task is to be executed in close collaboration with JRA1.

5.8.2. Task 7.1.2: Describe site access control architecture in documentation

Artifact: DJRA3.2 public document describing the new uniform site access architecture
Start: PM6 End: PM8

This document should be based on the user requirements gathered in MJRA3.1, and discuss the comprehensive access architecture that will unify access to hosted and native systems. Discussion of RBAC models, distributed AAA decision making and Web services and WSRF security systems should be considered, as well as the way authorization information can be propagated from the site to the other grid components. Linked to the global security architecture.

5.9. RECURRENT TASKS

5.9.1. Support of existing tools and software

Artifact:
Start: PM1 End: PM18

Maintenance of components that are currently deployed: edg-java-AuthN/AuthZ, LCAS/LCMAPS, JobRepository (JR) and broadening the integration of these tools. In particular, the GridFTP server needs integration of LCMAPS, and the same may hold for integration of some edg-java-authZ/authN for the VO monitoring systems like R-GMA.

5.9.2. Support of new software

Artifact:
Start: PM6 End: PM24
We need to support our new software.

5.9.3. Operation of the EUGridPMA

Artifact: An operation PMA for grid authentication for e-Science in Europe
Start: PM1 End: PM24
New communities will continuously join the group, the guidelines documents must be update to reflect changes in the best community practices, and a global trust domain needs to be maintained by organizing periodic meetings, approximately 3-4 per year.

5.9.4. Quality Assurance

Artifact: Software, documentation that comply with the quality guidelines of the project
This includes software verification by code inspection and updating. *We will classify part of the software testing as QA.*

6. TOOLS

6.1. COLLABORATIVE TOOLS

In addition to the adopted project tools (Agenda Maker, EDMS, EGEE web site, Savannah) there seems to be a lack of collaborative tools. JRA3 is currently investigation a Python based portal framework which have a number of plugins available. Examples of plugins are: wiki and discussion forums are well as file document sharing.

The intent is to use this framwork for structuring the working notes and discussions that take place within JRA3 and the Security Group. Membership can be tighly controlled.

7. ISSUES

There are number of uncertain ascpects that have to be clarified:

- Security Group (SecG): mandate, objective and members. The SecG should act as a practical clearinghouse for security related issues for the project. It should combine regular and short status meetings (2 per week) with regular working (phone) meetings. As the tasks so require it may also happen that physical meetings of up to three times per year may need to be organized.
- Software development and support (old and new): what will be required during PM1—PM9 when it comes to support of new and old components (VOMS,…)
-