



Project no: **RI031844-OMII-Europe**

Project acronym: **OMII-Europe**

Project title: **Open Middleware Infrastructure Institute for Europe**

Instrument: **Integrated Infrastructure Initiative**

Thematic Priority: **Communication network development**

Deliverable JRA3.3
First report on all the sub-tasks of the common security task

Due date of deliverable: 2007-04-30

Actual submission date: 2007-05-21

Start date of project: **1 May 2006**

Duration: **2 years**

Kungliga Tekniska Högskolan [KTH]

Revision [1.0]

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)

Dissemination Level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Control Sheet

Document	Title: First report on all the sub-tasks of the common security task	
	ID: D:JRA3.3	
	Version: 1.0	Status: Final
	Available at: http://omii-europe.org	
	Software Tool: Microsoft Word 2003	
	File(s): DJRA3.3.doc DJRA3.3.pdf	
Authorship	Written by:	Azadeh Bararsani, KTH (AB) Katerina Stamou, KTH (KS) Fredrik Hedman, KTH (FH) Andrea Ferraro, INFN (AF) Morris Riedel, FZJ (MRi)
	Contributors:	JRA3/Task1+2 Activity Teams
	Reviewed by:	Valerio Venturi, INFN Sergio Anderozzi, INFN
	Approved by:	Technical Committee

Document Status Sheet

0.0.1	2007-03-19	Draft	Initial structure (KS+AB+FH).
0.1.0	2007-03-23	Draft	Structure expansion into draft (KS+AB+FH).
0.1.1	2007-03-28	Draft	Formatting and minor tweaks (FH).
0.1.2	2007-03-30	Draft	Fixed a number of parts in sections dealing with GT4 and gLite (AF).
0.1.3	2007-04-02	Draft	Integrated changes from AF into main document (FH).
0.2.0	2007-05-07	Draft	Changed doc scope after F2F Juelich meeting (AF).
0.2.1	2007-05-11	Draft	Adding some sections (FH).
0.2.2	2007-05-14	Draft	Text added (FH).
0.2.3	2007-05-14	Draft	Edited 4 th subtask (AF).
0.2.4	2007-05-17	Draft	Added Partners and Efforts section and some corrections.
0.2.5	2007-05-18	Draft	Review (Xee).
0.2.6	2007-05-21	Draft	Review (MRi).
0.2.8	2007-05-21	Final Draft	Triage of comments review (FH).
0.2.9	2007-05-21	Final Draft	Updated effort table (FH).
0.3.0	2007-05-22	Final Draft	Removed overall Executive summary. Added Conclusion and a paragraph on Credential management. (FH)
0.3.1	2007-05-25	Final Draft	Partners section moved to D:JRA3.1 (FH).
0.3.2	2007-05-30	Final Draft	JRA3 team comments integrated (FH).
0.3.3	2007-06-04	Final Draft	Reviewer comments taken into account (FH).
1.0	2007-06-05	Final	Last comments added (FH).

Executive Summary

This document gives an overview of the achievements of the JRA3 Common Security Infrastructure activity in the first year of the OMII–Europe project (May 2006 - April 2007) and an update of the plans for the following year. The Common Security Infrastructure activity (Task1), lead by KTH, is one of the two tasks in JRA3—the other, lead by FZJ, is Infrastructure Integration (Task2). Overall, the JRA3 activity is coordinated by KTH. Task1 strives to harmonise and define a core set of security features that will enable users to make use of multiple middlewares with a single underlying security infrastructure. Special focus is on a closer integration of UNICORE and gLite—to facilitate job execution on UNICORE or gLite submitted jobs—although efforts are also directed to address GLOBUS and CROWNGrid interoperability.

During the first year we have defined a common security technology base starting with an initial set of standards that are widely adopted, together with an emerging specification from OGF. We have also implemented a solution for credential provisioning for UNICORE based on proxy certificates. For [the coming 12 months](#) we plan to update the common security technology base using the experiences gained from the joint efforts of Task1 and Task2 in evolving our initial profile with the second iteration of the multi-platform [Grid](#) infrastructure of Task2. The work on a prototype credential management system, that will support both legacy and emerging middleware, [is under way and](#) will be completed at the end of M18. To adequately report on the further developments of the common security technology activities we suggest adding one milestone in M22.

Table of Contents

1	Introduction.....	6
2	Progress.....	6
2.1	Common Security Technology Base	7
2.1.1	Progress for Year 1	7
2.1.2	Plans for Year 2	7
2.2	Credential Provisioning for UNICORE.....	8
2.2.1	Progress for Year 1	8
2.2.2	Plans for Year 2	8
2.3	Credential management	8
2.3.1	Plans for Year 2	8
2.4	Other security assessments	9
2.4.1	Progress for Year 1	9
2.4.2	Plans for Year 2	9
3	Summary.....	9
4	References.....	10

1 Introduction

The objective of the JRA3 Infrastructure Integration Activity is to initiate tighter integration of Grid infrastructures than would be achieved merely through the adoption of common services supporting inter-working of different Grid infrastructures. Furthermore, the intention is to greatly increase their usability by enabling a much more flexible approach to Virtual Organizations (VOs). This document gives an overview of the achievements for the first year of the JRA3 Common Security Infrastructure activity (Task1). This task strives to harmonise and define a core set of security features that enables user access to multiple middlewares from a single underlying security infrastructure. The deliverables and milestones for Task 1 (Table 1) during the first year are

No.	Title	Date	Completed
M:JRA3.1	Definition of a common security technology base	M12	M12
M:JRA3.2	Credential provisioning in UNICORE	M12	M12
D:JRA3.3	1 st yearly report on the Common security task (this doc)	M12	M12
D:JRA3.1	1 st Report on the Infrastructure Integration Activity	M12	M12

Table 1. Year 1 milestones and deliverables for Task 1

More details on the progress of these efforts are given in the sections below. Deliverable D:JRA3.1 is the combination of reports from Task1 and Task2. For the coming 12 months we plan to update the common security technology base using the experiences gained from the joint efforts of Task1 and Task2. We are in the process of developing a prototype credential management system, supporting both legacy and emerging middleware. We suggest adding a milestone in M22 to describe the second iteration of the common security technology base for the coming year. Task1 milestones and deliverables (Table 2) are summarized by

No.	Title	Date
M:JRA3.3	Prototype credential managements system	M18
M:JRA3.6	2 nd iteration of common security technology base (new)	M22
D:JRA3.4	2 nd yearly report on the Common security task	M24
D:JRA3.2	2 nd report on the Infrastructure Integration Activity	M24

Table 2. Year 2 milestones and deliverables for Task 1

2 Progress

This section gives an overview of the achievements of JRA3 Task1 during the project's first year. Full technical details are available in the Milestone documents M:JRA3.1 and M:JRA3.2, available from the OMII-Europe web [\[1\]](#).

2.1 Common Security Technology Base

2.1.1 Progress for Year 1

During the first year we have defined a common security technology base. The starting point is the emerging HPC Basic Profile, Version 1.0 [2]. For the scope of this project we assume that the management of VO-related attributes such as membership to VO/group/roles is implemented by VOMS; additionally we have also adopted proxy certificates [3], attribute certificate [4], SAML2.0 [5] and XACML2.0 [6] to support both existing production environments and newer [Web-services](#) based platforms as represented by [the](#) first prototype of the Multi-Platform Grid Infrastructure of Task2. The defined common security technology base (security profile) is detailed in the milestone M:JRA3.1.

Assuming that proxy certificates can be supported by all the involved middleware [means](#) that UNICORE needs to be extended to also [accept these](#) certificates. Extending the generality of UNICORE in this particular way opens up the possibility of a rather general interoperability scenario in the security domain. Using this feature in production Grid scenarios then becomes a site policy issue. Initial discussion with people involved in these types of policy decisions at UNICORE sites indicate that this feature should be acceptable—especially since interoperability is becoming a key enabler and concern in more and more production environments. We have implemented and tested this extension for UNICORE 5. The implementation approach adopted is a useful starting point also for [the recently](#) released [Web services-based beta version of](#) UNICORE 6. More details on this work are found below in the section “Credential Provisioning for UNICORE”.

2.1.2 Plans for Year 2

To advance further on the security profile we should expect to update the profile based on the joint efforts of Task1 and Task2. This is because as we proceed into the second year of the project we will most certainly uncover blind spots in the profile, as the second iteration of the Multi-Platform Grid Infrastructure unfolds. This may involve additions to the profile, but due to time and resource constraints it may also mean that some issues will be out-of-scope for this project. The goal is to move the emphasis from the current username-password client authentication to a certificate-based authentication following the HPC Basic Profile. The second iteration of the security profile (M:JRA3.1) will be documented in a proposed additional milestone, M:JRA3.6 in M22. The input for the updated profile will be generated in the close collaboration of Task1 and Task2. Furthermore, with a solution in place for authentication we intend to investigate solutions for authorization and policy decision points ([PDP](#)) that may be included in the profile. Implementing the profile requires that the middleware components of Task2 are adapted. The current priority list for re-engineering work is currently as follows: Job Management, Accounting, VOMS, Information Foundation, Portals and Database Access.

2.2 Credential Provisioning for UNICORE

2.2.1 Progress for Year 1

This work has focused on the definition of a uniform method and service interface to provide applications with the required credentials, in the form of proxy certificates, at runtime. This problem has been addressed in GLOBUS and gLite, but not in UNICORE. In the security profile we have adopted proxy certificates (RFC 3820) as common base line to authentication for use in this project. [A solution to accommodate this choice is to extend UNICORE to accept also proxy certificates.](#) The core of our modification is the customization of the Java Trustmanager. We override the default java native certificate path validation algorithm with an external proxy certificate path validation algorithm. This algorithm is provided by COG JGlobus project classes. [These classes provide a wide spectrum of different proxy certificate validation schemes and ensure that the same authentication fabric can be shared between gLite, UNICORE, GLOBUS and CROWNGrid.](#) A more detailed [discussion](#) of the pros and cons of these solutions can be found in the Milestone M:JRA3.2.

2.2.2 Plans for Year 2

During the first year we have focused our efforts on the stable UNICORE5 version. During the second year, these extensions will be migrated to the new [Web services-based UNICORE6](#) version by making a direct connection with the work planned for the next milestone.

2.3 Credential management

2.3.1 Plans for Year 2

The objective is to simplify the currently difficult task of Credential management for end-users in gLite, UNICORE, GLOBUS and CROWNGrid. This will be addressed through the use of MyProxy and the PURSE registration tool, which are used to acquire a proxy certificate. Work in this area has started and is making good progress towards the milestone M:JRA3.3 at M18. PURSE is being refined and the integration with UNICORE has started. An interesting synergy has also been identified with the JRA1 Portals activity: some of the registration and security features can be nicely provided via PURSE. Progress of this activity has been demonstrated at OGF20 and we also expect to contribute our developments back into the PURSE GLOBUS incubator branch.

[The new SAML-based VOMS server](#) developed in the JRA1-VOMS task has a central role in the context of authorization in the prototype multi-platform Grid infrastructure developed in [JRA3-Task 2](#). [The new open standard compliant and SAML-based VOMS server is loosely coupled with respect to any specific Grid middleware and usable with a standalone Web service container such as Apache Tomcat.](#) This means that the new [VOMS server](#) can act as [a powerful and loosely coupled component, usable in conjunction with all Grid middlewares of OMII-Europe.](#) [Via the close collaboration with JRA3-Task 2](#) we will further investigate how to fully exploit this component together with the services provided by MyProxy. Thus, our next steps in this task [are](#) to develop an interface that can combine information from MyProxy and an attribute authority (e.g.VOMS). We note that attribute certificates (RFC 3281) are used in several places, implemented individually. For compatibility, usability and standardisation reasons we are in the process of refactoring this

functionality into a commonly used Open Source library, OpenSSL. People in the project who are also committers of OpenSSL do this work. [An OpenSSL](#) snapshot of this will be available in M16 and the regular release will be included in M:JRA3.3.

2.4 Other security assessments

2.4.1 Progress for Year 1

The objective of this subtask is covering other security issues not covered by other subtasks. In particular it is analyzing mechanisms adopted by the main [Grid](#) infrastructures to achieve security goals different from authentication. Its main interests [are](#) focused on authorization, accounting confidentiality and trust. A lot of heterogeneous information has been collected from established non-OMII working groups (as OGSA AuthZ-WG and EGEE MSWG) and from online documentation in order to produce some draft internal papers posted in JRA3 wiki. The difficult aspect of [a](#)uthorization integration and implementation [has been](#) studied in order to be adopted in a multi [Grid](#) SOA environment. We found that all authorization mechanisms were dedicated and intimately related to specific middleware services.

2.4.2 Plans for Year 2

The presence of widely accepted authorization policy standard languages (as XACML) does not guarantee transparent authorization compatibility among the main involved middlewares. Another field covered by this task is trust management. It is concerned with Certificate Authorities (CAs) agreements and renewals of certificates in the current main infrastructures. Every infrastructure uses its own mechanism for updating CA certificates (OSG/VDT, EGEE, etc). Some infrastructures use automatic ways, others manual ways. Site administrators often do not update them automatically for security reasons, but when they do not, Virtual Organizations (VOs) have problems such as good certificates not being accepted because a CA is not recognized. On the other hand automatically updating CAs certificates can crush all security precautions if infrastructures lack a very careful updating mechanism.

OMII interests apply also to accounting matters. While JRA1 accounting is focused on accounting interoperability, it is a JRA3 duty to guarantee the strict confidentiality of accounting data exchanged among different [Grid](#) infrastructures. In this context, where no standards are widely accepted, we are evaluating possible approaches that can be accepted by different administrative domains. The result of this subtask will be included in the report M:JRA3.6 at M22.

3 Summary

The JRA3 Infrastructure Integration Activity is initiating tighter integration of [Grid](#) infrastructures and also increasing their usability by enabling a much more flexible approach to Virtual Organizations ([VOs](#)). We have defined a common security technology base with the emerging HPC Basic Profile, Version 1.0 as the starting point; additionally we have also adopted proxy certificates (RFC 3820), attribute certificates (RFC 3281), SAML2.0 and XACML2.0—to support both existing production environments and newer [Web-services](#) based platforms as represented by [the](#) first prototype of the Multi-Platform Grid Infrastructure of Task2. For the scope of this project we assume that [Virtual Organizations \(VO\)](#) are [implemented](#) by VOMS. We also assume that proxy

certificates can be supported by all the involved middlewares. This assumption holds for all major Grid middlewares except UNICORE 5. Consequently we implemented and tested this extension for UNICORE 5. The implementation approach adopted is a useful starting point also for [the recently released](#) Web services-based [beta version of](#) UNICORE 6.

To advance the security profile we expect to update the profile based on the joint efforts of Task1 and Task2. We intend to move the emphasis from the current username-password client authentication to a certificate-based authentication, following the HPC Basic Profile. These developments will be documented in a new milestone, M:JRA3.6 in M22. This milestone will also include the investigations covered in the subtask that is analyzing mechanisms adopted by the main [Grid infrastructures](#) to achieve security goals different from authentication.

Improved credential management for end-users in gLite, UNICORE, GLOBUS and CROWNGrid will be addressed through the use of MyProxy and the PURSE registration tool. Work on this is progressing, has been demonstrated at OGF20, and will be reported in the milestone M:JRA3.3 at M18. Furthermore, the PURSE developments will be contributed into the PURSE GLOBUS incubator branch. Through [the close collaboration with JRA3-Task 2](#) we will further investigate how to fully exploit the new SAML-based VOMS server – developed in the JRA1-VOMS activity – together with the services provided by MyProxy. Attribute certificates (RFC 3281) are used in several commonly used software packages, implemented individually. For reasons of compatibility, usability and standardisation we are in the process of adding attribute certificates (RFC 3281) to OpenSSL. [The work is performed by](#) one of the [committees of OpenSSL](#) who is on part of the JRA3 team. [An OpenSSL](#) snapshot that includes attribute certificates will be available in M16 and a regular release will part of M:JRA3.3 at M18.

Deleted: 1

4 References

- [1] OMII-Europe web <http://omii-europe.org>
- [2] HPC Basic Profile 1.0
http://www.ogf.org/Public_Comment_Docs/Documents/Feb-2007/HPC_Basic_Profile_v1.0.pdf
- [3] RFC 3280 <http://www.ietf.org/rfc/rfc3280.txt>
- [4] RFC 3281 <http://www.ietf.org/rfc/rfc3281.txt>
- [5] SAML2.0 <http://www.oasis-open.org/specs/index.php#samlv2.0>
- [6] XACML2.0 <http://www.oasis-open.org/specs/index.php#xacmlv2.0>