EUROPEAN MIDDLEWARE INITIATIVE

DJRA1.3.2 – SECURITY AREA WORK PLAN AND STATUS REPORT

EU DELIVERABLE: D5.3.2

Document identifier:	**EMI-DJRA1.3.2-1277568-Security_Area_Work_Plan_M12-v1.0.doc**
Date:	**30/04/2011**
Activity:	**JRA1**
Lead Partner:	**UH**
Document status:	**Final**
Document link:	**http://cdsweb.cern.ch/record/1277568**

Abstract:
This deliverable contains the detailed work plan of the Security Services technical area compliant with the overall EMI Technical Development Plan. The plan is released early in the project life and updated every year including a status report on the achievements of the past 12 months compared to the planned objectives. This status report covers the current status and plans for the next years while the work plan at M36 will provide recommendations for further work.

Delivery Slip

	Name	Partner / Activity	Date	Signature
From	John White	UH/JRA1	17/05/2011	
Reviewed by	Enol Fernandez, Andre Giesler	CSIC/JRA1, JUELICH/JRA1,SA1	25/05/2011	
Approved by	PEB		01/06/2011	

Document Log

Issue	Date	Comment	Author / Partner
1	08/04/2011	Table of Contents	John White/UH
2	17/05/2011	v0.5 for review	John White/UH
3	20/05/2011	v0.6 for review	John White/UH
4	01/06/2011	v1.0 PEB approved version	PEB

Document Change Record

Issue	Item	Reason for Change
1		
2		
3		

TABLE OF CONTENTS

1. INTRODUCTION

1.1. PURPOSE

This deliverable contains the current status and detailed work plan of the security services technical area compliant with the overall EMI Technical Development Plan. The first plan was released early in the project life and is updated every year including a status report on the achievements of the past 12 months compared to the planned objectives.

1.2. DOCUMENT ORGANISATION

This document describes the current state of progress, with respect to the technical objectives of previous work plan, of the Security Area of EMI. Then the technical objectives of the second year of EMI are described along with the work foreseen to achieve these objectives.

1.3. REFERENCES

R1	The Globus Project http://www.globus.org/
R2	UNICORE Project http://www.unicore.eu/
R3	YAIM Ain't an Installation Manager http://yaim.info/
R4	AAI Workshop https://www.egi.eu/indico/sessionDisplay.py?sessionId=11&confId=48
R5	The Virtual Organization Management Registration Service http://computing.fnal.gov/docs/products/vomrs/
R6	Shibboleth http://shibboleth.internet2.edu/
R7	Kerberos, The Network Authentication Protocol http://web.mit.edu/kerberos/
R8	Chemomentum Project http://www.chemomentum.org/
R9	MyProxy Credential Management Service http://grid.ncsa.illinois.edu/myproxy/
R10	Open Middleware Infrastructure Institute http://omii-europe.org/
R11	Open Science Grid http://www.opensciencegrid.org/
R12	LHC Computing Grid http://lcg.web.cern.ch/lcg/
R13	Gridsite http://www.gridsite.org/
R14	EPEL

	http://fedoraproject.org/wiki/EPEL
R15	Open Nebula http://opennebula.org/
R16	Open Grid Forum http://www.gridforum.org/
R17	EUGridPMA http://www.eugridpma.org/
R18	DNA1.3.1 Technical Development Plan (M02) http://cdsweb.cern.ch/record/1277540
R19	DNA1.3.2 Technical Development Plan (M11) http://cdsweb.cern.ch/record/1277543
R20	DJRA1.3.1 Security Area Work Plan and Status Report (M03) http://cdsweb.cern.ch/record/1277566
R21	DJRA1.3.2 Security Area Work Plan and Status Report (M12) DJRA1.3.2 Security Area Work Plan and Status Report GANTT (M12) http://cdsweb.cern.ch/record/1277568
R22	European Grid Initiative http://www.egi.eu/
R23	Common XACML Authorization Profiles https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4XACML
R24	UMD Security Capabilities Quality Criteria https://documents.egi.eu/public/RetrieveFile?docid=240&version=8&filename=EGI-SECURITY-QC-V1.3.pdf
R25	AAI Usecases https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4AAI
R26	Required features of the caNl https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4CaNlRequirements
R27	Components using TLS/SSL authentication and code providers https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4CaNlComponents
R28	The caNl SSL/TLS and X.509 API https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4CaNlAPI
R29	Common SAML attribute profile Strawman proposal RC1 https://twiki.cern.ch/twiki/bin/view/EMI/CommonProfileStrawmanProposalV3
R30	UVOS -> VOMS https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1SecCompRemoval#UVOS_VOMS
R31	https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1SecCompRemoval
R32	Credential Delegation in EMI https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4DelegationInEmi
R33	Argus Work Plan https://twiki.cern.ch/twiki/bin/view/EMI/ArgusPTWorkplan
R34	Analysis of move to OpenSAML2 library in UNICORE https://twiki.cern.ch/twiki/bin/view/EMI/UNICORESecurityPTSopenSAML

R35	Analysis of usage of short lived certificates in UNICORE https://twiki.cern.ch/twiki/bin/view/EMI/UNICORESecurityPTSLC
R37	Common CE XACML Authorization Profile, Version 1.0 https://twiki.cern.ch/twiki/bin/view/EMI/XACMLCommonCEProfileV1_0
R38	Common Virtual Organization Attribute Profile version 1.0 https://twiki.cern.ch/twiki/bin/view/EMI/CommonSAMLProfileV1_0_1
R39	EMI Description of Work (Public DoW) https://twiki.cern.ch/twiki/pub/EMI/EmiDocuments/EMI-Part_B_20100624-PUBLIC.pdf

1.4. DOCUMENT AMENDMENT PROCEDURE

This document can be amended by the authors further to any feedback from other teams or people. Minor changes, such as spelling corrections, content formatting or minor text re-organisation not affecting the content and meaning of the document can be applied by the authors without peer review. Other changes must be submitted to peer review and to the EMI PEB for approval.

When the document is modified for any reason, its version number shall be incremented accordingly. The document version number shall follow the standard EMI conventions for document versioning. The document shall be maintained in the CERN CDS repository and be made accessible through the OpenAIRE portal.

1.5. TERMINOLOGY

AC	Attribute Certificate
AA	Attribute Authority
AAI	Authentication and Authorization Infrastructure
API	Application Programming Interface
AREX	ARC Remote Execution service
AuthN	Common short-hand for Authentication
AuthZ	Common short-hand for Authorization
CLI	Command Line Interface
CREAM	Computing Resource Execution and Management
DCI	Distributed Computing Infrastructure
EGI	European Grid Initiative
ETD	Explicit Trust Delegation
EES	Execution Environment Service (Argus)
EES	EMI Execution Service
GACL	Grid Access Control Language
GSI	Globus Security Infrastructure
HEAD	ARC Hosting Environment Daemon
HiLa	UNICORE High Level API for Grid Applications

IdP	Identity Provider
KPI	Key Performance Indicator
LCG	LHC Computing Grid
LHC	Large Hadron Collider
LRMS	Local Resource Management System
OCCI	Open Cloud Computing Interface
PAM	Pluggable Authentication Modules
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
PSNC	Poznan Supercomputing and Networking Center
REST	REpresentational State Transfer
RfC	Request for Comment
SAML	Security Assertion Markup Language
SCAS	Site Central Authorization Service
SLCS	Short Lived Certificate Service
SPL	Simplified Policy Language
STS	Security Token Service
UCC	UNICORE Command line Client
USE	UNICORE Services Environment
UVOS	UNICORE Virtual Organization System
VOMS	Virtual Organization Management System
XACML	Extensible Access Control Markup Language

2. EXECUTIVE SUMMARY

This Security work plan document gives the status of the Security Area work after the first year of the EMI project and the plans for the second year and a best as possible the third year. These plans exclude work such as regular maintenance and bug-fixing of components in production usage. This document is organized into a Security Area status report and a work plan.

The Security Area status report section gives the current status of work performed to achieve the objectives described in DNA1.3.1 Technical Development Plan (M2) [R18] and DJRA1.3.1 Security Area Work Plan (M3) [R20]. These status reports are organized by objective and give the actual state versus the schedule provisioned in DJRA1.3.1. The year one Security Area objectives described in DNA1.3.1 were achieved overall. There are small number cases where the schedule has fallen behind, e.g. AAI strategy work, due to the higher than planned effort needed to configure, package and certify Security Area products compliant with the release process policies. The technical highlights in EMI year one have included the GSI-free VOMS release, Argus authorization system release and preliminary integration to UNICORE and ARC. Other technical highlights are the agreements on common EMI profiles for SAML and XACML and the common authentication library APIs. The details are given in Section 3. The last sub-section of Section 3 gives an overview of the work performed in the past year of the EMI project within each EMI Security Area product team. The work reported in this last sub-section is work performed that is not directly aimed at the achievement of the objectives in DNA1.3.1. e.g. user requests for improvements.

The Security Area work plan outlines the work for the second year and, where possible, third year. This section is also organized by objective. The section organization differs to that of the status section in that some of the objectives from DNA1.3.1 have been modified to reflect the experience of the past year. Also, some new objectives have been set, available here and also in DNA1.3.2 Technical Development Plan (M11) [R19]. These objectives have been set as a result of a set of requirements from EMI customers, notably EGI [R22] and LCG [R12]. These requirements were prioritized in DNA1.3.2 and the appropriate items taken by the Security Area. As this section is organized by objective there can be more than one product team reporting.

The main points are as follows: The common attribute authority (VOMS-SAML) work, in conjunction with the common EMI SAML profile, has moved to the implementation/integration stage, e.g. integration to the UNICORE [R2] stack. Likewise, the APIs for a common set of authentication libraries are defined and the implementation of new code and re-factoring of existing code will proceed in year 2. The integration of the Argus authorization system, along with the common EMI XACML profile, will continue. The EMI Security Area components will be released to operating systems other than SL5/64bit and will comply with the operating system standard practices. Following the theme of reducing the complexity for users, the AAI strategy now moves to a phase to actually implement the services needed. Likewise release and support for the services needed for encrypted data storage and user identity protection will be continued. There are some objectives which have been noted but will need more user input: configuration of database backends; performance of services; denial of service attack protection; writing of monitoring probes. The removal of the Globus [R1] GSI continues with the common non-GSI delegation agreement in the works.

3. SECURITY AREA STATUS REPORT

The following subsections describe the work performed to achieve the DNA1.3.1 technical objectives. Any deviations and their justifications are also provided.

3.1. COMMON SECURITY ATTRIBUTES

The objective is described as "Agreement on a minimal common set of security attributes to be used in policies". The work performed for this objective started with a general agreement that Argus will become the common authorization system for the three middleware stacks in EMI. In order for the job management systems of the three stacks to be enabled to use this common service a common XACML profile was produced. The XACML group determined the following:

• Gathered the XACML profile requirements of the different Compute Elements.

• Determined the work needed to modify/extend the current (CREAM) CE XACML profile.

• Clarified that the full XACML spec is met within Argus.

• Attempted to collect requirements from the EMI Execution Service (EES) and Data Management.

These last requirements have not been gathered by the time of publication of the XACML profile. It was deemed more important to go ahead with the profile. An amendment will be made later once the information is forthcoming. This profile can be found at [R23].

The integration of computing elements, from the three middleware stacks of EMI, with Argus is underway.

3.2. SECURITY CREDENTIAL MANAGEMENT

This objective is stated as: "Simplified management of security credentials by reducing the complexities of handling certificates and integrating different security mechanisms like Shibboleth [R6] and Kerberos [R7] across the EMI stack that allows users to use their own authentication system to access a 'Grid'".

The work started by forming a group within the Security Area in order to discuss and plan the strategy. A requirement from EGI was received as follows: "Users should be able to access grid resources using institutional authentication systems" from the EGI document [R24].

Based on the results of the workshop, "AAI for DCIs" workshop [R4], a set of use-cases [R25] have been developed. These are being used to produce the high-level requirements of the Security Token Service (STS) prototype that will depend on the Shibboleth IdP v.3 and in collaboration with the WS-Trust interoperability group.

The AAI strategy work has been impacted by the higher than planned effort needed to build, install and certify Security Area products compliant with SA2 policies. During the last months of the first year, the main goal was to have the first EMI major release and this took precedence over development tasks. It is reasonable to expect that this activity can proceed with greater speed after EMI 1. The planned merging of the VOMS Attributes from Shibboleth (VASH) functionality into VOMS needs to be reviewed.

3.3. COMMON AUTHENTICATION LIBRARIES

This objective is stated as: "Provide common authentication libraries supporting X.509 and optionally SAML". The duplicate authentication (AuthN) systems and libraries will be removed and a standard solution of a common set of AuthN libraries will be provided across the three middleware stacks. The "Common Authentication Library" group has collected:

• A set of requirements on the AuthN common lib API [R26]

• An inventory of existing code that uses AuthN code [R27]

• The API definitions in C/C++ and Java [R28]

The work up to now has consisted of getting the above steps finished and especially making sure that the API definitions are suitable for the three middleware stacks in the EMI release. Once the API definitions were agreed they were independently reviewed by members of the project outside the immediate Security Area in order to catch mistakes or biases. This has been completed for the Java API, C/C++ still pending.

The estimate of effort and timelines for producing missing parts has not been completed due to the complexity and length of the above tasks. The prototype versions of these libraries, planned for month 8 in the first year of the EMI project, will not be available due to other commitments for the EMI 1 release but the implementation is still planned for the end of the second year. This will be discussed in the later section of this document. Likewise, the optional updates of the X.509 API based on comments from product teams are delayed. Also, the integration of these libraries to EMI components is likewise delayed. Although in the previous document it was anticipated this work would not be available for EMI 1.

The need for a SAML authentication library was investigated, as described in the previous document. As the three middleware stacks use X.509 credentials for their "first" authentication step, it was deemed that the effort required for a SAML AuthN library can wait. This decision was made also based on some of the strategy decisions of the Authentication and Authorization Infrastructure group.

3.4. REDUCTION OF SECURITY COMPONENTS

This objective has been stated as "Consolidation and reduction in the number of security clients and CLIs so that the users don't have to face the very different clients and utilities". For this objective, the net result over the first year of the EMI project is that there have been no removals of clients or Command Line Interfaces (CLIs). The list of components to be released in the EMI 1 release is produced by all the EMI product teams. As a result, no truly common client packages have been found that can function with the three middleware stacks in the EMI 1 release.

3.5. COMMON ATTRIBUTE AUTHORITY

This objective is stated as "Agreement and full support for a common single SAML based Attribute Authority Service integrated with all EMI components".

The SAML profile group has been formed and performed the following work:

• The OMII [R10]-Chemomentum [R8] profile document was used as a starting point for the common SAML profile.

• The SAML profile proposal has been finalized between the three middleware stacks [R29].

The work items that still need to be performed are:

• The coordination of the move of all middleware stacks to the opensaml2 library.

• The requirements gathering from EGI on the usage of SAML with respect to the granularity of authorization decisions by the LHC Computing Grid (LCG).

• Investigation of SAML delegation as a means of restriction of privilege of security tokens.

• Plan the replacement of UNICORE Virtual Organisations System (UNICORE UVOS) with VOMS-SAML.

• Producing time lines for the future work.

These items still need to be completed due to the longer than anticipated process to reach an agreement on the SAML profile that satisfied all three middlewares.

The planning of the replacement of UNICORE UVOS by VOMS-SAML, a task of this group has started. The first discussions on this subject are available at [R30]. The main results of these first observations are that the effort expected for this task will be large on both the UNICORE Security and VOMS product teams. Also, the feature list of UNICORE UVOS matched to VOMS needs to be finalized. This work is foreseen to touch other development areas of the EMI project, for example: the discovery of the VOMS address by the UNICORE client requires the existence of an EMI Registry.

3.6. REDUCTION IN COMPONENTS

This objective is stated as "Substantial simplification and reduction in the number of all Security Area libraries, internal components and services, and internal components". This objective has been started with a series of component replacement scenarios. In order to replace a component its functionality must be carried by another component, implying redundancy. If a functionality has been declared as obsolete by EMI clients (e.g. EGI), then a component maybe removed from the EMI stack. This activity has considered the cases in [R31]. The possibility of removing components in order to be replaced by others has been considered.

The general observation as a result of this work is that the component reduction task is not well-defined. Reducing the amount of code to be maintained would be a practical target. Merging components is not a simple task unless the resulting component can completely take over the super-set of functionalities.

The most promising candidates in this process are: replacing the Trustmanager/Util-Java in the newly created Common Authentication Libraries (still to be implemented); replacement of the VOMS server by VOMS-Admin; replacement of UNICORE UVOS by VOMS-SAML (as mentioned above as part of the Common Attribute Authority objective). These are the most reasonable proposals since they are currently logical and are controlled by one product team. Other proposals, such as the replacement of LCAS/LCMAPS or gLExec, are less likely due to their widespread (and potentially unknown) usage and the need for work to cross product team boundaries. This would probably lead to resistance from clients within EGI (and others such as OSG [R11]) and the removal of such components needs further investigation.

The question of the overall phase-out and replacement of the gLExec component was studied. gLExec has been reviewed numerous times and is well suited for the task in the Grid environment. The effort to replace gLExec with sudo as described in the previous document cannot be justified currently. The results of these studies have concluded that the way to proceed is to create a PAM interface next to LCMAPS for gLExec and generic PAM Argus module, which can be used by gLExec. At this stage, there could be the possibility LCAS/LCMAPS may be removed from the worker nodes.

3.7. DATA ENCRYPTION AND ANONYMIZATION

This objective is stated as "Provide a transparent solution for encrypted storage utilizing ordinary EMI SEs". The Hydra keystore service, used by the biomedical community, is being released in EMI 1. The correction of the issues found in the EGEE-III SA3 code reviews by PSNC will have to wait for an update as the work to build Hydra in the EMI environment was more difficult than anticipated. The integration of the Hydra key stores to Cloud resources is underway, although the internal milestone document is not ready. The pseudo-anonymity service, that provides an anonymous yet audit-able identity, is also being worked on to release in EMI 1. The original implementation was built on the gLite SLCS, which is now understood to be not released by EMI. Therefore the pseudonymity service implementation is currently being updated to remove dependencies to SLCS and other unsupported components.

3.8. COMMON DELEGATION SOLUTION

This objective was stated in DNA1.3.1 as "The legacy Globus security infrastructure (GSI) will be replaced with a common security solution based on TLS/SSL still including the delegation capability". The progress of this work is tracked at [R32]. The current status of this work is that the gridsite [R13] delegation, already widely used in the gLite stack, should be used as the standard delegation method. A working group is being established within OGF [R16] to handle the standardization of gridSite. The group will be formed to look into establishing an OGF standard for delegation and the first item will be to write up gridSite as an OGF document.

3.9. EVOLVE EMI COMPONENTS TO MEET SPECIFIC USER REQUESTS

This section gives the current status of work performed by the product teams over the last year in relation to the plans given in DJRA1.3.1.

3.9.1 ARC Security Utils Product Team

The ARC Security Utils Product Team releases their products as a part of the ARC middleware stack hence releases no separate versions. The latest version, ARC-11.04, is released for EMI 1. There was no new functionality introduced to the code. The work mostly concentrated on enhancing existing code-base and functionality. As part of the effort for reducing the number of components the update-crl utility has been replaced by fetch-crl provided by EPEL [R14].

3.9.2 Argus Product Team

The Argus Product Team has released both Argus versions 1.2 (for gLite 3.2) and 1.3 (for EMI 1). The work plan can be referenced at [R33]. The features added in these releases include:

Argus 1.3 (EMI 1):

- EMI 1 release of the Argus Authorization Service.
- The Argus components have all been repackaged to be compliant with EMI packaging policies.
- A new thread-safe Argus PEP client library for C has been released.
- Support for the DPM/LFC banning engine has been added to the Argus PEP Server.
- Support for direct PDP XACML requests for UNICORE has been improved in the Argus PDP.
- Some minor bugs have been fixed.

Argus 1.2 (gLite 3.2):

- Implemented the required security recommendations made by PSNC Security Team.
- Policy Enforcement Point (PEP) daemon mapping obligation handler.
- Implemented a consistent FQAN/DN based user mapping strategy.
- Added support for DN based group account mapping in group-mapfile.
- Finalized the XACML Grid CE profile [R8] v.1.0 for CREAM.
- Updated Policy Information Point (PIP) to support the XACML Grid CE (CREAM) profile.
- Released the PEP-Java client library.
- Added the pap-admin add-policy -obligation <obligation-id> parameter.

The EES prototype has been written and includes an Obligation Handler for the Argus PEPd. The plug-ins needed to start and stop VMs need adaptation in order to conform to the developing Cloud APIs (e.g. Open Nebula 2 [R15]).

3.9.3 VOMS Product Team

The common SAML-enabled VOMS (VOMS-SAML) version has been released for EMI 1 as planned. The VOMS-SAML integration to other middleware components is being planned as the common SAML profile within the middleware has been agreed upon. The Globus-free version of VOMS server and client (VOMS 2.0) is released for EMI 1. This EMI 1 version also provides a REpresentational State Transfer (REST)-ful interface for obtaining X.509 attribute certificates.

For the VOMS-Admin the support for external Virtual Organization (VO) membership databases has been added, initially consisting of support for the CERN orgdb currently in use by the Large Hadron Collider (LHC) experiments VOs. VOMS-Admin also provides a SAML attribute authority implementing the common VO SAML profile described elsewhere in this document.

3.9.4 gLite Security Product Team

The reorganization of Trustmanager and Util-Java into more logical components and plug-ins and a more flexible configuration have been released for EMI 1. The support for RFC3820 proxies has been added to delegation-java and released for EMI 1.

The LCAS/LCMAPS versions for EMI 1 have been prepared and released. The LCMAPS-c-pep plug-in has been released for EMI 1 with the required Argus 1.3 compliance. gLExec has been released for EMI 1, as planned. The version released addresses logging and feature requests concerning security checks. The EMI 1 version of gLExec includes fixes, requested from a security vulnerability assessment (as part of EMI SA1), to enable SGE and Condor tracking GIDs to work across a gLExec call, the installation of a default glexec.conf file and a default lcmaps-glexec.db file. The build-time configuration steps have been simplified through support for specifying LCAS/LCMAPS db files on the configure command line.

3.9.5 UNICORE Security Product Team

The integration of Argus to UNICORE has proceeded with the policy requirements covering the current default policy provided. A list of typical UNICORE use-cases for Argus and a list of relevant authorization attributes have been given to the Argus product team. An Argus callout has been made for the UNICORE Services environment. This is available for EMI 1.

The UNICORE product team contributed to and participated in the establishment of the common SAML profile in order to proceed with the common attribute issuing authority (in this case VOMS-SAML) over the three middleware stacks.

The evaluation of opensaml as a replacement of the samly2 library for UNICORE regarding missing features and blocking bugs was made [R34].

The current decision is to not replace the samly2 library for now.

In order to provide support for short-lived certificates, a list of required changes in the server-side code has been completed. The detailed results can be found at [R35].

It was found that no changes will be needed to the server side. The changes to the client identified and the coordination of their implementation in components managed by other Product Teams is still to be started.

3.9.6 CESNET Security Product Team

The CESNET Security Product Team maintained the delegation and MyProxy [R9] code as planned. Participation in the GSI/delegation group has resulted in no major work requested yet on the delegation tool.

4. SECURITY AREA WORK PLAN

This section gives the work plans of the Security Area in order to attempt to achieve the prescribed technical objectives from DNA1.3.2. The subsections below follow the technical objectives, giving a precise quotation of the objective (with a reference to the numbering scheme in DNA1.3.2), broader description and then the work plans of the individual product team or activity group. Some of the technical objectives persist from the previous deliverable DNA1.3.1 and have been re-stated where required.

Where appropriate, the JRA1 key performance indicators addressed by the objective are given. These are (from the EMI DoW [R39]):

- KJRA1.1: Number of adopted open standard interfaces.
- KJRA1.2: Number of interoperable interface usage.
- KJRA1.3: Number of reduced lines of code.
- KJRA1.4: Number of reduced released products.

The Security Area GANTT chart is available at [R37]. It illustrates the start and finish dates of the Security technical objectives and their sub-tasks. Dependencies between sub-tasks, where relevant, are also included.

4.1. EVOLUTION OF EMI COMPONENTS

This overall technical objective (DNA1.3.2 ref: X16) is stated as "Evolve EMI components to meet specific user requests".

The components affected by this work are All EMI Security Area components, taken from DNA1.3.1[1]: update-crls, nordugridmap, arcproxy, VOMS, VOMS-Admin, Trustmanager, Util-Java, LCAS, LCMAPS, LCMAPS-plugins-c-pep, gLExec, Hydra, Delegation Java, SLCS, org.glite.security.gss, org.glite.security.proxyrenewal, org.gridsite, Argus, Argus-EES, UNICORE {Gateway, XUUDB, UVOS, Services Environment}.

Risks: There are no major risks foreseen with this technical objective. The user requests will arrive through the approved channels and be dealt with according to their severity and priority. This is a normal activity for all product teams.

This work does not directly address any JRA1 KPIs.

4.1.1 Hydra

Hydra will respond to properly submitted and described user requests and bugs. This is a continuous process, starting on M13 and finishing on M36.

4.1.2 Trustmanager/Util-java

Trustmanager will respond to properly submitted and described user requests and bugs. As trustmanager will be subsumed into the new common authentication library and util-java has been factored away, there will only be effort within the constraints of the personnel. This is a continuous process, starting on M13 and finishing on M36.

[1] Component names alignment to follow DNA1.3.2 convention will be done in year 2. This applies to all Security Area year 2 technical objectives

4.1.3 Argus EES

The Argus Execution Environment Service (EES) open-nebula plug-in will be adapted according to input from users. This work is expected to take 1 person month but the start date is unknown.

4.1.4 VOMS-Admin

VOMS-Admin will implement the missing features of VOMRS [R5] into VOMS-Admin in order to complete the transition to one administrative interface. This work is planned to start in M14 and end in M20.

4.2. IMPROVING USABILITY OF CLIENT TOOLS

This technical objective (DNA1.3.2 ref: X8) is stated as "Improve usability of client tools based on customer feedback". There are sub-objectives stated as: "Better more informative, less contradictory error messages" and "Coherency of commands line parameters".

The affected components are All EMI Security Area components, taken from DNA1.3.1: update-crls, nordugridmap, arcproxy, VOMS, VOMS-Admin, Trustmanager, Util-Java, LCAS, LCMAPS, LCMAPS-plugins-c-pep, gLExec, Hydra, Delegation-Java, SLCS, org.glite.security.gss, org.glite.security.proxyrenewal, org.gridsite, Argus, Argus-EES, UNICORE {Gateway, XUUDB, UVOS, Services Environment}.

Risks: The risks associated to this activity are that it is necessary to receive requests from a wide range of users of all EMI components. Changing error messages without full agreement of the users is dangerous in that it can break higher-level non-Grid "services", for example large shell scripts that may control job submission. Likewise, changing command-line parameters could break similar services that rely on knowledge of the command-line options.

This work does not directly address any JRA1 KPIs.

4.2.1 Hydra

The error messages for Hydra, from either the server or client, can be changed according to the user feedback once the information has been registered. The command-line parameters will be adjusted to agree with the prescribed format (not defined). If there are users requests for changes in error messages and a standard set of command-line parameters are defined, this work can start in M16 and end in M20.

4.2.2 Trustmanager/Util-java

The errors exposed to the user from trustmanager have not had any official requests for improvements. As trustmanager will be subsumed by the common authentication library it is a low priority to assign effort here. It is seen to be better to concentrate on the future work.

4.2.3 Arcproxy

arcproxy will be extended in case the VOMS service functionality is moved to VOMS-Admin, as part of the consolidation plan. Work will start as soon as corresponding changes are implemented in the services and is planned to end in 3 months. The error messages and supported options will be enhanced according to the user feedback once the information has been correctly registered in GGUS. This is a continuous process and will run until M36.

4.3. COMMON SECURITY ATTRIBUTES

The technical objective (DNA1.3.2 ref: S-) is stated as "Agreement on a minimal common set of security attributes to be used in policies". The XACML profile is agreed, modulo the missing information from Data Management and EMI Execution Service and in the EMI year two the general task is to push on with implementation/support for the profile in various services. The obvious first

choice is Argus. Apart from the integration of the Argus authorization system to the compute and data areas of the EMI project, Argus must also be integrated to the UNICORE and ARC stacks. The affected components are Argus, UNICORE Services Environment, ARC HED and A-REX.

The risk in this task is that the missing requirements from the EMI Execution service and Data Management may cause the profile to be re-opened. There is no effort budgeted for starting another round of discussions.

This work addresses KJRA1.1 and KJRA1.2.

4.3.1 Argus support for common XACML profile

The Argus authorization service will implement the final version of the EMI common XACML authorization profile [R37] in order to support the integration with the UNICORE/ARC authorization stacks. The work will include:

- Argus PAP support for multi-profile;
- Argus PAP extension of the simple policy language (attr_1 == attr_2);
- Argus PAP import of raw XACML policies;
- Argus PEP Server support for the common XACML authorization profile.

This work is planned to start in M14 and end in M17.

4.3.2 Argus integration with UNICORE

Argus authorization service will be integrated to UNICORE as a part of the overall objective to have one common authorization service in the EMI stack.

4.3.2.1 PDP in USE

The USE will be updated to use the EMI XACML profile. The deliverable will be an implementation allowing UNICORE to perform an effective authorization using the Argus PDP. This work is dependent on the EMI common XACML profile availability in Argus. This work is planned to start in M15 and be fully complete when able to be tested against the Argus version that contains the common EMI XACML profile (M17).

4.3.2.2 Alternative PDP in USE

An alternative UNICORE pdp (in USE), which uses only the Argus PAP, will be implemented. The deliverable will be an implementation allowing UNICORE to perform an effective authorization using the Argus PAP. This work is dependent on the EMI common XACML profile availability in Argus. This work is planned to start in M16 and be fully complete when able to be tested against the Argus version that contains the common EMI XACML profile.

4.3.3 Argus integration into HED

The HED plug-in for communication with the Argus service will be extended to support the common EMI profile. This also includes work for integration of the plug-in into the ARC A-REX. This work is planned to start in M17 and end in M20. This timeline estimation is based on the estimate of the Argus support for common XACML profile in M17.

4.4. ADHERING TO OPERATING SYSTEM STANDARDS

This objective (DNA1.3.2 ref: X6) is stated as “Adhere to operating system standards for service operation and control regarding configuration, log and temporary file location and service start/status/stop”.

The affected components are all EMI Security Area components, taken from DNA1.3.1: VOMS, Trustmanager, Util-Java, Hydra and Argus.

Risks: The risk foreseen here is that as EMI components are ported to other operating systems, the compilation and production of installable products will become more complex and slow.

This work does not directly address any JRA1 KPIs.

4.4.1 All EMI Security components

The EMI release process, defined by SA2, clearly states that all components in an EMI release should follow the operating system-defined methods for service control. This being the case, any security service released through the EMI process will be checked by the quality group (SA2). There is no need for the EMI Security Area to expend effort in planning specifically for this objective.

4.5. RELEASES ON OTHER PLATFORMS

This objective (DNA1.3.2 ref:X7) is stated as "Port, release and support EMI components on identified platforms (full distribution on SL6 and Debian 6, UI on SL5/32 and latest Ubuntu)". All Security Area components will be required to perform this task and therefore specific planning is not needed.

The affected components are all EMI Security Area components, taken from DNA1.3.1: update-crls, nordugridmap, arcproxy, VOMS, VOMS-Admin, Trustmanager, Util-Java, LCAS, LCMAPS, LCMAPS-plugins-c-pep, gLExec, Hydra, Delegation Java, SLCS, org.glite.security.gss, org.glite.security.proxyrenewal, org.gridsite, Argus, Argus-EES, UNICORE {Gateway, XUUDB, UVOS, Services Environment}. The components listed above will be further developed according to user requirements and released on the listed platforms as well as the current SL5/64.

The risk foreseen in the work for this objective is that, similar to the experience of the release of EMI 1, it will needlessly take longer and tie-up resources that should be used for other development work.

This work does not directly address any JRA1 KPIs.

4.5.1 All EMI Security Components

The Security Area components will be ported by their respective product teams. They will be ported to the required platforms under the direction and schedule of the EMI EMT. The start and end dates of these activities are unknown and to be determined by EMI management above and outside the Security Area.

4.6. OPTIMIZED SEMI-AUTOMATED CONFIGURATION OF SERVICE BACK-ENDS

This objective (DNA1.3.2 ref:X13) is stated as "Provide optimized semi-automated configuration of service backends (e.g. databases) for standard deployment".

The affected components, that deploy databases, are VOMS and Hydra.

This work does not directly address any JRA1 KPIs.

4.6.1 Hydra

The Hydra service is configured using YAIM [R3]. Until there is a request from users to use a configuration other than the current, there are no changes planned to the configuration procedure.

4.6.2 VOMS

The VOMS service is configured using YAIM. Until there is a request from users to use a configuration other than the current, there are no changes planned to the configuration procedure.

4.7. PUBLISH COHERENT GLUE2-BASED VERSION INFORMATION

This objective (DNA1.3.2 ref:X1) is stated as "Publish coherent GLUE2-based version information as part of service description for service discovery and monitoring."

The affected components are All EMI Security Area components, taken from DNA1.3.1, are: VOMS, Hydra, Argus, UNICORE (any service that publishes to the information system). The relevant EMI security services will publish GLUE2-based information when instructed to do so. This work does not directly address any JRA1 KPIs.

4.8. AAI ACTIVITY

This objective (DNA1.3.2 ref:S2) is stated as: "Simplified management of security credentials by reducing the complexity of handling certificates and integrating different security mechanisms like Shibboleth and Kerberos across the EMI stack that allows users to use their own authentication system to access a 'Grid'". As described in the EMI DoW the goal of this activity is to lower the barrier of accessing DCIs using institutional or federated institutional authentication systems and to enable the usage of EMI components and services with other security infrastructures such as Kerberos or Shibboleth. In order to enable this access, a new security service, the Security Token Service (STS) is needed to translate these external credentials into the X.509 credentials needed by most Grid infrastructures. The UNICORE stack will also make some changes to comply with this work. There are no affected EMI components as this is a new development

The risks in this activity include that the majority of the work hinges on the release of the STS. The STS is dependent on the schedule of the Shibboleth/OpenSAML version 3. So far, there are no problems foreseen. Another risk noted is that, apart from the fact that EMI organized a workshop at the first EGI conference for ESFRI projects and national Grid infrastructures, there are still identity federation requirement-gathering exercises still ongoing. Another risk is that the foreseen number of developers is not available for the STS work in case of other tasks being promoted in priority (e.g. porting to other operating systems). This work addresses KJRA1.1 and 1.2 through the adoption of common APIs from Shibboleth/OpenSAML.

4.8.1 Security Token Service

The Security Token Service (STS) implements the service defined by the WS-Trust specification. STS is a Web service that issues security tokens, a collection of claims, for the authenticated clients. As the clients can authenticate to the service using different security token formats, the service can be seen as converting a security token from one format into another. As such the STS is used to bridge different trust domains. Contacts with EUGridPMA [R17] have been established in order to contribute to the necessary policy work. The EMI proposal specifically mentions obtaining X.509 based security token from Shibboleth-based AAI federations and Kerberos.

The current plan is that the STS will be implemented on top of the upcoming Shibboleth IdP version 3 and OpenSAML3 implementations. The IdP version 3 will provide support for SOAP binding and delegation: the SAML assertion will targeted to a service other than the requestor. The advantage of re-using the Shibboleth / OpenSAML3 code base is twofold: 1) it allows the re-use non-trivial webservice libraries and 2) it allows to "leverage" the STS from the beginning against the codebase of the most used AAI system in Europe. In addition, this service will exploit EMI common authentication library.

4.8.1.1 Profile revision

The WS-Trust profile will be revised for STS. This work is planned to start and end in M14.

4.8.1.2 Study of IdP API

The IdP API will be studied from the point of view of credential management. The result will be documentation of usage of the Enhanced Client or Proxy (ECP) profile within Shibboleth 2.x. This work is planned to start in M14 and finish in M17.

4.8.1.3 Profile handler

Work will start on the profile handler in M16 (once the IdP APIs are stable).

4.8.1.4 Initial STS version

The initial STS version will support client authentication by a SAML2 token in order to issue an X.509 token. The development is currently waiting for the Shibboleth/OpenSAML version 3 to be finished, which is scheduled for Fall 2011. The development depends on that milestone and, with the current estimates of the Shibboleth/OpenSAML version 3 schedule, can be provided in March 2012. Start date M16, end date M22. This development schedule is based on the availability of two developers to work on the STS.

4.8.1.5 STS Release

The testing, documentation and finally certification depends on the schedule of the previous task. If it meets the schedule above, this subtask can be finished in June 2012. Start date M16, end date M25.

4.8.2 Support for short lived certificates in UNICORE

The UNICORE stack needs to add some functionality (as described below) in order to support the proposed AAI solution. The following sub-tasks depend on AAI work performed by the dedicated task force in the Security Area. These actions are speculative and can be modified according to the final results of the task force. The components affected in this work are: UNICORE client and UNICORE Service Environment.

4.8.2.1 UNICORE STS requirements

The identification of requirements for UNICORE client side tools for integration with STS and AAI in general. The result (deliverable) of this work will be a list of requirements in a form of a detailed list of RfCs. This work can start once an STS prototype is available in M22 and will last for one month.

4.8.2.2 UNICORE STS client-side library

The development of a STS/AAI client-side library for UNICORE, useful for both UNICORE HiLA and UNICORE Client (URC will use this library as well, but outside the EMI project). This work needs to be performed, using common code, with other Java-based client software. It is noted that the majority of the Java-based client stack is in UNICORE. The result of this work will be the library itself. This work is planned to start once the STS is available in M22 and last fully into the year 3 of the project.

4.9. COMMON AUTHENTICATION LIBRARIES

This objective (DNA1.3.2 ref:S3) is stated as: “Provide common authentication libraries supporting X.509 and optionally SAML.” A standard solution of a common set of authentication (AuthN) libraries will be provided across the three middleware stacks. Once these libraries are available, the duplicate AuthN systems and libraries will be removed and the standard common set of AuthN libraries will be used.

As the APIs for the common authentication libraries have been agreed, the work plan for the second year of the EMI project is mainly implementation. There are no directly affected EMI components in the implementation stage, except for trustmanager and Util-java that will be subsumed.

The risk in this work is that in order to meet a schedule that will allow adoption of the library by the other EMI components, the effort will have to be ring-fenced. Another risk is that the conditions needed for the team to write the C library have not been clarified by the project management.

This addresses KJRA1.2 in that a common authentication interface will be provided for all EMI components.

4.9.1 Java library

The UNICORE Security product team anticipates writing the Java version of the common authentication library.

4.9.1.1 Java implementation

The UNICORE Security product team will take part in the implementation of the Java library. The work is planned to start in M14 and last until M22.

4.9.1.2 Adoption of Java library

This is work to adopt the usage of the Java library in UNICORE. This work is planned to start when the library is available (M22) and last into the year 3 of the project.

4.9.2 C Library

A part of the gLite security product team has been identified to write the C version of the common authentication library. As the magnitude and scope of this work was unforeseen at the start of the EMI project, the conditions for performing this work still need to be clarified by the project management.

4.9.3 C++ Library

The ARC Security product team is identified to write the C++ version of the common authentication library.

4.9.3.1 C++ Implementation

The implementation work is planned to start in M14 and last until M22. Presently, it is not decided if the C++ library will be implemented on top of the C version or will use an independent code-base. After this decision is taken the plans may be adapted.

4.9.3.2 Adoption of C++ library

The adoption of the C++ version of the common authentication libraries in the ARC security components will happen as continuous process along with implementation and is planned to end four months after development of library is completed, in M26. There is no information about adoption of common C++ authentication library in other EMI components.

4.10. COMMON ATTRIBUTE AUTHORITY

This objective (DNA1.3.2 ref:S4) is stated as: “Agreement and full support for a common single X.509 and SAML-based Attribute Authority Service integrated with all EMI components.” and “Implementation of the EMI SAML profile all over the middleware stack.” It is foreseen to have a common attribute authority that issues attributes to X.509 proxies or to SAML assertions that follow a common profile. The target to use a common attribute issuing authority (in this case VOMS-SAML) over the three middleware stacks is established. In order to achieve this target, an agreement on common set of SAML authorization attributes was planned and delivered by EMI the SAML group in the M4.

The affected components are VOMS-SAML, UNICORE UVOS. There are no risks seen for this work in that the SAML profile is already agreed (except for the EMI Execution service and Data Management risk).

This addresses KJRA1.1 and KJRA1.2 in that a common attribute authority for all EMI components will be provided and a standard (SAML) will be used.

4.10.1 VOMS

The VOMS service is naturally the first service to be worked on in order to have a common attribute authority.

4.10.1.1 SAML support in VOMS-SAML

The VOMS-SAML attribute authority (the VOMS-Admin part) will implement the final version of the EMI VO attribute SAML profile [R38]. This work is planned to start in M14 and last until M16.

4.10.1.2 Third-party SAML in VOMS-Admin

VOMS will be developed to accept third-party SAML requests. This work in planned to start in M14 and end in M24.

4.10.2 UNICORE

In order to use the common attribute authority the UNICORE Security product team will investigate the following points for interoperability with VOMS. This is related to the possibility to use VOMS as a replacement of UNICORE UVOS.

4.10.2.1 EMI SAML profile in UNICORE

Implementation of the EMI SAML profile in UNICORE Services Environment and will consist of a deliverable of an implementation allowing for consumption of SAML assertions issued by VOMS, and usage of them to provide attributes for the UNICORE authorization stack.

It is important to note that this is dependent on the implementation of the aforementioned SAML profile in VOMS-SAML.

The anticipated start of this work is M14 and will end at least one month after the availability of the new, common SAML profile in VOMS-SAML. This is anticipated in M16.

4.10.2.2 UNICORE Client-side tools for push mode AuthZ

The UNICORE Client-side tools with the push mode authorization are needed. These will be in the form of extensions of the UCC and HiLA clients using a common library, allowing querying VOMS for attribute assertions and sending them with a request to a UNICORE server. In addition this common library will be integrated with URC outside the EMI project. This work is dependent on the work above, the EMI SAML profile in UNICORE. This work will start on M16 and end on M18.

4.10.2.3 Analysis of UNICORE UVOS vs. VOMS

An analysis of the feature-wise incompatibilities between UNICORE UVOS and VOMS with respect to replacing UNICORE UVOS with VOMS will be made. The result of this analysis will be a list of feature requests for VOMS, with assessment of their impact factor. This work is also dependent on the EMI SAML profile in UNICORE. At M13 an initial, theoretical draft will be provided, a detailed evaluation will be performed after VOMS and UNICORE are updated to use EMI SAML Profile. This work will start in M14 and will end one month after the availability of VOMS-SAML.

4.10.2.4 Testing of push mode

The push mode implementation for client and server will be tested with VOMS-SAML. The result will be a set of test results, possibly including some new RfCs. This is dependent on the completion of the client-side tools for using the push mode. This testing will start on M19, or shortly after the availability of VOMS-SAML.

4.11. UNIVERSAL EMI SAML PROFILE

This objective (DNA1.3.2 ref:X11) is stated as: “Implementation of the EMI SAML profile all over the middleware stack”. The work for this objective may only start after the SAML profile is ready and

integrated into VOMS-SAML. The affected components in EMI year 2 are the UNICORE UVOS, VOMS-SAML and Argus. There are no risks foreseen for this work. This work addresses KJRA1.1 as SAML will be the adopted open standard.

4.11.1 VOMS-SAML integration to UNICORE

The VOMS-SAML attribute authority will be integrated into the UNICORE authorization stack by the VOMS and UNICORE Security product teams.

4.11.1.1 VOMS-Admin

It will be verified that VOMS-Admin implements all the VO management functionality needed to act as a UNICORE UVOS replacement. This work is planned to start once the EMI SAML profile support in VOMS-SAML is finished in M16 and last until M20.

4.11.1.2 UNICORE UVOS Clients

Also the existing UNICORE UVOS clients must be tested and possibly adapted to request attributes from VOMS-SAML. This work is planned to start once the VOMS-Admin verification (above) is finished in M20 and end in M24.

4.11.2 VOMS-SAML integration to Argus

Currently Argus renders authorization decisions based on attributes typically coming from a user X.509 proxy certificate containing VOMS extensions. Argus will be extended to gather information regarding a principal from SAML assertions. The possible support of SAML authentication assertions and the trust model adopted across the services will be investigated. This work is planned to start once the EMI SAML profile support in VOMS-SAML is finished in M16 and last until M24.

4.12. CONSOLIDATION

This objective (DNA1.3.2 ref:S1,S5) is stated as: “Plan for substantial simplification and reduction in the number of Security Area CLIs libraries, internal components and services: Security Area consolidation plan.”

This work will address KJRA1.4 as a reduction in the number of deployed components should be the result.

4.12.1 Convergence of LCAS, LCMAPS and EES

There will be a convergence, by the gLite security product team, of the underlying code used by LCAS, LCMAPS and EES. This work is planned to start in M15 and last until M21.

4.12.2 PAM integration

PAM modules will be written and integrated by the gLite security product team, where relevant. These include the basic Argus PAM module and the gLExec interface to PAM. The gLExec interface will require a preliminary requirement study. This work is planned to start in M15 and end in M18.

4.13. ENCRYPTED STORAGE

This objective (DNA1.3.2 ref:S6) is stated as: “Provide a transparent solution for encrypted storage utilizing ordinary EMI SEs”. This objective is relatively simple: to provide the services necessary to protect data and user identities on a “Grid”. These services are requested by user groups and NGIs that have stringent data protection requirements.

The affected components are the pseudo-anonymity (pseudonymity) service and the key storage service (Hydra) of the gLite-security product team.

The risk associated to the tasks in this objective is that the developers working on these services are diverted by other, high priority, tasks.

This work does not directly address any JRA1 KPIs.

4.13.1 Pseudonymity

The pseudonymity system is used to improve user privacy by hiding the real identity of a Grid user behind a pseudo-anonymous identity. The system consists of the pseudonymity service, the client tool, an online CA for issuing the pseudonymous certificates and an attribute authority to maintain the users' attributes. The service and the client tool are implemented in this task, supporting CMC and CMP protocols for interaction with the online CA. Currently, in accordance with the EMI project strategy, the only supported attribute authority is VOMS-SAML. In addition to VOMS-SAML, the pseudonymity service also exploits EMI common authentication library.

4.13.1.1 Removal of gLite SLCS

The Pseudonymity service will be re-factored, based on the previous implementation from the EGEE project, but without dependencies on SLCS or any other unsupported or non-standard components. The task also contains the testing, documentation and finally certification of the service. The task is scheduled to be ready by M16. It is an ongoing activity.

4.13.1.2 Pseudonymity Client tool

Implementation of a new Pseudonymity Client tool will be based on the previous implementation from the EGEE project but without dependencies on the SLCS client or any unsupported or non-standard components. The task also contains the testing, documentation and finally certification of the component. The task is scheduled to be ready by M16. Ongoing.

4.13.2 Encrypted data storage

The Hydra key storage service will be worked on in order to bring it up to the EMI release standards. This work will start in M14 and end in M18.

4.14. GLOBUS GSI REMOVAL

This objective (DNA1.3.2 ref:X12) is stated as: “The legacy Globus security infrastructure (GSI) will be replaced with a common security solution based on TLS/SSL and EMI delegation method”. An overall strategy to remove the Globus Security Infrastructure (GSI) protocol which functions as an enhanced SSL protocol (httpg) is outlined in the EMI DoW. This is due to the fact that these functions are replaceable by standard SSL/TLS readily available in target operating systems. Since the move to pure SSL/TLS is not compatible with the legacy GSI, however, the transition must be carefully planned such that operations are not impacted.

As reported above, the GSI-free VOMS has been released. The major work for EMI year 2 is the still agreement and implementation of the common delegation solution. This is handled by the “Common Delegation Group” and reported below.

This work addresses KJRA1.1 as a move away from the proprietary Globus GSI to TLS/SSL is the overall target.

4.15. COMMON DELEGATION METHOD

This objective (DNA1.3.2 ref:X3) is stated as: “Agreement on common EMI delegation method”. This is part of the process to remove the Globus GSI from the EMI stack, as described above. For delegation, the strategy will be for services to move to a separate delegation service or port type rather than rely on the GSI-dependent libraries.

The EMI Security Area components affected are gridsite (delegation) and possibly delegation-java.

A risk involved with this activity is the uncertainty on the requirements and schedule of the EMI Execution Service. Another risk is that the CESNET product team, responsible for gridsite integration to the EMI stack, does not have the resources and mandate for large changes to gridsite. An “EMI” branch of gridsite needs very careful consideration.

This work addresses KJRA1.1 as a move away from the proprietary Globus GSI to TLS/SSL is the overall target.

4.15.1 gridsite delegation

The work planned for this group in EMI year 2 is to form an OGF group for standardization of the gridsite delegation. This will result in a documented agreement (EMI technical document or OGF experience document) describing the common approach to delegation in M18. This is necessary in order to deliver working SRM systems, in the data area, that uses delegation by M25. The changes to gridsite, mainly due to requirements from the EMI-ES, are expected to be minor. These may be handled by the CESNET Security product team or the original gridsite developer, external to the project.

4.16. DENIAL OF SERVICE PROTECTION

This objective (DNA1.3.2 ref:X10) is stated as: "Introduce minimal DOS protection for EMI services via configurable resource limits."

Affected components are VOMS. Java-based services have resource limits built into the runtime environment.

There are no risks associated to this work.

This work does not directly address any JRA1 KPIs.

4.17. MONITORING PROBES FOR EMI SERVICES

This objective (DNA1.3.2 ref:X4) is stated as: "Provide and support monitoring probes for EMI services (e.g. Nagios)." This objective has come from an EGI requirement.

The services that could be monitored with NAGIOS are: Argus, VOMS, Hydra, STS, Pseudonymity. The Argus authorization service already has a set of simple probes, for LCG, that determine whether the service is alive or not. UNICORE also has a similar set of simple probes for SAM NAGIOS testing.

A risk involved with this work is that the requirement has no descriptive or quantitative substance. There is no description given of what information these probes should return. The experience of the Argus product team shows that simple probes are straightforward. Another risk identified is the question of the testing infrastructure required. Once a properly described set of requirements are received for monitoring probe provision and support, then a more detailed work plan may be created by each product team.

This work does not directly address any JRA1 KPIs.

4.18. INCREASE PERFORMANCE OF EMI SERVICES

This objective (DNA1.3.2 ref:X15) is stated as: "Increase performance of EMI services". This objective has come from an EGI requirement. As the objective has no descriptive or quantitative substance it is difficult to produce a detailed work plan. The only recourse offered would be to plan a program of measuring the (undefined by the requirement) performance of various EMI security services and then forward these results to the customers. Then based on those figures, the customers could point out the areas that need improvement. Assuming that the performance measurements made by the product teams are made on exactly the same infrastructure configuration used by the customers then an improvement plan can be drawn up.

The EMI security services affected are: Argus, VOMS, Hydra, STS, Pseudonymity, ARC and the UNICORE security stack.

The risks observed for this work is that the requirement has no description of the EMI security services that have a performance problem with quantitative targets set. The plan, based on the

requirement, would risk developer time in replicating a deployment scenario for a service, testing the service performance levels without targets predefined.

This work does not directly address any JRA1 KPIs.

4.18.1 UNICORE

The UNICORE Security product team has received user requirements, independent from the requirement above, on service performance.

4.18.1.1 Optimization of UNICORE security

The performance of the UNICORE security stack (UNICORE Service Environment) will be optimized with the usage of communication sessions and credentials storage. The deliverable will be a working implementation of the UNICORE security stack with tests results showing performance improvements. This task is not anticipated to take very long but will take a lower priority to maintenance and unforeseen events. This work is planned to start on M18 and last until M22.

4.18.1.2 Team work support in UNICORE

One of the common requests from UNICORE end-users: to share resources with their co-workers or teams they work in. In this context, “resources” refer to: files, "atomic" jobs and work-flows all represented by WSRF resources in UNICORE. For example to grant others the permission to control (pause, interact with, kill, get results) a work-flow that a user has submitted.

There will be an investigation towards better support for team work in the UNICORE stack. This task includes the sharing of UNICORE resources between small, ad-hoc created groups of users. The deliverable will be a document describing the possible solutions along with analysis of advantages, disadvantages and effort required to implement and maintain. Subsequently a list of RfCs will be generated. This work is planned to start in M14 and last until M20.

5. CONCLUSIONS

This document has described the status of the work performed by the EMI Security Area in the first year of the project. The work plan for the first year of the project has been described DJRA1.3.1. The status section generally follows the format of the first year work plan and also gives reasons if the work has not progressed according to the schedule.

The work plan for EMI Security Area in the second year of the EMI project follows the relevant objectives as described in DNA1.3.2 and is based on the best information at this time. The objectives are described in greater detail and the affected components and their product teams that will perform the necessary work are listed where appropriate. Any risks associated to the work for each objective are described and the JRA1 KPIs addressed are given. The next update of this document will be DJRA1.3.3 (M24).