EUROPEAN MIDDLEWARE INITIATIVE

DJRA1.3.1 – SECURITY AREA WORK PLAN AND STATUS REPORT

EU DELIVERABLE: D5.3.1

Document identifier:	**EMI-DJRA1.3.1-1277566-Security_Area_Work_Plan-v1.0.doc**
Date:	**31/07/2010**
Activity:	**JRA1**
Lead Partner:	**UH**
Document status:	**Final**
Document link:	**http://cdsweb.cern.ch/record/1277566**

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. The status report at M03 will cover the state-of-the art while the work plan at M36 will provide recommendations for further work.

Delivery Slip

	Name	Partner / Activity	Date	Signature
From	John White	UH / JRA1	01/09/2010	
Reviewed by	Florido Paganelli, Maria Alandes Pradillo Jozefs cernak	LU / SA1, CERN / SA1 UPJS/SA2	14/10/2010 26/10/2010 26/10/2010	
Approved by	PEB		17/12/2010	

Document Log

Issue	Date	Comment	Author / Partner
0.1	27/07/2010	Version 0.1 sent to security group	JohnWhite/UH
0.2	28/07/2010	Version 0.2 sent to security group	JohnWhite/UH
0.3	30/07/2010	Version 0.3 sent to security group	JohnWhite/UH
0.4	02/08/10	Version delivered for review.	JohnWhite/UH
		Review received on 14/10/2010 and 26/10/2010	
0.5	3.11.10	Version 0.5 incorporates changes.	JohnWhite/UH
0.7	15/11/2010	Further changes after more reviewers comments	JohnWhite/UH
0.8	15/12/2010	Added schedule table	JohnWhite/UH
1.0	17/12/2010	Public release v. 1.0 approved by PEB	Alberto Di Meglio/CERN

Document Change Record

Issue	Item	Reason for Change

TABLE OF CONTENTS

1. INTRODUCTION

1.1. PURPOSE

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 state-of-the art in place of the achievements of the past 12 months.

1.2. DOCUMENT ORGANISATION

This document describes the state of the art of components within the security area of EMI. Then the work plan for the security area in the first year of the EMI project. This work plan is split into two sections. The first section on harmonization describes work that is aimed to rationalize, reduce or converge the security components. The second section on evolution describes new development work planned.

1.3. REFERENCES

R1	Chemomentum Project. http://www.chemomentum.org
R2	MyProxy Credential Management Service. http://grid.ncsa.illinois.edu/myproxy
R3	Open Middleware Infrastructure Institute. http://omii-europe.org
R4	Open Science Grid. http://www.opensciencegrid.org
R5	The Globus Project. http://www.globus.org
R6	UNICORE Project. http://www.unicore.eu
R7	YAIM Ain't an Installation Manager. http://yaim.info
R8	gLite CREAM devlopment team. XACML Grid Computing Element Authorization Profile, 2010. https://edms.cern.ch/document/1078881/1
R9	IGE Project. http://www.ige-project.eu
R10	OMII Europe Project. http://www.omii-europe.org
R11	AAI Workshop. https://www.egi.eu/indico/sessionDisplay.py?sessionId=11&confId=48

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
CREAM	Computing Resource Execution and Management
ETD	Explicit Trust Delegation
GACL	Grid Access Control Language
GSI	Globus Security Infrastructure
HED	Hosting Environment Daemon
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
SAML	Security Assertion Markup Language
SCAS	Site Central Authorization Service
SLCS	Short Lived Certificate Service
SPL	Simplified Policy Language
UVOS	UNICORE Virtual Organization System
VOMS	Virtual Organization Management System
XACML	Extensible Access Control Markup Language

2. EXECUTIVE SUMMARY

The Security Work Plan document gives the work plan for the first year of the EMI project in work other than regular maintenance and bug-fixing of components.

The state of the art section describes the security infrastructure and components of the three middleware stacks in EMI. This includes the overall philosophy of each stack and the security tokens used.

The harmonization section outlines the work for the first year, organized by EMI product team. The harmonization section gives a description of the work that rationalizes components and roll out common profiles. The main points are as follows. 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. A common set of authentication libraries will reduce redundancy throughout the middleware and provide a uniform response from all components that will use them. In order to further reduce redundancy and provide a uniform authorization policy management system, Argus will be used as the common authorization system.

The evolution section contains work that is more speculative and reliant on client requests. Some of the work described is still dependent on the outcome of future EMI milestones. In general, the evolution section looks towards the Cloud computing interfaces in the form of the EES for Argus and the Hydra encrypted key storage system. Another general topic is the work necessary to integrate with alternative token services such as SLCS or STS (and the like). This work will start the general changes necessary to ease the use of Grids for users. Another development work is the exploration of moving away from the specifically written executable for user account switching to standard operating system components. This will ease the integration, to other operating system flavours, of the most widely deployed Grid node type.

3. STATE OF THE ART

The gLite and Advanced Resource Connector (ARC) security models are based on X.509 proxy credentials with added assertions in the form of Attribute Certificates added by the Virtual Organization Management Service (VOMS). In addition to VOMS attribute certificates and proxy credentials ARC security libraries are also capable handling other type of embedded policies including Security Assertion Markup Language (SAML) assertions.

As mentioned above, the system is based on a PKI infrastructure using X.509 certificate/private key pairs to identify Grid users. These credentials are obtained by the user from their home (national) certificate authority and are passed to the Grid system(s) in the form of a proxy certificate. For security reasons, proxies are not directly copied within the Grid infrastructure; rather they are transferred via a specific delegation mechanism.

The affiliation of a Grid user to their research community is expressed through the concept of Virtual Organizations (VOs) and the groups that the user belongs to and the roles they perform are expressed through Attribute Certificates (ACs). These ACs are added to credentials through a user-initiated request to the VOMS server.

The gLite security system is a collection of components and libraries that act to permit use of and protect the Grid infrastructure from misuse. A Grid user submitting a job presents their proxy certificate with the AC added by VOMS to the relevant Grid service, such as gLite Workload Management System (WMS), Computing Resource Execution and Management (CREAM) or Data Management, where they are authenticated via local and VOMS libraries and authorized locally. The proxy certificates are authenticated via diverse systems according to the service being contacted.

In the case of the gLite Workload Management System (WMS) the authentication of the X.509 proxies is handled by the Apache HTTP server through Grid Site plugins (mod ssl, mod gridsite). The Authorization is performed by Gridsite through the use of Grid Access Control Language (GACL).

As Grid jobs can typically last for many days, once delays in the batch system are taken into account and proxies should be valid for approximately 24 hours, there is a credential renewal mechanism. This renewal system is based on the MyProxy [2] system, VOMS and the proxy-renewal tool. Proxies are stored in MyProxy, retrieved by the renewal service and presented to VOMS for the addition of the AC. The renewed proxy is subsequently delegated to the required service and re-stored in MyProxy. This procedure is used in gLite only.

The delegation of proxy credentials is a multi-stage process involving certificate requests and signings. This delegation process uses either gridsite delegation or delegation-java for C/C++ and Java respectively.

Proxy credentials that are delegated to the CREAM computing element are authenticated by gLite Trust- manager and the authorization is performed by internal classes derived from the deprecated gLite Java Authorization Framework component. CREAM interacts with the Local Resource Management System (LRMS) and must therefore have a mechanism to map a X.509 Grid identity to a user id in the local file system. This mapping capability is provided by LCAS/LCMAPS, and gLExec. LCAS/LCMAPS checks that the proxy credential is authorized and consults a mapping resource to determine the X.509 to user id mapping; glexec subsequently performs a root-priviliged setuid operation to change to the specified local user id for use in the LRMS.

Argus, a site-central authorization system, is designed to render consistent authorization decisions for distributed services. The authorization policies are authored and maintained, in eXtensible Access Control Markup Language (XACML), by the Policy Administration Point (PAP) component in the service. The authored policies are evaluated by the Policy Decision Point (PDP). The data provided for evaluation against policies is consistent (in form and definition) and this is provided by the Policy Enforcement Point (PEP). The Argus authorization system is integrated into the gLite deployment in order to authorize and provide identical mappings of X.509 proxy credentials to local user ids over

multiple, separate worker nodes. Argus is in the process of being integrated into the CREAM deployment and plans for WMS and Data Management are underway.

There is another gLite authorization service: the Site Central Authorization Service (SCAS). This service uses existing components, LCAS and LCMAPS, at the service side and uses a SSL secured saml2- xacml2 WS-interface. This service was developed in collaboration with Open Science Grid [4] (OSG) and Globus [5] and is interoperable with the OSG GUMS service. The main deployment focus is to facilitate a centralized authorization and mapping service to work at the scale of current sites.

In the WS-based ARC middleware stack the central part is the Hosting Environment Daemon (HED). HED is a container for all other functional components of ARC, both on the server and client side. HED is also a development framework which provides powerful tools for Grid security and communication tasks. The HED security system has two main capabilities:

- Security capability embedded in the hosting environment.
- Security capability implemented as plug-ins which can be accessed by the hosting environment and Grid applications.

HED contains a framework for implementing and enforcing authentication and authorization. Each Message Chain Component (MCC) or Service has a common interface for implementing various authentication and authorization functionalities. This functionality is implemented via pluggable components called Security Handlers (SecHandler). The SecHandler components provide methods for processing messages traveling through Message Chains of the HED. Each MCC or Service implements a queue each of SecHandlers for incoming and outgoing messages. All SecHandler components attached to a queue are executed sequentially and if any of them fails, the message processing fails as well.

In the basic authorization model, ARC services support a simple X.509 certificate subject (Distinguished Name) mapping to UNIX users through the grid-mapfile mechanism. For advanced authorization, the majority of ARC services are capable of acting purely on the Grid identity of the connecting client without relying on local identities. In addition, VOMS and general VO membership (through external information gathering tools) other identification mechanisms are supported. In addition to access-level authorization, many services make use of the client Grid identities internally to provide fine-grained access control through GACL.

UNICORE [6] on the other hand adopts a security model that does not require proxy certificates, relying on full X.509 certificates for authentication and signed SAML assertions for trust delegation.

UNICORE authenticates communication peers by usage of client-authenticated TLS connections. Trust delegation is achieved by usage of Explicit Trust Delegation (ETD). ETD uses two principal roles that are assigned to entities such as real users and software agents when using the UNICORE middleware:

- The consignor is the entity which actually sends a request to the UNICORE service either directly or through the Gateway.
- The user is an entity on whose behalf the request is performed. We can use the analogy to the UNIX effective user identifier of a process.

Currently the roles are identified by the X.509 certificate or the DN of the certificate. A certificate is required to identify the entity as the entities carrying the role can either establish an authenticated TLS connection (the consignor), sign requests or issue signed ETD assertions (the user).

The ETD allows the user to certify that a given consignor can act on their behalf. The assertions of ETD may also be chained. A consignor must present a valid ETD assertion (or assertions chain) issued by a user when the consignor want to perform a request on behalf of the user. The UNICORE Virtual Organizations System (UVOS) provides a possibility to also use other credentials to log into a Grid, but this is achieved by mapping those credentials to the X.509 certificate which are used to identify the entity to the UNICORE middleware.

The majority of the security data in UNICORE is encoded using the SAML 2.0 format. The role of SAML in UNICORE is standard in the authorization area: SAML is used to query (usually the UVOS server) for the attributes of the user and subsequently encode them. SAML, due to its universal format, is used by UNICORE to carry also UNICORE-specific security data such as the trust delegation assertions.

In UNICORE 6 authorization is attribute-centric. Using flexible users and attribute databases (such as XUUDB and UVOS), administrators can manage users and their attributes. The UNICORE server can be configured to use several attribute sources with various merging algorithms. The access policy file for the UNICORE server is stored in XACML format and is rarely modified as typical access restrictions (e.g. user banning) are achieved by changing the user role attribute. The XACML policy may be changed to achieve advanced results, e.g. to allow only for read-only access or permit users only in a specific time frame.

The concept of non-repudiation in UNICORE 6 is achieved by creating a digital signature of the request by the consignor. The signing process entails a significant performance penalty. Therefore the UNICORE 6 server uses a special policy which dictates which operations must be signed (e.g. the operation used to submit a new job). Some simple operations (such as getting a job status) need not be signed and in those cases non-repudiation is not guaranteed.

4. WORKPLAN

The work plan for the security area follows the technical objectives given in EMI document DNA1.3.1. The workplan from each Product Team (PT) presented here focuses on the first year of the EMI project.

The activities in this workplan can be classified under the two main strategic directions of the project:

- Harmonization. The overall goal of harmonization is to converge the three middleware stacks through the implementation of standard solutions, removal of duplications and simplification of usage and maintenance.
- Evolution. New client-driven development that addresses requirements of Grid and Cloud user communities anticipates change through pro-active maintenance or adapts to changes in technologies.

The Product Teams will provide harmonization and evolution security best practices that will be incorporated into EMI (SA) documents. Therefore this material will not be discussed in detail in this work plan.

4.1. HARMONIZATION

The first year plans of the security area for harmonization activities are given here. The projected dates, generally given on the scale of EMI project months, are approximate. This is due to the fact that in the early stages of this project these work actions depend also on other project activities. Some of these activities lie outside of one work area and, given that the workplan documents and technical overview are delivered simultaneously, are not yet precisely scheduled. The following sections are given in order of product teams that are, by definition, responsible for development and testing of their own work.

4.1.1 ARC Security Utils Product Team

The harmonization work in the first year of the EMI project for the ARC Security Utils that consist of the components update-crls, nordugridmap and arcproxy are as follows. The phase-out of “update-crls” from ARC deployment and its replacement with “fetch-crl”, this will be ready for the EMI-1 release. The “nordugridmap” should be made the base for a common gridmap file generator utility. The arcproxy utility should be introduced as the general purpose EMI proxy creation and manipulation tool. These developments are foreseen for the first year of the EMI project.

4.1.2 Argus Product Team

The Argus work plan can be referenced at:

https://twiki.cern.ch/twiki/bin/view/EMI/ArgusPTWorkplan

In the first year of the EMI project, the Argus 1.2 release is planned. This should be in time for EMI Release 0. The Argus 1.2 release was planned for the end of project month 3 (actually released in month 6) and consists of many minor improvements based on the feedback received during the pilot phase of the deployment:

- Security
  - Implement the required security recommendations made by PSNC Security Team.
  - Policy Enforcement Point (PEP) daemon mapping obligation handler.

  - Implement a consistent FQAN/DN based user mapping strategy.
  - Add support for DN based group account mapping in group-mapfile.
  - Add preferDNForGroupName configuration property.
- XACML profiles.
  - Finalize the XACML Grid CE profile [8] v.1.0 for CREAM.
  - Update Policy Information Point (PIP) to support the XACML Grid CE (CREAM) profile.
- PEP client library.
  - Release the PEP-Java client library, with the eventual modifications required for the CE.
  - profile and CREAM (feedback required).
- Policy Administration Point (PAP) admin.
  - Add the pap-admin add-policy -obligation <obligation-id> parameter.

For the remaining part of the first year of the EMI project the main goal for the Argus Product Team is to add the functionality required by other components and middleware stacks (CREAM, data management, ARC, UNICORE) in order to allow the integration of Argus. These include:

- Update the XACML profiles to support other use cases.
- Clustered obligation handlers for the PEP daemon (high availability, load balancing).
- Policy repository on a Relational DataBase Management System (RDBMS) with initial support for mysql.
- Improved PAP CLI response time.
- YAIM [7] support for generic remote PAPs configuration.
- Temporal attributes support in Simplified Policy Language (SPL) policies, to enable policies like “this principal is allowed to do this action on this resource only at night on weekdays”.
- Web based policy search/management interface (may be further postponed the next year).

4.1.3 VOMS Product Team

For the first year of the EMI project the harmonization plans for the Virtual Organization Management Service (VOMS) and its administrative interface, VOMS-Admin, will follow those set out in the DoW. In order to harmonize the three middleware stacks the long-term strategy is to use a common SAML assertion source and subsequently a common SAML profile. In order to be fully compatible, a common SAML-enabled VOMS version (VOMS-SAML) version will be deployed. The VOMS-SAML was first developed in conjunction with the OMII-Europe and is now supported by gLite and ARC. The VOMS-SAML integration will proceed once the common SAML profile within the middleware is agreed upon.

The first-year plans for VOMS and VOMS-Admin are as follows. Continuing from the EGEE-III programme of work and overall strategy, continued in EMI, the removal of the Globus GSI protocol will proceed resulting in a first Globus-free client and server release (VOMS 2.0). Support will be added for external Virtual Organization (VO) membership databases. Initially this consist of support

for the CERN orgdb currently in use by the Large Hadron Collider (LHC) experiments VOs. A REpresentational State Transfer (REST)-ful interface for obtaining X.509 attribute certificates will be provided. These developments will be released by project month 10 and will be ready for inclusion into the EMI Release 1.

There are developments for VOMS/VOMS-Admin that are scheduled for later in the first year of EMI. Some of these developments are dependent on results of the "AAI for DCIs" workshop [R11] and preceding development work. It is planned to merge the VOMS Attributes from Shibboleth (VASH) functionality into VOMS, this will depend on some results from the above-mentioned "AAI for DCIs" workshop. In order to harmonize, especially with the UNICORE middleware stack, it is planned to allow third parties to request VOMS credentials for users and subsequently make provisions to allow some user credentials to be kept private. The above developments are planned to be released, as VOMS-Admin 2.6, by month 12 of the EMI project.

4.1.4 gLite Security Product Team

The following give the first year plans for the gLite security product team that in comprised of the components Trustmanager/Util-java, Delegation, Site Central Authorization Service (SCAS), Local Centre Authorization Service (LCAS)/ Local Credential MAPping Service (LCMAPS), gLExec Hydra, Security Token Service (STS), Short Lived Credential Serviced (SLCS) and Pseudonymity.

Trustmanager/Util-Java. For the Trustmanager and Util-Java, the necessary development work in the first year will be determined by the results of the Common Authentication libraries working group (see section 4.1.7.) that will be available in month 7. Also, for Trustmanager and Util-Java there will be a reorganization into more logical (from the functional point of view) components and plugins and also a more flexible configuration. These will be ready for release by project month 8.

Delegation. For delegation, support for RFC3820 proxies will be added by project month 9. Also an interface to allow configuration options for the resulting proxy by project month 9.

SCAS. The SCAS service is planned to be replaced by Argus and therefore there is no Harmonization or Evolution work planned for this in EMI. Support will be discontinued as soon as practicable.

LCAS/LCMAPS. The LCAS/LCMAPS components, apart from regular maintenance, will work in the first year of the EMI project as follows. As LCAS and LCMAPS form integral parts of other services they must be supported. The Globus Grid Security Infrastructure (GSI) independence work will proceed after the results of the GSI-removal working group, see section 4.1.6. A backwards-compatible API upgrade will be released by EMI-1 (project month 10).

- Control the behavior of the VOMS API. A requirement from the OSG project and other use cases which might involve the disablement of this feature when already verified in a different way.
- Add the ability to use native X.509 structures to use LCAS and LCMAPS. This was a requirement from xrootd and is a key feature to restrict all the Generic Security Services Application Program Interface (GSSAPI) and GSI interactions to the gt4-interface library.

gLExec. For gLExec the main work in the first year of the EMI project is to continue support and maintenance. For development, a rewrite of parts of the code, include logging, parsing of configuration file is necessary and also there are feature requests concerning security checks. The code "auditability" also needs improvement. A "final" gLExec version has been released in project month 7. gLExec will inherent the dependencies from LCMAPS on the run-time installation and build.

Hydra. The Hydra keystore service, used by the Biomedical community, will continue to be supported. In the first year of the EMI project there will be a release for EMI1 that will correct the issues found in the EGEE-III SA3 code reviews by PSNC.

STS. In order that STS will work with all three middleware stacks, the common SAML profile and Common Authentication Libraries must be understood.

4.1.5 UNICORE Security Product Team

In the UNICORE Security product team the plans for the first year of the EMI project are as follows. In order to integrate Argus to UNICORE the policy requirements covering the current default policy must be provided. Also a list of typical UNICORE use-cases for Argus along with a list of relevant authorization attributes will be given and the creation of an Argus callout in the UNICORE XACML-entity will be added. The deliverable will be an available callout and a demonstration of UNICORE/X showing that Argus receives the proper request, and that a valid answer is accepted by the callout. This deliverable is scheduled for EMI project month 8, in time for EMI Release 1.

The general 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 project month 4. This UNICORE deliverable consists of the input to the profile published by the SAML security group (section 4.1.9) and active participation in the profile design.

As a harmonization step, the replacement of the samly2 library with the opensaml2 version is proposed. The evaluation of opensaml as a replacement of samly2 library for UNICORE regarding missing features and blocking bugs will be made. This deliverable will be a statement on the applicability of the changeover and will be delivered in EMI project month 9.

The UNICORE Security Product Team also takes part in the creation of the specification of a detailed list of features and definition of the API for a common authentication library, see section 4.1.7. A UNICORE deliverable to this group's activities is a the features required from the UNICORE side delivered in EMI project month 3. The input to the API definition of the library is planned.

As mentioned before, the projected months given above are very approximate as most of these work actions depend also on other project activities which are not yet precisely scheduled.

The summary of the above work plan is as follows:

- M3: Requirements for the common authentication library identified and delivered.
- M4: UNICORE requirements for SAML attributes profile delivered.
- M8: UNICORE Argus Callout finished.
    - M7: (internal milestone) UNICORE XACML entity updated to use XACML 2 with the herasf library (the same which is used by Argus PDP).
- M9: Applicability of the replacement of the samly2 library with the opensaml2 library investigated and decided.

4.1.6 CESNET Security Product Team

The CESNET Security Product Team does not plan any harmonization work on the products that they maintain. The only possible exception may be that some work on the delegation tool that may be needed in response to requirements from other middleware areas.

4.1.7 GSI Removal

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. A group has been formed, primarily within the Security area, that will determine the effort needed and implications of such a code change. This group also includes members from Data and Workload management areas. Also, contact is planned with the IGE project [R9]. 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. 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. In the first months of the EMI project the GSI group will address the following points:

- Tabulate a "list of effort" to see how much effort and resulting reward to remove GSI from components.
- Understand the implications of moving to OpenSSL 1.0.x.
- Explore the possibility to send a message to the IGE project requesting an implementation of GSI that is compatible with the future OpenSSL versions.
- Requirement on services to move to a separate delegation service or port type rather than rely on the GSI-dependent libraries.

In conclusion, the GSI removal problem needs more discussion across more than one technical area. This plan should be concluded before EMI project month 9.

4.1.8 Common Authentication Libraries

As a part of the harmonization strategy, duplicate authentication (AuthN) systems and libraries will be removed and a standard solution of a common set of authentication libraries provided across the three middleware stacks. It is expected that these libraries should support X.509/TLS which is currently the only authentication mechanism widely used in all stacks. Optionally and SAML authentication support will be added basing on requirements which are to be decided. A "Common Authentication library" group has been formed, consisting of members from each middleware consortium, and will provide:

- A set of requirements on the AuthN common lib API.
- An inventory of existing code.
- An estimate of effort and timelines for producing missing parts.

These points have been addressed in EMI project month 4. Once the direction is clear then the work necessary to write new code or modify existing code can begin. It is expected that a prototype version of these libraries will be available for testing within the first year of the EMI project. Once the Common Authentication libraries are produced, it will become the task of the individual product teams to integrate these libraries into their components. This would imply that the results of this work will not be released even in EMI Release 1.

The tentative schedule of this action is as follows:

- M4: Requirements for the library collected and summary established.

- M6: The library model is decided.
- M8: The need for SAML authentication library is investigated.
- M8: The X.509 library APIs in three languages is finalized.
- M9: Optional updates of the X.509API applied basing on comments received from the relevant product teams.
- M12: The library is fully implemented and available for testing.

4.1.9 Common SAML Profile

SAML assertions are used in production by UNICORE and are seen as a way forward in order to "future-proof" gLite and ARC for client requests. In order to harmonize the three stacks to use a common SAML assertion source the long-term strategy is to deploy a common VOMS-SAML version and a common SAML profile. This was first developed in conjunction with the OMII-Europe [R10] and is now deployed in gLite and ARC. Another harmonization move can be made by moving all three stacks to a common version of the opensaml2 library. Particular attention is taken to the current suitability of VOMS-SAML for UNICORE with regards to fundamental questions in the VO administration and push/pull assertion model.

The SAML working group has been formed. The first milestone for this group will be a document that explains the following points:

- The OMII-Chemomentum profile document can be used as a starting point for a common SAML profile.
- The amount of work, in UNICORE and VOMS-SAML to update to a new SAML profile, to be determined.
- Coordinate the move of all middleware stacks to the opensaml2 library.
- Gather requirements from LHC Computing Grid (LCG), through EGI, for SAML usage with respect to the granularity of authorization decisions.
- Investigate SAML delegation as a means of restriction of privilege of security tokens.
- Plan the replacement of UNICORE Virtual Organisations System (UVOS) with VOMS-SAML.
- Produce time lines for the above tasks.
- The above points, the basis for the internal milestone, are to be understood by EMI project at month 8.

4.1.10 Compute Area Authorization

In order to follow the overall harmonization strategy of removing duplicate components and providing a standard(ized) solution it is proposed that Argus should become the standard authorization system for the three middleware stacks in EMI. This will entail producing a common XACML profile for all job management components between the three stacks. The integration of the gLite CREAM computing element with Argus is underway and the XACML profile has been drafted which will form the starting point for the common profile. A group, sourced from both within and externally to the Argus PT, will gather the following facts for this task and then the integration of Argus into all stacks can proceed.

- Gather the XACML profile requirements of the different Compute Elements of the middleware.
- Determine the work needed to modify/extend the current (CREAM) CE XACML profile.
- Clarify whether the full XACML spec is met within Argus.
- Collect the requirements for WMS and Data integration to Argus.

The first three points are to be understood by EMI project month 8 whereas the last point is planned to be addressed by EMI project month 10. After the requirements gathering, an internal milestone document answering the above points will be produced in month 9. For the rest of the first year of the EMI project, the work in producing the common XACML profile will proceed after the internal milestone document is accepted.

The different methods and locations, within the middleware, of mapping of users to local accounts will be investigated for consistency.

4.2. EVOLUTION

The first year plans of the security area for evolution activities are given here. The following sections are given in order of product teams that are, by definition, responsible for development and testing of their own work.

4.2.1 ARC Security Utils Product Team

In terms of evolution and new development of ARC Security Utils components the following work is anticipated in the first year of the EMI project.

The arcproxy utility will have to respond to client requests for features. The ARGUS Authorization system will need to be integrated to the ARC Security Utils as will VOMS-SAML. The support for MyProxy will be improved. The integration of the Argus policies into the mapfile generator should be completed.

4.2.2 Argus Product Team

The Argus Product Team does not anticipate completely new developments in the first year of the EMI project. Argus will respond to requirements from clients and the results of integration to the middle-ware stacks. A survey is planned, along with the "Security for Data" milestone, in order to clarify the integration options for Argus for data management solutions.

One area that will require new development is the Execution Environment Service (EES) that ensures that the correct environment required by a user is available and provided. The EES configures, starts/stops and manages VMs taking into account the policies as defined within the Argus system. This includes booting the correct image. The basic EES development and integration to Argus is planned for EMI project month 10 and will be available for EMI Release 1.

In a Cloud context the EES would configure, start, manage and stop VMs taking into account the policies as defined within the Argus system. The EES is envisioned to also interact with commercial Cloud providers through the Open Cloud Computing Interface (OCCI) interface and other cloud-specific interfaces. The Cloud-specific development, mandated in the EMI DoW, is planned for EMI project month 10.

4.2.3 VOMS Product Team

In the areas of Proactive Maintenance and Evolution the following work is planned. The C++ APIs will be rewritten to make them more easily maintainable and expandable. An automated test suite will be written for the VOMS-Admin component, for both the Web interface and the APIs. These are planned for release in month 12 of the EMI project, after EMI-1.

4.2.4 gLite Security Product Team

gLExec: There is a plan to study the overall phase-out of the gLExec component. gLExec is used on gLite Computing Elements (CE) and Worker Nodes (WN) to map Grid credentials to local userids. On a gLite CE, some gLExec calls may be substituted by calling the operating system-standard sudo command. This is due to the fact that a CE can provide the information to sudo by passing on the mapping information from Argus. On a WN the situation is different as there is no trusted environment in which system-native credentials of the target account can be passed to sudo. Additionally, sudo itself cannot yet obtain information directly from Argus.

The plan is to create a set of modules following the Pluggable Authentication Modules (PAM) standard that will interact with Argus in order to test their suitability. Once these provide the same functionality as the present situation then gLExec may be migrated to use the PAM modules. gLExec would then perform its basic checks only and work fully on the PAM module(s). Once this works then the move away from gLExec can be foreseen and sudo can take over, using the standard interfaces. This is the roadmap and inherently sets out the transitions for the current gLExec towards a pure O/S integration on which more services may be built in the future. In the first year the PAM modules that will interact with Argus are planned to be released for EMI Release 1.

LCAS/LCMAPS. For the LCMAPS-plugins-c-pep the development work planned for EMI Release 1 is the Argus 1.2 compliance.

Hydra. In the first year of the project the feasibility of integrating the Hydra keystore concept to Cloud resources is planned. A milestone planned for this work would be a document describing whether this work is useful. The document will be available at project month 10.

Pseudonymity. In order to satisfy user privacy requests, both from international projects and specific countries, the pseudo-anonymity service, that provides an anonymous yet auditable identity, will need to be released correctly by EMI. The minor work of producing and release for EMI-1 should be ready by project month 10.

STS. The Security Token Service (STS) development and requirements are dependent on the results of the "AAI for DCIs" workshop milestone. In order that the STS will work with all three middleware stacks the requirements to be met should take into account the SAML profile work and Common Authentication Library work. An STS prototype, dependent on the Shibboleth IdP v.3 and in collaboration with the WS-Trust interoperability group, will be ready after the first year of the EMI project.

4.2.5 UNICORE Security Product Team

In order to provide support for the Short-Lived Credential Service (SLCS) or similar services, that provides users an easier method to obtain X.509 credentials, there must be a verification performed of the UNICORE server side with respect to support for DN-based identification of entities everywhere. There will be a deliverable of a list of required changes (if any) in the server-side code for SLCS support at EMI project month 10. The implementation of the changes identified above and the coordination of implementation of those changes in components managed by other Product Teams (if needed) should be finished by EMI project month 11. This deliverable will demonstrate that the usage of SLCS does not interfere with usage of any of the UNICORE server components.

It is also planned for the support of a priori assessment whether a given entity has an access to a given grid site(s). Also, the optimization of the UNICORE security stack performance with usage of

communication sessions and credentials storage. Those efforts are in early planning stage and it is yet not possible to provide concrete finish dates.

The schedule is:

- M10: Identification of possible problems in UNICORE stack with respect to usage of short lived certificates.
- M11: UNICORE server side is updated to use short lived certificates.

4.2.6 CESNET Security Product Team

The CESNET Security Product Team does not plan any evolution work on the products that they maintain. The only possible exception may be that some work on the delegation tool that may be needed in response to requirements from other middleware areas.

5. CONCLUSIONS

This document describes the first year work plan for the security area of the EMI project. The plan is based on the best information at the time and follows the general plan set out in the parallel DNA1.3.1 overall technical plan. This document will be updated by the DJRA1.3.2. The tasks described in the above document are summarized in the table below.

Task Description	Responsible Group	Start	End
Argus Release 1.2	Argus PT	PM1	PM6 (finished)
Argus 1.2 updates	Argus PT	Ongoing	PM12
Finalize the XACML Grid CE profile [8] v.1.0 for CREAM.	Argus PT	Ongoing	PM8
Update-crls replacement	ARC Security PT	Ongoing	PM9
Arcproxy/Nordugridmap	ARC Security PT	Ongoing	PM12
VOMS 2.0	VOMS PT	Ongoing	PM10
VOMS-Admin 2.6	VOMS PT	Ongoing	PM12
Trustmanager Re-organization	Glite-Security PT	Ongoing	PM8
Delegation: RFC3820 proxies, proxy configuration.	Glite-Security PT	PM8	PM9
LCAS/LCMAPS API Upgrade	Glite-Security PT	Ongoing	PM10
Glexec v0.8	Glite-Security PT	PM1	PM7 (Completed)
Hydra Release	Glite-Security PT	PM1	PM12
Argus Call-out in UNICORE/X	UNICORE Security PT	PM4	PM8
UNICORE SAML AuthZ attributes.	UNICORE Security PT	PM1	PM4 (Completed)
Samly2 to opensaml replacement	UNICORE Security PT	PM7	PM9
UNICORE input to common authn lib	UNICORE Security PT	PM1	PM3 (Completed)
GSI Removal Plan	GSI Group plus Delegation TF	Ongoing	PM9
Common AuthN Lib, requirements, inventory,effort	Common Authentication Library Group	PM1	PM4 (Completed)
Common Authn Lib release for testing	Common Authentication Library Group	PM7	PM12

Common SAML profile requirements and time line	Common SAML profile Group	PM1	PM8
Common CE XACML profile: Acceptance by CREAM	Argus PT and Common CE XACML profile group	PM2	PM8 (completed)
Needed extensions to CREAM XACML	Argus PT and Common CE XACML profile group	PM7	PM9
Argus full XACML spec check.	Argus PT and Common CE XACML profile group	PM3	PM8
Requirements for DM and WMS Argus integration	Argus PT and Common CE XACML profile group and DM, Compute members	PM6	PM10
EES for Argus prototype	Argus product team	PM1	PM10
VOMS automated test suite and new APIs	VOMS product team	PM1	PM12
PAM module replacement for gLexec	Glite Security Product Team	PM3	PM10
LCAS/LCMAPS compliance with Argus 1.2	Glite Security Product Team	PM1	PM10
Integration of pseudonymity	Glite Security Product Team	PM6	PM10
Hydra/Cloud integration feasibility	Glite Security Product Team	PM3	PM10
Study of UNICORE server for SLCS	UNICORE Security Product Team	PM3	PM10
Update of UNICORE server for SLCS	UNICORE Security Product Team	PM10	PM11