EUROPEAN MIDDLEWARE INITIATIVE

Security Workshop

EU MILESTONE: MJRA1.1

Document identifier:	
Date:	**July 5, 2010**
Activity:	**JRA1**
Lead Partner:	**University of Helsinki**
Document status:	**DRAFT**
Document link:	

Abstract:
A security workshop, attached to the EMI kick-off meeting will examine the status and immediate plans for the following subjects:

- Removal of GSI for replacement by SSL/TLS. For this subject it will be necessary to confirm and tabulate the components that are still dependent on GSI and which will benefit from this standardization. This includes non-security components.
- Common authentication libraries. At this stage we should be able to project whether the common library should be X.509 only or include SAML support. The use-cases within each stack must be presented.
- Usage of the SAML-enabled VOMS service. Usage of this service within ARC/gLite must be understood and a medium-term plan for possible replacement or coexistence of attribute certificates with SAML made.
- Review of the Authorization decision mechanisms of all job management systems. A plan for any necessary integration with the common libraries and security tokens made.

The results of the security workshop will be presented and taken into account in the first deliverable document, Security Area Work Plan and Status Report (Part 1). This document will present the status of the security infrastructures and components, the integration plan and a work plan for the first year of the project as requested in the Evaluation Report.

Delivery Slip

	Name	Partner/Activity	Date	Signature
From	John White	UH/JRA1	June 23rd 2010	Huh?
Reviewed by	Bàlazs Konya	LU/NA1	July July 1st	
Approved by				

Document Log

Issue	Date	Comment	Author/Partner
1			
2			
3			

Document Change Record

Issue	Item	Reason for Change
1	Minor stuff	July 1st : Comments from Bàlazs
2		
3		

1. Workshop Organization

The Security Workshop was held on May 25-26th at CERN. The agenda is found here:

`http://indico.cern.ch/conferenceDisplay.py?confId=92643`

In order to access this event a Google search with "indico CERN 92643" will give the above page. All the talks given have been uploaded to the above timetable page of the event. A list of registrants is visible from the event page, it is noted that the minority of people who attended the workshop were registered.

This workshop was held very early in the project schedule, in agreement with the EU, in order to provide some early responses and directions in the security area. These are needed in order to produce a first year security middleware plan for harmonization between the three stacks and also a direction for the mid-term evolution of the EMI security components.

2. Workshop Subjects

As outlined in the abstract, the following subjects were identified as needing early agreement in the project.

2.1. GSI

During the last three years, there has been work to remove the GSI protocol from certain critical Grid middleware (notably VOMS). The GSI code is replaced by standard SSL/TLS.

In this case GSI refers to the family of protocols, one of which is provided by the Globus Security Infrastructure (GSI) protocol which functions as an "enhanced" SSL protocol that allows proxies and proxy delegation.

There were presentations given on this subject by representatives of various middleware components and areas that would be affected by the removal of GSI and its replacement with SSL/TLS. These presentations, available on the event URL above, came from the Virtual Organization Management System (VOMS), the general Data Management area, Delegation and Proxy Renewal from gLite and the ARC collaboration. The UNICORE middleware stack does not use the Java GSI library and is thus immune to these problems.

There is a version of VOMS that provides GSI-free libraries and that the ARC middleware stack would be interested in obtaining and using these libraries. The version of openSSL, either in the underlying operating system, or installed by the middleware is a related issue since `openSSL 0.9.8k` does support proxies which negates some of the need for GSI.

From Data Management the question was posed as to why do we need to move away from GSI. Also within the Data Management area there is the question of the SRM interfaces eg. `srm-copy` that do use GSI. Also, GSIftp obviously uses GSI and is a critical part of data transfer services. For example: The endpoints for the SRM (SURLs) are stored in catalogues, the migration from GSI http(g) to standard https would require running services which provide both protocols on the same host/port for a transition period.

Delegation is another similar case but requiring a move towards dedicated delegation service or port-type (C/C++ and Java respectively) would negate the GSI problem. gLite Logging and Bookkeeping (L&B) uses the GSI Globus libraries only internally and uses the standard SSL protocol over the network. Since the utilization of GSI does not pose any limitation for the L&B clients and any change to the communication layer would be very complex and risky, there is no plan for transition to another implementation.

gLite L&B acknowledges the generality of the GSS-API allowing for a quick transition to an alternative security protocol (Kerberos), which has been demonstrated in a real deployment.

The resulting discussion brought the following points that need to be addressed:

- Need to tabulate a “list of effort” to see how much effort and resulting reward to remove GSI from components.
- Need to understand the implications of moving to OpenSSL 1.0.x in the future.
- Explore the possibility to send a message to the IGE project requesting an implementation of GSI that is compatible with the relevant OpenSSL versions.
- For delegation, there is a requirement for 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 should be concluded before month 4 of the project.

2.2. SAML

For this subject there were presentations from VOMS, ARC, UNICORE and the projected standard Authorization system, Argus.

The VOMS-SAML version, first developed in conjunction with the OMII-Europe, is now deployed in gLite and ARC. Through the availablity and deployment of VOMS-SAML, the gLite and ARC middleware stacks do have a capability to produce SAML assertions and use them in limited cases. The main underlying reason for non-usage of SAML is a lack of requests and requirements from the Grid user communities.

UNICORE, on the other hand, has SAML capabilities and uses SAML within the stack. The SAML assertions are generated by the UNICORE Virtual Organization System (UVOS). UNICORE does not use the openSAML2 library as it was not available at the time that the move to SAML2 was made but does have a documented draft SAML profile.

From these presentations and the following discussions a group has been called on to perform the following work for SAML integration. The following points were noted:

- 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 LCG (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 UVOS with VOMS-SAML.
- Produce timelines for the above tasks.

2.3. Common Authentication Libraries

It is given that a common set of authentication libraries between the three middleware stack is desirable. At this stage we should be able to project whether the common libraries should be X.509 only or include SAML support. The use-cases within each stack were presented.

UNICORE uses the standard TLS/SSLv3 authentication with regular X.509 certificates with mutually authenticated connections. UNICORE presented a well-defined set of requirements on a common authentication library:

- Java API and implementation.
- Standard TLS/SSLv3 with standard X.509 certificates supported.
- All features optional & configurable.
- For instance host name checking can be seen as a valuable addition to UNICORE but must not be mandatory.
- Programmatic configuration must be possible (without relaying on system-wide settings).
- HTTP auth (user & password) possible.

gLite presented work performed and experiences within the VOMS authentication library. Requirements include:

- Ability to switch off parts of the authentication when necessary.

For ARC, the requirements include that the code is “thread-friendly”.

The action taken here is to set up an “Authentication library” group consisting of members from each middleware consortium. This group should provide, ideally before the end of July 2010 (Project Month 3):

- 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.

2.4. Compute Area Authorization

This section (listed in the workshop agenda as “Job Management Authorization”) eventually consisted of a general review of the authorization mechanisms of each middleware stack.

The ARC CE (in production Grid Manager and in development A-REX) use the “standard” set of attributes for authorization: X.509 subject, VOMS attributes and WS-Sec tokens. The information is analyzed with internal policies in GACL and preliminary XACML support. A move to Argus Authorization is appreciated providing that a common CE XACML profile can be written.

The UNICORE authorization model is different to the two other stacks by virtue of their infrastructure; the user name is always known. The policy decision point (PDP) is XACML-based using the SUN 1.2 version library. The Authorization is made based on attributes (SAML in this case). The similarities to Argus means UNICORE is willing to move to adopt Argus as a site-central Authorization system. Some of the points that need clarification (see below) include whether Argus implements the full XACML specification and can a XACML policy be added to Argus. There were also some questions about the Argus simplified policy language from UNICORE.

From the gLite WMS, the authorization mechanisms were explained. The question of moving towards a site-central Authorization system depends on the fact that WMS would need to do the Authorization at the match-making stage that currently uses BDII.

The gLite CREAM integration to Argus is underway and the XACML profile has been drafted [1].

From the discussion it was decided that, within the Argus Product Team, a group should be formed that will perform the following work:

- Gather the XACML profile requirements of the different CEs.
- 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 integration to Argus.

2.5. OTHER SUBJECTS

Other topics, not necessarily in the agenda, that were touched on in the workshop included the two other upcoming security milestones.

2.5.1. AAI NEEDS OF DCIS

This is milestone MJRA1.9 due in project month 7. This consist of a security “workshop” at the EGI technical forum in September 2010. The meeting has been requested from the EGI workshop organizers and a list of interested client communities has been started. Of particular interest will be viewpoints from some of the more organized countries in terms of identity management eg: UK, Switzerland.

2.5.2. “DATA” SECURITY NEEDS.

This is milestone MJRA1.5 (Agreement on common security methods for data systems) due in project month 5. It was noted with the Data area leader that this milestone will need significant input from the security area and that work should proceed as soon as possible.

2.5.3. SECURITY TOKEN SERVICE.

As stated in the EMI proposal, there is a need for interoperabilty support between X.509 and other security tokens, most notably SAML and Kerberos. This can be achieved through a security token service that allows to transform one type of security token into another. Prototype work has been initiated during the EGEE-III project. It is planned to evaluate this prototype work and decide on its possible future use after Month 7 when the milestone MJRA1.9 has been achieved (see 2.5.1.).

References

[1] gLite CREAM devlopment team. **XACML Grid Computing Element Authorization Profile**, 2010. `https://edms.cern.ch/document/1078881/1`.