EUROPEAN MIDDLEWARE INITIATIVE

MJRA1.1 – SECURITY WORKSHOP

EC MILESTONE: MS26

Document identifier:	**EMI_MS26.doc**
Date:	**05/07/2010**
Activity:	**WP5-JRA1**
Lead Partner:	**UH**
Document status:	**Final**
Document link:	**http://cdsweb.cern.ch/record/1277565?ln=en**

Delivery Slip

	Name	Partner / Activity	Date	Signature
From	John White	UH/WP5-JRA1	05/07/2010	
Approved by	PEB			

Document Log

Issue	Date	Comment	Author / Partner
1			
2			
3			

Document Change Record

Issue	Item	Reason for Change
1		
2		
3		

MILESTONE REPORT

The EMI Security Workshop was held at CERN on 25-26th of May 2010. It was a successful meeting with around 20 EMI security experts registered for the event, although much more turned up during the two-day meeting. As agreed with the EC, the security workshop was organised very early in the project execution to be able to get initial input on the strategies and directions of the security area. The workshop provided useful information for the first year security middleware plan which covers, among many things, the harmonisation of the security mechanisms of ARC, gLite and UNICORE and also provide a strategy for the mid-term evolution of the EMI security components. Technical details about the workshop is attached as annex to this document.

More information about the workshop, including agenda and presentations, are available at the event page http://indico.cern.ch/conferenceDisplay.py?confId=92643.

ANNEX: SECURITY WORKSHOP TECHNICAL REPORT

GSI, SAML, Common Authentication Libraries and Compute Area Authorisation are some of the important topics discussed, and required agreement on, at the Security Workshop.

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 came from 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. 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, questions on the the need to move away from GSI and SRM interfaces eg. srm-copy that do use GSI were raised. 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:

- Provide 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 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 by August 2010.

2. SAML

SAML presentations were given by 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 the lack of requests and requirements from the users. 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 of 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 formed 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 (via 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.

3. COMMON AUTHENTICATION LIBRARIES

It is given that a common set of authentication libraries between the three middleware stacks is desirable. At this stage, the project can anticipate 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 and 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. gLite requires the ability to switch off parts of the authentication when necessary. For the ARC middleware, it requires the code to be “thread-friendly”.

The “Authentication library” group was set-up consisting of members of the middleware consortia. This group should provide, ideally before the end of July 2010:

- 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.

4. COMPUTE AREA AUTHORIZATION

The workshop also covered an overview of the authorisation mechanisms of ARC, gLite and UNICORE. The ARC CE (referred to as Grid Manager in production and A-REX in development) uses the “standard” set of attributes for authorization: X.509 subject, VOMS attributes and WS-Sec tokens. The information is analysed with internal policies in GACL and preliminary XACML support. A move to Argus Authorization is appreciated provided 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 include whether Argus implements the full XACML specification and can a XACML policy be added to Argus. Questions on Argus simplified policy language from UNICORE were also raised.

The authorisation mechanisms of gLite WMS were explained. The question of moving towards a site-central Authorisation system depends on the fact that WMS would need to do the Authorisation 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]. 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.

5. OTHER SUBJECTS

Several topics, not originally included in the agenda, were discussed at the workshop.

5.1. AAI REQUIREMENTS OF DCIS

MJRA1.9 AAI Requirements of DCIs due in November 2010 is a checkpoint for the Security Workshop at the EGI Technical Forum in September 2010, as requested by EGI. Of particular interest will be viewpoints from some of the more organised countries in terms of identity management eg: UK, Switzerland.

5.2. “DATA” SECURITY NEEDS.

MJRA1.5 Agreement on common security methods for data systems due in September 2010 will need significant input from the security area and that work should proceed as soon as possible, as agreed with the data area leader.

5.3. SECURITY TOKEN SERVICE.

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 November 2010 when the milestone MJRA1.9 is expected to be reached.

REFERENCES

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