EUROPEAN MIDDLEWARE INITIATIVE

MJRA1.5 - AGREEMENT ON COMMON SECURITY METHODS FOR DATA SYSTEMS

EC MILESTONE: MS30

Document identifier: EMI-MS30-1277626-Common_Security_Methods-v1.0.doc
Date: 31/07/2010
Activity: JRA1
Lead Partner: DESY
Document status: Final
Document link: http://cdsweb.cern.ch/record/1277626?ln=en
Copyright notice:

Copyright (c) Members of the EMI Collaboration. 2010.

See http://www.eu-emi.eu/about/Partners/ for details on the copyright holders.

EMI ("European Middleware Initiative") is a project partially funded by the European Commission. For more information on the project, its partners and contributors please see http://www.eu-emi.eu.

This document is released under the Open Access license. You are permitted to copy and distribute verbatim copies of this document containing this copyright notice, but modifying this document is not allowed. You are permitted to copy this document in whole or in part into other documents if you attach the following reference to the copied elements: "Copyright (C) 2010. Members of the EMI Collaboration. http://www.eu-emi.eu ".

The information contained in this document represents the views of EMI as of the date they are published. EMI does not guarantee that any information contained herein is error-free, or up to date.

EMI MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, BY PUBLISHING THIS DOCUMENT.
## Delivery Slip

<table>
<thead>
<tr>
<th>Name</th>
<th>Partner / Activity</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Patrick Fuhrmann</td>
<td>DESY</td>
<td>21/01/2011</td>
<td></td>
</tr>
<tr>
<td>Approved by</td>
<td>PEB</td>
<td>04/02/2011</td>
<td></td>
</tr>
</tbody>
</table>

## Document Log

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Comment</th>
<th>Author / Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>22/9/2010</td>
<td>Initial Version</td>
<td>Patrick Fuhrmann/DESY</td>
</tr>
<tr>
<td>2</td>
<td>27/12/2010</td>
<td>Updated with statements from CASTOR and BeStMan</td>
<td>Patrick Fuhrmann/DESY</td>
</tr>
<tr>
<td>3</td>
<td>21/1/2011</td>
<td>Modified based on reviews by Balazs and Morris.</td>
<td>Patrick Fuhrmann/DESY</td>
</tr>
</tbody>
</table>

## Document Change Record

<table>
<thead>
<tr>
<th>Issue</th>
<th>Item</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## References

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Storage Resource Manager</td>
<td><a href="https://sdm.lbl.gov/srm-wg/">https://sdm.lbl.gov/srm-wg/</a></td>
</tr>
<tr>
<td>2</td>
<td>GLOBUS</td>
<td><a href="http://www.globus.org">http://www.globus.org</a></td>
</tr>
<tr>
<td>3</td>
<td>GLOBUS/GSI</td>
<td><a href="http://globus.org/toolkit/docs/3.2/gsi/">http://globus.org/toolkit/docs/3.2/gsi/</a></td>
</tr>
<tr>
<td>4</td>
<td>BeStMan</td>
<td><a href="https://sdm.lbl.gov/bestman/">https://sdm.lbl.gov/bestman/</a></td>
</tr>
<tr>
<td>5</td>
<td>CASTOR</td>
<td><a href="http://castor.web.cern.ch">http://castor.web.cern.ch</a></td>
</tr>
</tbody>
</table>
MILESTONE REPORT

This document indicates the agreement to migrate the SRM[1] security mechanisms from the current Grid Security Infrastructure (GSI) to standard SSL/TLS with X509 and a new delegation method. The important agreement that will help the data area to overcome current incompatibilities applies to all EMI data components and is also supported by CASTOR(CERN) and BeStMan(LBNL).

Background

The Storage Resource Manager (SRM)[1] protocol is a mechanism to remotely manage storage. It negotiates file transfer protocols, manages name spaces, reserves spaces and assigns storage attributes, e.g. data retention policies and access latencies, to files or file collections.

As those operations have a significant impact on the operation of a site, proper authentication and authorization is required. Moreover, some of the SRM operations subsequently need to perform actions on other systems on behalf of the initial requestor. This requires credential delegation.

At the time of the initial definition of the SRM, the GLOBUS [2] framework offered a convenient way to cover those requirements with the single protocol known as the GSI [3]. The disadvantage however is that this protocol approach (i.e. httpg://) is not compatible with standard security mechanism used elsewhere, e.g. SSL/TSL with X509 (i.e. https://). This lack of standard-compliance is a hindrance to enable a broader usage of the SRM technologies that go beyond dedicated Grid-based setups to more Web-based (and thus potentially also commercial) environments.

Agreement

As standardization is one of the goals of EMI and to allow for utilizing OS provided libraries instead of proprietary software stacks, the EMI-Data area together with others in our Grid community agreed to migrate the SRM security mechanism from the traditional GLOBUS/GSI towards SSL/TSL with X509. The parties required to agree are the EMI storage elements dCache, DPM, StoRM plus CASTOR[5], and BeStMan[4]. The both later ones are SRM implementations that the EMI project is collaborating with but having no direct influence on their developments. In addition, client software providers have to agree, which are GFAL(gLite) and the ARC middleware data clients, both part of EMI-Data.

This actual agreement requires two steps

1. The agreement to migrate from GLOBUS/GSI to SSL/TSL with X509.
2. An agreement which delegation method to use.

This milestone is only about the general agreement that has been achieved for both steps. Nevertheless, a working group, combining people from EMI data, security, and computing plus people from CASTOR and BeStMan, is currently evaluating the most appropriate delegation method arising from the aforementioned second agreement.

This milestone is achieved, because all EMI-Data middleware component providers (dCache, DPM, StoRM) have agreed on the aforementioned steps implicitly through the EMI DoW and explicitly in meetings and e-mail discussions.

In addition, the agreements by CASTOR and BeStMan are attached to this document. This is an important addition to the milestone in order to ensure that EMI solutions will be not considered as storage islands having another security mechanism than the overall Grid community.
Agreement on the SRM security protocol by CASTOR

This is a statement from Dirk Düllmann (CERN), responsible for CASTOR, from Dec 15, 2010 on the migration from GSI to SSL/TSL X509.

“For Castor we did already agree with the move at the Desy SRM meeting and will collaborate with the working group to achieve a consistent move. We'll draft in the development necessary to support the additional protocol in April 2012 and Giuseppe (*) will follow the working group activities until then to make sure we are ware of the implications for the castor SRM.”

* Giuseppe Lo Presti is the CASTOR chief developer.
December 20, 2010

Re: SRM security protocol in BeStMan for EMI collaboration

To whom it may concern,

As group leader of the group that developed the Berkeley Storage Manager (BeStMan) and corresponding Storage Resource Manager (SRM) client tools at Lawrence Berkeley National Laboratory, I agree to collaborate with the European Middleware Initiative (EMI) - Data area in order to migrate the SRM security mechanism from the current Grid Security Infrastructure (GSi) to https/x.509. Details, especially on how to resolve the necessary delegation, are discussed in the corresponding EMI-Data working group, where BeStMan would be represented.

Please feel free to contact me for any further information.

Sincerely,

Aric Shoshani

Aric Shoshani, Ph.D
Senior Staff Computer Scientist
Group Leader, Scientific Data Management Research Group
Lawrence Berkeley National Laboratory
One Cyclotron Road, MS 50B-3238
Berkeley, CA 94720
Tel: 510-486-5171
E-mail: Shoshani@LBL.Gov