



# EGI-InSPIRE

## UMD SECURITY CAPABILITIES QUALITY CRITERIA v2 DRAFT 1

---

Document identifier:	EGI-SECURITY-QC-V2.DRAFT-1.docx
Date:	<b>22/06/2011</b>
Document Link:	<a href="https://documents.egi.eu/document/346">https://documents.egi.eu/document/346</a>

---

### Abstract

This document describes the UMD Security Capabilities Quality Criteria.



### Copyright notice

Copyright © Members of the EGI-InSPIRE Collaboration, 2010. See [www.egi.eu](http://www.egi.eu) for details of the EGI-InSPIRE project and the collaboration. EGI-InSPIRE (“European Grid Initiative: Integrated Sustainable Pan-European Infrastructure for Researchers in Europe”) is a project co-funded by the European Commission as an Integrated Infrastructure Initiative within the 7th Framework Programme. EGI-InSPIRE began in May 2010 and will run for 4 years. This work is licensed under the Creative Commons Attribution-Noncommercial 3.0 License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/3.0/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, and USA. The work must be attributed by attaching the following reference to the copied elements: “Copyright © Members of the EGI-InSPIRE Collaboration, 2010. See [www.egi.eu](http://www.egi.eu) for details of the EGI-InSPIRE project and the collaboration”. Using this document in a way and/or for purposes not foreseen in the license, requires the prior written permission of the copyright holders. The information contained in this document represents the views of the copyright holders as of the date such views are published.

### Document Log

Issue	Date	Comment	Author/Partner
1.0	15/11/2010	First draft	Enol Fernández
1.1	19/11/2010	Added criteria for more capabilities.	Enol Fernández
1.2	17/01/2011	Completed criteria for Credential Management, User Management and Authorisation.	Enol Fernández
1.3	09/02/2011	Added delegation criteria, Authorisation review	Enol Fernández
2 DRAFT 1	10/05/2011	Update criteria to release 2	E. Fernández

## TABLE OF CONTENTS

<b>1</b>	<b>Authentication</b>	<b>5</b>
1.1	<b>Authentication Interface</b>	<b>5</b>
	AUTHN_IFACE_1	5
	AUTHN_IFACE_2	5
1.2	<b>Delegation Interface</b>	<b>6</b>
	AUTHN_DELEG_1	6
1.3	<b>CAs root certificates Distribution</b>	<b>6</b>
	AUTHN_CA_1	6
	AUTHN_CA_2	7
	AUTHN_CA_3	8
<b>2</b>	<b>Attribute Authority</b>	<b>9</b>
2.1	<b>Attribute Authority Interface</b>	<b>9</b>
	ATTAUTH_IFACE_1	9
	ATTAUTH_IFACE_2	10
	ATTAUTH_IFACE_3	11
	ATTAUTH_IFACE_4	12
2.2	<b>VO management</b>	<b>13</b>
	ATTAUTH_MGMT_1	13
	ATTAUTH_MGMT_2	14
	ATTAUTH_MGMT_3	15
	ATTAUTH_MGMT_4	17
	ATTAUTH_MGMT_5	18
2.3	<b>VO Management Web Interface (VOMS-Admin)</b>	<b>19</b>
	ATTAUTH_WEB_1	19
	ATTAUTH_WEB_2	20
	ATTAUTH_WEB_3	21
	ATTAUTH_WEB_4	22
	ATTAUTH_WEB_5	23
<b>3</b>	<b>Authorisation</b>	<b>24</b>
3.1	<b>Policy Management</b>	<b>24</b>
	AUTHZ_MGMT_1	24
	AUTHZ_MGMT_2	25
3.2	<b>Policy Definition</b>	<b>27</b>
3.2.1	Central policy management (Argus)	27
	AUTHZ_PCYDEF_1	27
	AUTHZ_PCYDEF_2	28
3.2.2	Service Based Authorisation (Not Argus)	29
	AUTHZ_PCYDEF_3	29
	AUTHZ_PCYDEF_4	30
3.3	<b>Policy Decision Point</b>	<b>31</b>
	AUTHZ_PDP_1	31
3.4	<b>Policy Enforcement</b>	<b>32</b>
	AUTHZ_PEP_1	32
	AUTHZ_PEP_2	33
<b>4</b>	<b>Credential Management</b>	<b>34</b>
4.1	<b>Credential Management Interface</b>	<b>34</b>
	CREDMGMT_IFACE_1	34
	CREDMGMT_IFACE_2	35



CREDMGMT_IFACE_3.....	36
<b>4.2 Institutional Authentication Systems Linking.....</b>	<b>37</b>
CREDMGMT_LINK_1.....	37
<b>5 References.....</b>	<b>38</b>

## 1 AUTHENTICATION

An authentication token that is strongly bound to an individual must be applied consistently across the software used within the production infrastructure. The authentication system should be capable of supporting a delegation model.

### 1.1 Authentication Interface

<b>X.509 Certificate support</b>	
<b>ID</b>	<b>AUTHN_IFACE_1</b>
<b>Description</b>	Primary authentication token within the infrastructure is the X.509 certificate and its proxy derivatives. The certificates and any proxy schemes must follow specifications that are fully integrated into the https protocol.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authentication Appliances.
<b>Input from Technology Provider</b>	Test suite for the use of X.509 proxy support for authentication If the component exposes a WebService that requires authentication, it must use the X.509 certificates/proxies with the https protocol. The exact content of the test suite depends on the component interface.
<b>Pass/Fail Criteria</b>	X.509 proxies are accepted for authentication. WebServices must use https. For the major release of UMD, products still using GSI authentication (with httpg for WebServices) may be accepted, <u>this exception may be dropped</u> in future releases of the criterion.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	V2: Added GSI (httpg) exception for products that have not yet transitioned
<b>SAML authentication</b>	
<b>ID</b>	<b>AUTHN_IFACE_2</b>
<b>Description</b>	SAML 2.0 can be used as authentication interface within the infrastructure.
<b>Mandatory</b>	NO
<b>Applicability</b>	Authentication Appliances with SAML 2.0 support.
<b>Input from Technology Provider</b>	Test suite for the use of SAML 2.0 support for authentication. The exact contents of the test suite depend on the component interface.
<b>Pass/Fail Criteria</b>	Pass if SAML2.0 authentication is supported in the appliance.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

## 1.2 Delegation Interface

Delegation Interface	
<b>ID</b>	<b>AUTHN_DELEG_1</b>
<b>Description</b>	Delegation of credentials must be provided using one of the supported delegation interfaces: GridSite or Globus 4.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authentication Appliances that provide (require) delegation.
<b>Input from Technology Provider</b>	Test suite for the delegation interface that includes all functions in the WSDL. Test erroneous input and generation of error messages.
<b>Pass/Fail Criteria</b>	Pass if the delegation interface is tested and works as expected. Appliances must support at least one of the following interfaces: GridSite delegation or Globus 4 delegation.
<b>Related Information</b>	UMD Roadmap [R 1] GridSite Delegation [R 4] Globus Delegation [R 5]
<b>Revision Log</b>	V2: Merged AUTHN_DELEG_1 & 2.

## 1.3 CAs root certificates Distribution

These QC deal with the distribution of the EuGridPMA [R 5] root certificates.

CA Checksum	
<b>ID</b>	<b>AUTHN_CA_1</b>
<b>Description</b>	The CA distribution must assure that the distributed CA certificates are correct.
<b>Mandatory</b>	YES
<b>Applicability</b>	Trust Anchor Distribution
<b>Input from Technology Provider</b>	Checksum test of each of the root certificates distributed.
<b>Test Description</b>	<p><b>Pre-condition</b> None</p> <p><b>Test</b> Test checksum of the CA certificates.</p> <p><b>Expected Outcome</b> All checksums are correct.</p>
<b>Pass/Fail Criteria</b>	All CA certificates have correct checksum.
<b>Related Information</b>	
<b>Revision Log</b>	

CA valid dates	
<b>ID</b>	AUTHN_CA_2
<b>Description</b>	Dates of the distributed CA certificates are valid for the current date.
<b>Mandatory</b>	YES
<b>Applicability</b>	Trust Anchor Distribution
<b>Input from Technology Provider</b>	Data validity test of each of the root certificates distributed.
<b>Test Description</b>	<p><b>Pre-condition</b> None</p> <p><b>Test</b> Check the current date is in the range of the valid dates of the certificate.</p> <p><b>Expected Outcome</b> All dates are valid.</p> <p><b>Sample Test</b></p> <pre>#!/bin/sh check_dates() {   certfile=\$1   start=`openssl x509 -in \$certfile -noout -startdate   cut -f2 -d "="`   if [ \$? -ne 0 ] ; then     echo "Error while processing \$certfile"     return 1   fi   now=`date +%s`   start_sec=`date +%s -d"\$start"`   if [ \$now -lt \$start_sec ] ; then     echo "\$start is before now in \$certfile!"     return 1   fi   end=`openssl x509 -in \$certfile -noout -enddate   cut -f2 -d "="`   if [ \$? -ne 0 ] ; then     echo "Error while processing \$certfile"     return 1   fi   end_sec=`date +%s -d"\$end"`   if [ \$end_sec -lt \$now ] ; then     echo "\$end is after now in \$certfile!"     return 1   fi   return 0 }</pre>
<b>Pass/Fail Criteria</b>	All CA certificates have correct dates.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>CA CRL check</b>	
<b>ID</b>	<b>AUTHN_CA_3</b>
<b>Description</b>	The CRL of the CAs must be available for download and must be valid.
<b>Mandatory</b>	YES
<b>Applicability</b>	Trust Anchor Distribution

<b>Input from Technology Provider</b>	Test that the CRL of the CA is available for download and it's valid.
<b>Test Description</b>	<p><b>Pre-condition</b> List of URLs for each CRL is available.</p> <p><b>Test</b> Download CRL and load it.</p> <p><b>Expected Outcome</b> All CRLs can be downloaded and loaded correctly.</p> <p><b>Sample Test</b></p> <pre>#!/bin/sh  check_crl() {     url_file=\$1     url=`cat \$url_file`     crl=`mktemp`     wget -q \$url -O \$crl     if [ \$? -ne 0 ] ; then         echo "Unable to download crl from \$url"         rm \$crl         return 1     fi     openssl crl -in \$crl -noout &gt; /dev/null     if [ \$? -ne 0 ] ; then         # try in other format         openssl crl -inform der -in \$crl -noout &gt; /dev/null         if [ \$? -ne 0 ] ; then             echo "Unable to load crl"             rm \$crl             return 1         fi     fi     rm \$crl     return 0 } </pre>
<b>Pass/Fail Criteria</b>	All CRLs can be downloaded and loaded.
<b>Related Information</b>	
<b>Revision Log</b>	



## 2 ATTRIBUTE AUTHORITY

### 2.1 Attribute Authority Interface

Proxy Issue	
<b>ID</b>	ATTAUTH_IFACE_1
<b>Description</b>	Users must be able to get proxies with VO related information.
<b>Mandatory</b>	YES
<b>Applicability</b>	Attribute Authority Appliances
<b>Input from Technology Provider</b>	Test the creation of proxies for different users, roles and groups. Test for error situations (not registered user, unknown VO, non existing role/group, unreachable server)
<b>Test Description</b>	<b>Pre-condition</b> Valid user certificate, user registered in VO <b>Test</b> Create proxy for user in the given VO. <b>Expected Outcome</b> Valid proxy created.
	<b>Pre-condition</b> Valid user certificate, user registered in VO, user in a given group/role <b>Test</b> Create proxy for user in the given VO and group/role <b>Expected Outcome</b> Valid proxy created with correct group/role information.
	<b>Pre-condition</b> Valid user certificate, user not registered in VO <b>Test</b> Create proxy for user in the given VO. <b>Expected Outcome</b> Issue a error message stating that the user is unknown to the VO.
<b>Pass/Fail Criteria</b>	Tests for the creation of proxies work as expected. Groups/Roles/Attributes can be included in the created proxy.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>Proxy Information</b>	
<b>ID</b>	<b>ATTAUTH_IFACE_2</b>
<b>Description</b>	Users must be able to get information about their proxies.
<b>Mandatory</b>	YES
<b>Applicability</b>	Attribute Authority Appliances
<b>Input from Technology Provider</b>	Test tools for getting proxy information.
<b>Test Description</b>	<b>Pre-condition</b> Valid user proxy <b>Test</b> Get information from proxy. <b>Expected Outcome</b> Return proxy information.
	<b>Pre-condition</b> Non existent user proxy <b>Test</b> Get information from proxy <b>Expected Outcome</b> No information returned and error message issued.
<b>Pass/Fail Criteria</b>	Proxy information can be obtained. Complete Groups/Roles/Attributes is also shown.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>Proxy Destroy</b>	
<b>ID</b>	<b>ATTAUTH_IFACE_3</b>
<b>Description</b>	Users must be able to destroy a previously created proxy.
<b>Mandatory</b>	YES
<b>Applicability</b>	Attribute Authority Appliances
<b>Input from Technology Provider</b>	Test the proxy destroy.
<b>Test Description</b>	<p><b>Pre-condition</b> Valid user proxy</p> <p><b>Test</b> Destroy user proxy.</p> <p><b>Expected Outcome</b> Proxy is destroyed.</p>
<b>Pass/Fail Criteria</b>	Proxy is destroyed, no operations requiring a proxy can be done with it.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>SAML Assertion Support</b>	
<b>ID</b>	<b>ATTAUTH_IFACE_4</b>
<b>Description</b>	Users should be able to obtain SAML assertions with the VO information.
<b>Mandatory</b>	NO
<b>Applicability</b>	Attribute Authority Appliances with SAML support.
<b>Input from Technology Provider</b>	Test the generation of SAML assertions for different users, roles and groups. Test for error situations (not registered user, unknown VO, non existing role/group, unreachable server)
<b>Test Description</b>	<b>Pre-condition</b> Valid user, user registered in VO/group/role. <b>Test</b> SAML attribute query for user for the VO/group/role <b>Expected Outcome</b> Valid SAML assertion returned with VO information
	<b>Pre-condition</b> Valid user, user not registered in VO <b>Test</b> SAML attribute query for user in the given VO. <b>Expected Outcome</b> Issue a error message stating that the user is unknown to the VO.
<b>Pass/Fail Criteria</b>	Tests for the creation of SAML assertions work as expected. Groups/Roles/Attributes can be included in assertions.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

## 2.2 VO management

<b>VO Creation</b>	
<b>ID</b>	<b>ATTAUTH_ MGMT_1</b>
<b>Description</b>	The service administrator must be able to create new VOs in the service.
<b>Mandatory</b>	YES
<b>Applicability</b>	Attribute Authority Appliances
<b>Input from Technology Provider</b>	Test the creation of VOs, test for incorrect input.
<b>Test Description</b>	<b>Pre-condition</b> Administrator privileges in VO service. Configured service. <b>Test</b> Create a new VO <b>Expected Outcome</b> New database is created and initialized.
	<b>Pre-condition</b> Administrator privileges in VO service. Configured service. Existent VO name <b>Test</b> Create a VO with already existent name. <b>Expected Outcome</b> No action performed, warning message issued.
<b>Pass/Fail Criteria</b>	Pass if the administrator is able to create VOs for all the supported underlying databases.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>VO Administrators</b>	
<b>ID</b>	<b>ATTAUTH_ MGMT_2</b>
<b>Description</b>	The service administrator must be able to define who has VO administrator privileges.
<b>Mandatory</b>	YES
<b>Applicability</b>	Attribute Authority Appliances
<b>Input from Technology Provider</b>	Test adding VO administrators, test for incorrect input.
<b>Test Description</b>	<b>Pre-condition</b> Administrator privileges in VO service. Configured service. User certificate of new admin. <b>Test</b> Define VO administrator with user certificate. <b>Expected Outcome</b> User is added as VO administrator.
	<b>Pre-condition</b> Administrator privileges in VO service. Configured service. User certificate of already existent admin. <b>Test</b> Define VO administrator with user certificate. <b>Expected Outcome</b> No action performed, warning message is issued.
	<b>Pre-condition</b> Administrator privileges in VO service. Configured service. User certificate of new admin. <b>Test</b> Define VO administrator with user certificate for a nonexistent VO. <b>Expected Outcome</b> Error message stating that the VO is not existent.
<b>Pass/Fail Criteria</b>	Pass if the administrator is able to assign administrator privileges to other users.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>VO Role/Group/Attribute Management</b>	
<b>ID</b>	<b>ATTAUTH_ MGMT_3</b>
<b>Description</b>	Authorized users must be able to define roles, groups and attributed and manage the users with those assigned.
<b>Mandatory</b>	YES
<b>Applicability</b>	Attribute Authority Appliances

<b>Input from Technology Provider</b>	Test creation of roles, groups, attributes and the assignment and de-assignment of users to those.
<b>Test Description</b>	<p><b>Pre-condition</b> Authorized user to manage VO role/group/attribute. Role/Group/Attribute name.</p> <p><b>Test</b> Create a new role/group/attribute in the VO.</p> <p><b>Expected Outcome</b> New role/group/attribute is created in the VO</p>
	<p><b>Pre-condition</b> Authorized user to manage VO role/group/attribute. Already existent Role/Group/Attribute name.</p> <p><b>Test</b> Create role/group/attribute in the VO.</p> <p><b>Expected Outcome</b> No action performed; issue warning message about the role/group/attribute already existing.</p>
	<p><b>Pre-condition</b> Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name.</p> <p><b>Test</b> Create a new role/group/attribute in the VO.</p> <p><b>Expected Outcome</b> No action performed, issue error message.</p>
	<p><b>Pre-condition</b> Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. VO User to add</p> <p><b>Test</b> Assign role/group/attribute to user.</p> <p><b>Expected Outcome</b> User has the role/group/attribute assigned.</p>
	<p><b>Pre-condition</b> Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. VO User to add</p> <p><b>Test</b> Assign role/group/attribute to user.</p> <p><b>Expected Outcome</b> No action performed, issue error message.</p>
	<p><b>Pre-condition</b> Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign</p> <p><b>Test</b> De-assign role/group/attribute to user.</p> <p><b>Expected Outcome</b> Role/Group/Attribute is de-assigned.</p>

	<p><b>Pre-condition</b> Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign without assigned role/group/attribute</p> <p><b>Test</b> De-assign role/group/attribute to user.</p> <p><b>Expected Outcome</b> No action performed, warning message issued.</p>
	<p><b>Pre-condition</b> Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign</p> <p><b>Test</b> De-assign role/group/attribute to user.</p> <p><b>Expected Outcome</b> No action performed, issue error message.</p>
<b>Pass/Fail Criteria</b>	Pass if authorized users are able to manage the role/groups/attributes for a given VO and the users that assigned to them.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	



<b>VO User Management</b>	
<b>ID</b>	<b>ATTAUTH_ MGMT_4</b>
<b>Description</b>	Authorized users must be able to add and remove users to the VO
<b>Mandatory</b>	YES
<b>Applicability</b>	Attribute Authority Appliances
<b>Input from Technology Provider</b>	Test adding/removing users to the VO.
<b>Test Description</b>	<b>Pre-condition</b> Authorized user to manage VO users. User to add to VO. <b>Test</b> Add user to VO <b>Expected Outcome</b> User is correctly added to the VO.
	<b>Pre-condition</b> Non-Authorized user to manage VO users. User to add to VO. <b>Test</b> Add user to VO <b>Expected Outcome</b> No action performed, issue error message.
	<b>Pre-condition</b> Authorized user to manage VO users. User to add to VO that already belongs to the VO. <b>Test</b> Add user to VO <b>Expected Outcome</b> No action performed, issue a warning message.
<b>Pass/Fail Criteria</b>	Pass if authorized users are able to add/remove other users for a given VO.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>ACL Management</b>	
<b>ID</b>	<b>ATTAUTH_ MGMT_5</b>
<b>Description</b>	Authorized users must be able to change the different ACLs of the VO.
<b>Mandatory</b>	YES
<b>Applicability</b>	Attribute Authority Appliances
<b>Input from Technology Provider</b>	Test for changing ACLs of users of the VO.
<b>Test Description</b>	<b>Pre-condition</b> Authorized user to manage ACLs. <b>Test</b> Change ACL for a given user. <b>Expected Outcome</b> ACL is correctly changed.
	<b>Pre-condition</b> Non-Authorized user to manage ACLs. <b>Test</b> Change ACL for a given user. <b>Expected Outcome</b> No action performed, error message issued.
<b>Pass/Fail Criteria</b>	Pass if authorized users are able to manage the ACLs for other users for a given VO. The following list of ACLs is expected to be managed: <ul style="list-style-type: none"> <li>• browse users of VO</li> <li>• management of groups</li> <li>• management of roles</li> <li>• management of attributes</li> <li>• management of ACL</li> <li>• add/remove users</li> </ul>
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

### 2.3 VO Management Web Interface (VOMS-Admin)

<b>VO List View</b>	
<b>ID</b>	<b>ATTAUTH_WEB_1</b>
<b>Description</b>	Users connecting to the web interface should be able to list the VOs handled by the server.
<b>Mandatory</b>	YES
<b>Applicability</b>	Web Portal for Attribute Authority Appliances management
<b>Input from Technology Provider</b>	Provide a web view with the list of VOs in the server.
<b>Test Description</b>	<p><b>Pre-condition</b> VO Web server running, authorized user</p> <p><b>Test</b> Access VO list page.</p> <p><b>Expected Outcome</b> Web page with a list of all VOs in supported by the server and browsable by user.</p>
<b>Pass/Fail Criteria</b>	VO list view is provided and shows only VOs that are viewable by user.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>VO Membership Request</b>	
<b>ID</b>	<b>ATTAUTH_WEB_2</b>
<b>Description</b>	Users should be able to request membership to a VO from the web interface.
<b>Mandatory</b>	YES
<b>Applicability</b>	Web Portal for Attribute Authority Appliances management
<b>Input from Technology Provider</b>	<p>Provide a page for requesting VO membership and test its functionality. This page must ask for the following information:</p> <ul style="list-style-type: none"> <li>• Full name</li> <li>• Institution</li> <li>• Contact details (phone, e-mail, address)</li> </ul> <p>Once the information is entered, users receive an email to confirm the membership request. Once confirmed, VO Admins should receive a notification of the new request.</p>
<b>Test Description</b>	<p><b>Pre-condition</b> VO Web server running, valid credentials of user.</p> <p><b>Test</b> User requests membership from VO.</p> <p><b>Expected Outcome</b> User gets an email to confirm the membership request.</p>
	<p><b>Pre-condition</b> VO Web server running, valid credentials of user, membership confirmation link.</p> <p><b>Test</b> User accesses the membership confirmation link.</p> <p><b>Expected Outcome</b> VO admin(s) receive a notification of the new request.</p>
<b>Pass/Fail Criteria</b>	Pass if the VO membership request page provides the requested functionality.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>VO Membership Authorisation</b>	
<b>ID</b>	<b>ATTAUTH_WEB_3</b>
<b>Description</b>	VO admins should be able to allow or deny pending membership request from the web interface.
<b>Mandatory</b>	YES
<b>Applicability</b>	Web Portal for Attribute Authority Appliances management
<b>Input from Technology Provider</b>	Provide a web page for listing pending membership requests and allowing or denying them.
<b>Test Description</b>	<b>Pre-condition</b> VO Web server running, valid admin credentials, membership request. <b>Test</b> Admin accepts the membership request. <b>Expected Outcome</b> User is added to the VO. Notification email is sent to user.
	<b>Pre-condition</b> VO Web server running, valid admin credentials, membership request. <b>Test</b> Admin rejects the membership request. <b>Expected Outcome</b> User is not added to the VO.
<b>Pass/Fail Criteria</b>	Pass if the admin can accept/reject VO membership requests from users.
<b>Related Information</b>	

<b>VO Administration</b>	
<b>ID</b>	<b>ATTAUTH_WEB_4</b>
<b>Description</b>	Authorized users should be able to manage VO groups, roles, attributes and ACLs from the web interface.
<b>Mandatory</b>	YES
<b>Applicability</b>	Web Portal for Attribute Authority Appliances management
<b>Input from Technology Provider</b>	Provide pages for managing the groups, roles, attributes and ACLs of the VO. They must allow the creation of new items, assigning and removing users for those items, deleting items.
<b>Test Description</b>	<b>Pre-condition</b> VO Web server running, valid credentials. <b>Test</b> Create new group/role/attribute using web interface. <b>Expected Outcome</b> The new group/role/attribute is created.
	<b>Pre-condition</b> VO Web server running, valid credentials. <b>Test</b> Remove existing group/role/attribute using web interface. <b>Expected Outcome</b> The group/role/attribute is deleted.
	<b>Pre-condition</b> VO Web server running, valid credentials. <b>Test</b> Assign group/role/attribute to user using web interface. <b>Expected Outcome</b> The group/role/attribute is assigned to user.
	<b>Pre-condition</b> VO Web server running, valid credentials. <b>Test</b> Remove user from group/role/attribute using web interface. <b>Expected Outcome</b> User no longer has group/role/attribute assigned.
<b>Pass/Fail Criteria</b>	Pass if the admin can accept/reject VO membership requests from users.
<b>Related Information</b>	

<b>VO Browse</b>	
<b>ID</b>	<b>ATTAUTH_WEB_5</b>
<b>Description</b>	Authorized user should be able to browse the VO members, groups, roles or attributes.
<b>Mandatory</b>	YES
<b>Applicability</b>	Web Portal for Attribute Authority Appliances management
<b>Input from Technology Provider</b>	Provide pages for listing the VO members, groups, roles and attributes for a given VO.
<b>Test Description</b>	<p><b>Pre-condition</b> VO Web server running, valid credentials.</p> <p><b>Test</b> Browse VO members by groups/roles/attributes.</p> <p><b>Expected Outcome</b> Web pages with list of users for groups/roles/attributes is delivered.</p>
<b>Pass/Fail Criteria</b>	Pass if the VO browsing pages are provided and members can be listed by groups, roles and, or attributes.
<b>Related Information</b>	
<b>Revision Log</b>	

### 3 AUTHORISATION

#### XAMCL

#### 3.1 Policy Management

Policy Listing	
<b>ID</b>	<b>AUTHZ_ MGMT_1</b>
<b>Description</b>	Administrators must be able to list the policies stored in the service.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances with PAP
<b>Input from Technology Provider</b>	Test of policy listing
<b>Test Description</b>	<p><b>Pre-condition</b> Policy repository available.</p> <p><b>Test</b> List policies</p> <p><b>Expected Outcome</b> List of stored policies.</p>
<b>Pass/Fail Criteria</b>	Pass if the test suite is provided and passes
<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 6]
<b>Revision Log</b>	



<b>Policy Repositories Management</b>	
<b>ID</b>	<b>AUTHZ_ MGMT_2</b>
<b>Description</b>	Administrators must be able to manage the remote Policy Repositories to be used by the service.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances with PAP

<b>Input from Technology Provider</b>	Test for the management of Policy Repositories that will be used in the service.
<b>Test Description</b>	<b>Pre-condition</b> Remote policy repository available. <b>Test</b> Add remote policy repository. <b>Expected Outcome</b> Remote repository added; remote policies retrieved.
	<b>Pre-condition</b> Configured Remote policy repository. <b>Test</b> Remove remote policy repository. <b>Expected Outcome</b> Remote repository removed, policies no longer available.
	<b>Pre-condition</b> Configured Remote policy repository <b>Test</b> Update remote policies. <b>Expected Outcome</b> Remote policies retrieved.
	<b>Pre-condition</b> Enabled policy repository. <b>Test</b> Disable policy repository. <b>Expected Outcome</b> Policies from repository no longer used.
	<b>Pre-condition</b> Disabled policy repository. <b>Test</b> Enable policy repository. <b>Expected Outcome</b> Policies from repository used.
	<b>Pre-condition</b> Several policies repositories configured. <b>Test</b> Show policy repository order. <b>Expected Outcome</b> Policy repository order shown.
	<b>Pre-condition</b> Several policies repositories configured. <b>Test</b> Set new policy repository order. <b>Expected Outcome</b> New policy repository is set.
	<b>Pass/Fail</b>



<b>Criteria</b>	disabling, enabling and establishing an order for them.
<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 6]
<b>Revision Log</b>	

## 3.2 Policy Definition

### 3.2.1 Central policy management (Argus)

<b>(un) Banning Policies</b>		
<b>ID</b>	<b>AUTHZ_PCYDEF_1</b>	
<b>Description</b>	Administrators must be able to define policies that ban users or FQANs.	
<b>Mandatory</b>	YES	
<b>Applicability</b>	Authorisation Appliances with PAP	
<b>Input from Technology Provider</b>	Test of banning for different user DNs and FQANs; test also re-establishing already existing banning.	
<b>Test Description</b>	<b>Pre-condition</b> Policy repository available. Banning policy for DN/FQAN not defined <b>Test</b> Define ban policy for DN/FQAN <b>Expected Outcome</b> Ban policy for DN/FQAN stored in policy repository.	
	<b>Pre-condition</b> Policy repository available. Banning policy for DN/FQAN defined <b>Test</b> Unban policy for DN/FQAN <b>Expected Outcome</b> Ban policy for DN/FQAN no longer stored in policy repository.	
	<b>Pass/Fail Criteria</b>	Pass if the banning policies can be defined (and removed)
	<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 6]
<b>Revision Log</b>		

Policy Definition from file	
<b>ID</b>	<b>AUTHZ_PCYDEF_2</b>
<b>Description</b>	Administrators must be able to manage the policies in the service, loading them from a file. File syntax could be XAMCL or a simplified equivalent.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances with PAP
<b>Input from Technology Provider</b>	Test of policy definitions for different DNs and FQANs, test both <i>allow</i> and <i>deny</i> policies for different resources and actions.
<b>Test Description</b>	<b>Pre-condition</b> Policy repository available. Policy file with policies. <b>Test</b> Add policies from file. <b>Expected Outcome</b> Policies from file now stored in repository.
	<b>Pre-condition</b> Policy repository available with a policy to update. Update description in policy file. <b>Test</b> Update policy from file. <b>Expected Outcome</b> Update policy stored in repository.
	<b>Pre-condition</b> Policy repository available with a policy to remove. <b>Test</b> Remove policy. <b>Expected Outcome</b> Policy no longer stored in repository.
<b>Pass/Fail Criteria</b>	Pass if the administrator cans add/update/remove policies for DNs and or FQANs.
<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 6]
<b>Revision Log</b>	

### 3.2.2 Service Based Authorisation (Not Argus)

<b>Ban User/FQAN</b>	
<b>ID</b>	<b>AUTHZ_PCYDEF_3</b>
<b>Description</b>	Administrators must be able to define policies that ban users or FQANs.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances without PAP
<b>Input from Technology Provider</b>	Test of banning for different user DNs and FQANs.
<b>Test Description</b>	<b>Pre-condition</b> Configured system.
	<b>Test</b> Ban policy for DN/FQAN. Test access for DN/FQAN.
	<b>Expected Outcome</b> Ban policy is correctly enforced.
	<b>Pre-condition</b> Configured system. Banning policy for DN/FQAN defined
<b>Test Description</b>	<b>Test</b> Unban DN/FQAN. Test access for DN/FQAN.
	<b>Expected Outcome</b> DN/FQAN is allowed.
<b>Pass/Fail Criteria</b>	Pass if the banning policies can be defined and enforced.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>Allowed users definition</b>	
<b>ID</b>	<b>AUTHZ_PCYDEF_4</b>
<b>Description</b>	Administrators must be determine which users/FQANs are allowed in the system
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances without PAP
<b>Input from Technology Provider</b>	Test for allowing DNs/FQANs in the system.
<b>Test Description</b>	<p><b>Pre-condition</b> Configured system.</p> <p><b>Test</b> Allow DN/FQAN access into system. Test access fro DN/FQAN.</p> <p><b>Expected Outcome</b> DN/FQAN is allowed in the system.</p>
<b>Pass/Fail Criteria</b>	Pass if the policies can be defined and enforced
<b>Related Information</b>	
<b>Revision Log</b>	V2: Restricted policy definition to allowing access (full control of policy is expected in Argus like systems)

### 3.3 Policy Decision Point

XACML Interface	
<b>ID</b>	<b>AUTHZ_PDP_1</b>
<b>Description</b>	PDPs must support the XACML interface
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances with PDP
<b>Input from Technology Provider</b>	Test suite of for XACML requests for accessing the PDP from clients (PEP). The test suite must cover correct and erroneous input for the API, authorize and deny policies taking into account DNs, VOs, FQAN, and proxies.
<b>Test Description</b>	<p><b>Pre-condition</b> Configured PEP and PDP.</p> <p><b>Test</b> Testsuite for XACML requests to PDP</p> <p><b>Expected Outcome</b> Log of actions.</p>
<b>Pass/Fail Criteria</b>	Pass if the testsuite is provided and passes.
<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 6] XACML [R 7]
<b>Revision Log</b>	

### 3.4 Policy Enforcement

Policy Enforcement	
<b>ID</b>	<b>AUTHZ_PEP_1</b>
<b>Description</b>	The defined policies in the authorisation capability must be enforced when applicable
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances
<b>Input from Technology Provider</b>	Test suite for the policy enforcement, test for policies expressed in terms of DNs and/or FQANs. The user can be authenticated with a certificate chain or SAML assertions.
<b>Test Description</b>	<b>Pre-condition</b> Configured system. User certificate chain (or SAML assertions) of user allowed to perform action.
	<b>Test</b> Test if the user can perform action
	<b>Expected Outcome</b> Permission is granted to user.
	<b>Pre-condition</b> Configured system. User certificate chain of user (or SAML assertions) NOT allowed to perform action.
<b>Test Description</b>	<b>Test</b> Test if the user can perform action
	<b>Expected Outcome</b> Permission is NOT granted to user.
<b>Pass/Fail Criteria</b>	Pass if policies are correctly enforced for supported authentication systems (user certificates or SAML assertions).
<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 6]
<b>Revision Log</b>	V2: Added SAML assertions support.



<b>User Mapping</b>	
<b>ID</b>	<b>AUTHZ_PEP_2</b>
<b>Description</b>	The authorisation capability should provide mapping of authorized users to local accounts.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances
<b>Input from Technology Provider</b>	Test Suite for the mapping of users to local accounts; test with and without VOMS attributes, and with/without pool accounts. The preferred mapping mechanism is the gridmap dir using gridmapfiles for defining the mappings.
<b>Test Description</b>	<b>Pre-condition</b> Configured system. No previous mapping for user. <b>Test</b> Accepted authorisation. <b>Expected Outcome</b> GID/UID of the mapping returned. Primary group determined by FQAN if available. New entry in grid map is created.
	<b>Pre-condition</b> Configured system. Previous mapping for user existing. <b>Test</b> Accepted authorisation. <b>Expected Outcome</b> GID/UID of the previous mapping returned.
<b>Pass/Fail Criteria</b>	Pass if the mapping is performed correctly for authorised users using gridmap dir entries. The mapping of accounts is done according to a gridmapfile. Pool accounts must be supported. Other mechanisms for mapping may be accepted.
<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 6]
<b>Revision Log</b>	

## 4 CREDENTIAL MANAGEMENT

### 4.1 Credential Management Interface

Credential Storage	
<b>ID</b>	<b>CREDMGMT_IFACE_1</b>
<b>Description</b>	Credential Management Appliances must provide an interface for storing user credentials.
<b>Mandatory</b>	YES
<b>Applicability</b>	Credential Management Appliances
<b>Input from Technology Provider</b>	Test suite for storing user credentials in the service (with and without VOMS extensions).
<b>Test Description</b>	<b>Pre-condition</b> Valid user credentials (X509 certificate), user allowed in the service. <b>Test</b> Store user credential in the service <b>Expected Outcome</b> Credential is stored in the system
	<b>Pre-condition</b> Valid user credentials (X509 certificate), user not allowed in the service. <b>Test</b> Store user credential in the service <b>Expected Outcome</b> Error message is issued; no credentials are stored.
<b>Pass/Fail Criteria</b>	User can successfully store the credentials in the appliance with and without VOMS extensions.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>Credential Retrieval</b>	
<b>ID</b>	<b>CREDMGMT_IFACE_2</b>
<b>Description</b>	Credential Management Appliances must provide an interface for retrieving user credentials in the service.
<b>Mandatory</b>	YES
<b>Applicability</b>	Credential Management Appliances
<b>Input from Technology Provider</b>	Test suite for retrieving user credentials in the service (with and without VOMS extensions).
<b>Test Description</b>	<b>Pre-condition</b> Valid user credentials stored in service, user allowed in the service. <b>Test</b> Retrieve user credential <b>Expected Outcome</b> User credentials returned.
	<b>Pre-condition</b> No valid user credentials stored in the service. <b>Test</b> Retrieve user credential <b>Expected Outcome</b> Error message is issued; no credentials are returned.
<b>Pass/Fail Criteria</b>	User can successfully retrieve previously store credentials from the appliance with and without VOMS extensions.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>Credential Renewal</b>	
<b>ID</b>	<b>CREDMGMT_IFACE_3</b>
<b>Description</b>	Credential Management Appliances must provide an interface for renewing user credentials in the service.
<b>Mandatory</b>	YES
<b>Applicability</b>	Credential Management Appliances
<b>Input from Technology Provider</b>	Test suite for renewing user credentials in the service (with and without VOMS extensions).
<b>Test Description</b>	<b>Pre-condition</b> Valid user credentials stored in service, host allowed to renew credentials. <b>Test</b> Renew user credential <b>Expected Outcome</b> User credentials renewed.
	<b>Pre-condition</b> Valid user credentials stored in service, host not allowed to renew credentials. <b>Test</b> Renew user credential <b>Expected Outcome</b> Error message is issued; no credentials are renewed.
	<b>Pre-condition</b> No valid user credentials stored in the service. <b>Test</b> Renew user credential <b>Expected Outcome</b> Error message is issued; no credentials are renewed.
<b>Pass/Fail Criteria</b>	Services/Users can successfully renew previously retrieved credentials from the appliance with and without VOMS extensions.
<b>Related Information</b>	
<b>Revision Log</b>	

## 4.2 Institutional Authentication Systems Linking

Institutional Authentication Linking	
<b>ID</b>	<b>CREDMGMT_LINK_1</b>
<b>Description</b>	Users should be able to access grid resources using institutional authentication systems.
<b>Mandatory</b>	NO
<b>Applicability</b>	Credential Management Appliances
<b>Input from Technology Provider</b>	Test suite for linking institutional authentication system with the Credential Management implementation
<b>Test Description</b>	<p><b>Pre-condition</b> Valid institutional user credentials, user allowed in the service.</p> <p><b>Test</b> User requests grid credentials using his/her institutional credentials</p> <p><b>Expected Outcome</b> Short-lived X.509 credential for used created.</p>
<b>Pass/Fail Criteria</b>	Short-lived X.509 credentials are created for authorized users. Test should be provided for each of the authentication systems supported (e.g. Kerberos or Shibboleth)
<b>Related Information</b>	
<b>Revision Log</b>	

## 5 REFERENCES

<b>R 1</b>	UMD roadmap: <a href="https://documents.egi.eu/public/ShowDocument?docid=100">https://documents.egi.eu/public/ShowDocument?docid=100</a>
<b>R 2</b>	Generic UMD Quality Criteria
<b>R 3</b>	GridSite Delegation Protocol: <a href="http://www.gridsite.org/wiki/Delegation_protocol">http://www.gridsite.org/wiki/Delegation_protocol</a>
<b>R 4</b>	Globus Delegation Service: <a href="http://www.globus.org/toolkit/docs/4.0/security/delegation/">http://www.globus.org/toolkit/docs/4.0/security/delegation/</a>
<b>R 5</b>	European Policy Management Authority for Grid Authentication (EuGridPMA): <a href="http://www.eugridpma.org/">http://www.eugridpma.org/</a>
<b>R 6</b>	ARGUS Authorization Service: <a href="https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework">https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework</a>
<b>R 7</b>	XACML: <a href="http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf">http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf</a>