



EGI-InSPIRE

UMD SECURITY CAPABILITIES QUALITY CRITERIA v3 DRAFT 2

Document identifier:	EGI-SECURITY-QC-V3-DRAFT2.docx
Date:	26/01/2012
Document Link:	https://documents.egi.eu/document/718

Abstract

This document describes the UMD Security Capabilities Quality Criteria.



Copyright notice

Copyright © Members of the EGI-InSPIRE Collaboration, 2010. See 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 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
2	03/08/2011	Release 2, taking comments from EMI	E. Fernández
3 DRAFT 1	13/10/2011	First draft of release 3	Enol Fernández
3 DRAFT 2	24/01/2012	Second draft of release 3	Enol Fernández

TABLE OF CONTENTS

1	Authentication	5
1.1	Authentication Interface	5
	AUTHN_IFACE_1	5
	AUTHN_IFACE_2	6
1.2	Delegation Interface	7
	AUTHN_DELEG_1	7
1.3	CAs root certificates Distribution	8
	AUTHN_CA_1	8
	AUTHN_CA_2	9
	AUTHN_CA_3	10
2	Attribute Authority	11
2.1	Attribute Authority Interface	11
	ATTAUTH_IFACE_1	11
	ATTAUTH_IFACE_2	12
	ATTAUTH_IFACE_3	13
	ATTAUTH_IFACE_4	14
2.2	VO management	15
	ATTAUTH_MGMT_1	15
	ATTAUTH_MGMT_2	16
	ATTAUTH_MGMT_3	17
	ATTAUTH_MGMT_4	19
	ATTAUTH_MGMT_5	20
2.3	VO Management Web Interface (VOMS-Admin)	21
	ATTAUTH_WEB_1	21
	ATTAUTH_WEB_2	22
	ATTAUTH_WEB_3	23
	ATTAUTH_WEB_4	24
	ATTAUTH_WEB_5	25
3	Authorisation	26
3.1	Policy Management	26
	AUTHZ_MGMT_1	26
	AUTHZ_MGMT_2	27
3.2	Policy Definition	29
3.2.1	Central policy management (Argus)	29
	AUTHZ_PCYDEF_1	29
	AUTHZ_PCYDEF_2	30
3.2.2	Service Based Authorisation (Not Argus)	31
	AUTHZ_PCYDEF_3	31
	AUTHZ_PCYDEF_4	32
3.3	Policy Decision Point	33
	AUTHZ_PDP_1	33
3.4	Policy Enforcement	34
	AUTHZ_PEP_1	34
	AUTHZ_PEP_2	35
4	Credential Management	36
4.1	Credential Management Interface	36
	CREDMGMT_IFACE_1	36
	CREDMGMT_IFACE_2	37



CREDMGMT_IFACE_3.....	38
4.2 Institutional Authentication Systems Linking	39
CREDMGMT_LINK_1.....	39
5 References	40

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

X.509 Certificate support	
ID	AUTHN_IFACE_1
Description	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.
Mandatory	YES
Applicability	Authentication Appliances.
Input from Technology Provider	X.509 proxy support for authentication If the component exposes a WebService that requires authentication, it should use the X.509 certificates/proxies with the https protocol.
Pass/Fail Criteria	X.509 proxies are accepted for authentication. WebServices 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.
Related Information	UMD Roadmap [R 1]
Revision Log	V2: Added GSI (httpg) exception for products that have not yet transitioned

SAML authentication	
ID	AUTHN_IFACE_2
Description	SAML 2.0 can be used as authentication interface within the infrastructure.
Mandatory	NO
Applicability	Authentication Appliances with SAML 2.0 support.
Input from Technology Provider	SAML 2.0 support for authentication. Ideally, a test suite for this support.
Pass/Fail Criteria	Pass if SAML2.0 authentication is supported in the appliance.
Related Information	UMD Roadmap [R 1]
Revision Log	

1.2 Delegation Interface

Delegation Interface	
ID	AUTHN_DELEG_1
Description	Delegation of credentials must be provided using one of the supported delegation interfaces: GridSite or Globus 4.
Mandatory	YES
Applicability	Authentication Appliances that provide (require) delegation.
Input from Technology Provider	Delegation interface that includes all functionality of the GridSite WSDL. Correct handling for erroneous input.
Pass/Fail Criteria	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.
Related Information	UMD Roadmap [R 1] GridSite Delegation [R 30] Globus Delegation [R 31]
Revision Log	V2: Merged AUTHN_DELEG_1 & 2.

1.3 CAs root certificates Distribution

These QC deal with the distribution of the EuGridPMA [R 32] root certificates.

CA Checksum							
ID	AUTHN_CA_1						
Description	The CA distribution must assure that the distributed CA certificates are correct.						
Mandatory	YES						
Applicability	Trust Anchor Distribution						
Input from Technology Provider	Checksum test of each of the root certificates distributed.						
Test Description	<table border="0"> <tr> <td>Pre-condition</td> <td>None</td> </tr> <tr> <td>Test</td> <td>Test checksum of the CA certificates.</td> </tr> <tr> <td>Expected Outcome</td> <td>All checksums are correct.</td> </tr> </table>	Pre-condition	None	Test	Test checksum of the CA certificates.	Expected Outcome	All checksums are correct.
Pre-condition	None						
Test	Test checksum of the CA certificates.						
Expected Outcome	All checksums are correct.						
Pass/Fail Criteria	All CA certificates have correct checksum.						
Related Information							
Revision Log							

CA valid dates	
ID	AUTHN_CA_2
Description	Dates of the distributed CA certificates are valid for the current date.
Mandatory	YES
Applicability	Trust Anchor Distribution
Input from Technology Provider	Data validity test of each of the root certificates distributed.
Test Description	<p>Pre-condition None</p> <p>Test Check the current date is in the range of the valid dates of the certificate.</p> <p>Expected Outcome All dates are valid.</p> <p>Sample Test</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>
Pass/Fail Criteria	All CA certificates have correct dates.
Related Information	
Revision Log	

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

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

2 ATTRIBUTE AUTHORITY

2.1 Attribute Authority Interface

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

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

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

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

2.2 VO management

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

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

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

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

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

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

ACL Management	
ID	ATTAUTH_ MGMT_5
Description	Authorized users must be able to change the different ACLs of the VO.
Mandatory	YES
Applicability	Attribute Authority Appliances
Input from Technology Provider	Support for changing ACLs of users of the VO.
Test Description	Pre-condition Authorized user to manage ACLs. Test Change ACL for a given user. Expected Outcome ACL is correctly changed.
	Pre-condition Non-Authorized user to manage ACLs. Test Change ACL for a given user. Expected Outcome No action performed, error message issued.
Pass/Fail Criteria	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"> • browse users of VO • management of groups • management of roles • management of attributes • management of ACL • add/remove users
Related Information	UMD Roadmap [R 1]
Revision Log	

2.3 VO Management Web Interface (VOMS-Admin)

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

VO Membership Request	
ID	ATTAUTH_WEB_2
Description	Users should be able to request membership to a VO from the web interface.
Mandatory	YES
Applicability	Web Portal for Attribute Authority Appliances management
Input from Technology Provider	<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"> • Full name • Institution • Contact details (phone, e-mail, address) <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>
Test Description	<p>Pre-condition VO Web server running, valid credentials of user.</p> <p>Test User requests membership from VO.</p> <p>Expected Outcome User gets an email to confirm the membership request.</p>
	<p>Pre-condition VO Web server running, valid credentials of user, membership confirmation link.</p> <p>Test User accesses the membership confirmation link.</p> <p>Expected Outcome VO admin(s) receive a notification of the new request.</p>
Pass/Fail Criteria	Pass if the VO membership request page provides the requested functionality.
Related Information	
Revision Log	

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

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

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

3 AUTHORISATION

3.1 Policy Management

Policy Listing	
ID	AUTHZ_ MGMT_1
Description	Administrators must be able to list the policies stored in the service.
Mandatory	YES
Applicability	Authorisation Appliances with PAP
Input from Technology Provider	Support for policy listing
Test Description	<p>Pre-condition Policy repository available.</p> <p>Test List policies</p> <p>Expected Outcome List of stored policies.</p>
Pass/Fail Criteria	Pass if the test suite passes
Related Information	UMD Roadmap [R 1] Argus [R 33]
Revision Log	

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

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



Criteria	disabling, enabling and establishing an order for them.
Related Information	UMD Roadmap [R 1] Argus [R 33]
Revision Log	

3.2 Policy Definition

3.2.1 Central policy management (Argus)

(un) Banning Policies		
ID	AUTHZ_PCYDEF_1	
Description	Administrators must be able to define policies that ban users or FQANs.	
Mandatory	YES	
Applicability	Authorisation Appliances with PAP	
Input from Technology Provider	Support for banning different user DNs and FQANs; also support re-establishing already existing banning.	
Test Description	Pre-condition Policy repository available. Banning policy for DN/FQAN not defined Test Define ban policy for DN/FQAN Expected Outcome Ban policy for DN/FQAN stored in policy repository.	
	Pre-condition Policy repository available. Banning policy for DN/FQAN defined Test Unban policy for DN/FQAN Expected Outcome Ban policy for DN/FQAN no longer stored in policy repository.	
	Pass/Fail Criteria	Pass if the banning policies can be defined (and removed)
	Related Information	UMD Roadmap [R 1] Argus [R 33]
Revision Log		

Policy Definition from file	
ID	AUTHZ_PCYDEF_2
Description	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.
Mandatory	YES
Applicability	Authorisation Appliances with PAP
Input from Technology Provider	Support for policy definitions with different DNs and FQANs, both <i>allow</i> and <i>deny</i> policies for different resources and actions.
Test Description	Pre-condition Policy repository available. Policy file with policies. Test Add policies from file. Expected Outcome Policies from file now stored in repository.
	Pre-condition Policy repository available with a policy to update. Update description in policy file. Test Update policy from file. Expected Outcome Update policy stored in repository.
	Pre-condition Policy repository available with a policy to remove. Test Remove policy. Expected Outcome Policy no longer stored in repository.
Pass/Fail Criteria	Pass if the administrator cans add/update/remove policies for DNs and or FQANs.
Related Information	UMD Roadmap [R 1] Argus [R 33]
Revision Log	

3.2.2 Service Based Authorisation (Not Argus)

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

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

3.3 Policy Decision Point

XACML Interface	
ID	AUTHZ_PDP_1
Description	PDPs should support the XACML interface
Mandatory	YES
Applicability	Authorisation Appliances with PDP
Input from Technology Provider	Support for XACML requests for accessing the PDP from clients (PEP). Ideally, a complete test suite of the API, that covers correct and erroneous input for the API, authorize and deny policies taking into account DNS, VOs, FQAN, and proxies.
Test Description	<p>Pre-condition Configured PEP and PDP.</p> <p>Test Test suite for XACML requests to PDP</p> <p>Expected Outcome Log of actions.</p>
Pass/Fail Criteria	Pass if the XACML API is supported. Non-complete implementations of the API may be accepted if this is documented and the missing functionality does not affect the operations of the infrastructure.
Related Information	UMD Roadmap [R 1] Argus [R 33] XACML [R 34]
Revision Log	

3.4 Policy Enforcement

Policy Enforcement	
ID	AUTHZ_PEP_1
Description	The defined policies in the authorisation capability must be enforced when applicable
Mandatory	YES
Applicability	Authorisation Appliances
Input from Technology Provider	Support for the policy enforcement, with policies expressed in terms of DN's and/or FQANs. The user may be authenticated with a certificate chain or with SAML assertions.
Test Description	Pre-condition Configured system. User certificate chain (or SAML assertions) of user allowed to perform action.
	Test Test if the user can perform action
	Expected Outcome Permission is granted to user.
	Pre-condition Configured system. User certificate chain of user (or SAML assertions) NOT allowed to perform action.
Test Description	Test Test if the user can perform action
	Expected Outcome Permission is NOT granted to user.
Pass/Fail Criteria	Pass if policies are correctly enforced for supported authentication systems (user certificates or SAML assertions).
Related Information	UMD Roadmap [R 1] Argus [R 33]
Revision Log	V2: Added SAML assertions support.

User Mapping	
ID	AUTHZ_PEP_2
Description	The authorisation capability should provide mapping of authorized users to local accounts.
Mandatory	YES
Applicability	Authorisation Appliances
Input from Technology Provider	Support for mapping of users to local accounts; with/without VOMS attributes, and with/without pool accounts. The preferred mapping mechanism is the gridmap dir using gridmapfiles for defining the mappings.
Test Description	Pre-condition Configured system. No previous mapping for user.
	Test Accepted authorisation.
	Expected Outcome GID/UID of the mapping returned. Primary group determined by FQAN if available. New entry in grid map is created.
	Pre-condition Configured system. Previous mapping for user existing.
Test Description	Test Accepted authorisation.
	Expected Outcome GID/UID of the previous mapping returned.
Pass/Fail Criteria	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.
Related Information	UMD Roadmap [R 1] Argus [R 33]
Revision Log	

4 CREDENTIAL MANAGEMENT

4.1 Credential Management Interface

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

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

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

4.2 Institutional Authentication Systems Linking

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

5 REFERENCES

R 1	UMD roadmap: https://documents.egi.eu/public/ShowDocument?docid=100
R 2	Web Services Data Access and Integration – The Relational Realisation (WS-DAIR) Specification, Version 1.0
R 3	Web Services Data Access and Integration – The XML Realization (WS-DAIX) Specification, Version 1.0
R 4	OGSA-DAI: http://www.ogsadai.org.uk/
R 5	gLite LFC: https://twiki.cern.ch/twiki/bin/view/EGEE/GliteLFC
R 6	AMGA: http://amga.web.cern.ch/amga/
R 7	AMGA WSDL: http://amga.web.cern.ch/amga/downloads/Metadata.wsdl
R 8	AMGA streaming API: http://amga.web.cern.ch/amga/protocol.html
R 9	AMGA Metadata Queries: http://amga.web.cern.ch/amga/queries.html
R 10	A. Konstantinov, ARC Computational Job Management Component – A-REX, NORDUGRID-TECH-14
R 11	CREAM: http://grid.pd.infn.it/cream/
R 12	EMI-ES: https://twiki.cern.ch/twiki/bin/view/EMI/EmiExecutionService
R 13	GRAM5: http://www.globus.org/toolkit/docs/latest-stable/execution/gram5/
R 14	OGF DRMAA: http://www.drmaa.org/
R 15	OGSA Basic Execution Service v1.0: http://www.ogf.org/documents/GFD.108.pdf
R 16	UNICORE UAS: http://www.unicore.eu/unicore/architecture/service-layer.php#anchor_uas
R 17	gLite WMS: http://web.infn.it/gLiteWMS/
R 18	SAGA-CORE-WG: A Simple API for Grid Applications (SAGA) v1.0 (GFD.90)
R 19	SAGA (A Simple API for Grid Applications): http://saga.cct.lsu.edu/
R 20	Instrument Element: http://www.dorii.eu/resources/adaptation:middleware:IE
R 21	DORII (Deployment of Remote Instrumentation Infrastructure) Project: http://www.dorii.eu/
R 22	GlueSchema Specification v1.3: http://glueschema.forge.cnaf.infn.it/Spec/V13

R 23	GlueSchema Specification v2.0: http://www.ogf.org/documents/GFD.147.pdf
R 24	JMS (Java Message Service Specification) 1.1: http://www.oracle.com/technetwork/java/jms/index.html
R 25	AMQP (Advanced Message Queuing Protocol): http://www.amqp.org/confluence/display/AMQP/Advanced+Message+Queuing+Protocol
R 26	Nagios Config Generator: https://tomtools.cern.ch/confluence/display/SAM/NCG
R 27	My EGI portal: https://tomtools.cern.ch/confluence/display/SAM/MyEGI
R 28	SAM Probes Documentation: https://tomtools.cern.ch/confluence/display/SAM/Probes
R 29	Accounting Portal: http://accounting.egi.eu/
R 30	GridSite Delegation Protocol: http://www.gridsite.org/wiki/Delegation_protocol
R 31	Globus Delegation Service: http://www.globus.org/toolkit/docs/4.0/security/delegation/
R 32	European Policy Management Authority for Grid Authentication (EuGridPMA): http://www.eugridpma.org/
R 33	ARGUS Authorization Service: https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework
R 34	XACML: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
R 35	Hydra encrypted file storage: https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS
R 36	gLite FTS: https://twiki.cern.ch/twiki/bin/view/EGEE/GLiteFTS
R 37	SRM v2.2: http://www.ggf.org/documents/GFD.129.pdf
R 38	S2 Test: http://s-2.sourceforge.net/
R 39	SRM-Tester: https://sdm.lbl.gov/twiki/bin/view/Software/SRMTester/WebHome
R 40	Lcg-utils: http://grid-deployment.web.cern.ch/grid-deployment/documentation/LFC_DPM/lcg_util/
R 41	Lcg-utils test suite: http://glite.cvs.cern.ch/cgi-bin/glite.cgi/org.glite.testsuites.ctb/UI/tests/test-lcg-utils.sh?view=markup
R 42	Open Cloud Computing Interface WG, OGF, http://www.ggf.org/gf/group_info/view.php?group=occi-wg
R 43	Virtualization Management (VMAN), DMTF http://www.dmtf.org/standards/vman