EGI-InSPIRE

UMD Quality Criteria
v5

Document identifier:	EGI-QC-V5-ARGUS.doc
Date:	**23/04/2013**
Document Link:	https://documents.egi.eu/document/1153

Abstract

This document describes the Quality Criteria that all software of the UMD distribution must meet.



Document Log

Issue	Date	Comment	Author/Partner
v0.1	02/11/2010	First draft	Enol Fernández
v1.0	03/11/2010	Changed Management, Traceability and Monitoring section	Enol Fernández
v1.1	03/11/2010	Added Probe description in GEN_MON_1	Enol Fernández
v1.2	11/11/2010	Some formatting update	Enol Fernández
v1.3	31/01/2011	Better test specification	Enol Fernández
1.4	09/02/2011	Review of criteria	Enol Fernández
2 DRAFT 1	24/06/2011	Preparation of new release	Enol Fernández
2	02/08/2011	Reorganisation, added new criteria.	Enol 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
4 DRAFT 1	21/05/2012	First public draft of release 4	Enol Fernández
4 DRAFT 2	23/07/2012	Second public draft of release 4	Enol Fernández
5	10/20/2013	Release 5	Enol Fernández

TABLE OF CONTENTS

1 DOCUMENTATION

Services in UMD must include a comprehensive documentation written in a uniform and clear style. All Quality Criteria described below may be met by a single document that contains all the requested sections.

Functional Description	
ID	**GENERIC_DOC_1**
Description	All products must provide a document with a brief functional description of the product.
Mandatory	NO
Applicability	All products

Input from Technology Provider	Document (or link) with a general description of the product that includes: • Purpose of the product • Capabilities meet by the product
Pass/Fail Criteria	The document should exist and contain the requested information.
Related Information	
Revision Log	V2: clarified the required documentation

Release Notes	
ID	**GENERIC_DOC_2**
Description	All products must provide a document with the release notes.
Mandatory	YES
Applicability	All products

Input from Technology Provider	Document (or link) with release notes of the product. They must include major the changes in the product: bug fixes, new features.
Pass/Fail Criteria	The document should exist and contain the requested information.
Related Information	
Revision Log	

User Documentation	
ID	**GENERIC_DOC_3**
Description	All products must provide a document describing how to use it.
Mandatory	NO
Applicability	All products with end-user tools and services.

Input from Technology Provider	Document (or link) with user guide describing the functionality of the software and how to use it.
Pass/Fail Criteria	The document should exist and contain the requested information.
Related Information	
Revision Log	

Online help (man pages)	
ID	**GENERIC_DOC_4**
Description	All products with end user command line tools must include man pages or online help.
Mandatory	NO
Applicability	All products with command line tools.

Input from Technology Provider	Man pages with information about the usage of commands. If man pages are not available, comprehensive help options must be included with the command with information about the usage (i.e. –h/--help option)
Pass/Fail Criteria	Online help should be available (man pages or command line help). Command line help should give meaningful cues (i.e., only a list of single-letter options is not sufficient) If both command line help (-h option) and man pages are provided they **must** be mutually consistent (describe the same set of options and their meaning).
Related Information	GGUS ticket # 73214
Revision Log	V3: Tighten wording to avoid situations as described in GGUS #73214

API Documentation	
ID	**GENERIC_DOC_5**
Description	Public API of product/appliances must be documented.
Mandatory	NO
Applicability	All products with public API.

Input from Technology Provider	Documentation (or link) of the API of the product. The documentation *should* cover all the existing public functionality of the API.
Pass/Fail Criteria	The document should exist and contain the API documentation. If the product implements a well-known or standard API, any missing functionality must be documented.
Related Information	
Revision Log	V2: review of the description

Administrator Documentation	
ID	**GENERIC_DOC_6**
Description	Products must provide an administrator guide describing installation, configuration and operation of the system.
Mandatory	NO
Applicability	All products managed by an administrator.

Input from Technology Provider	Documentation (or link) with requested documentation.
Pass/Fail Criteria	The document should exist and contain the requested information.
Related Information	
Revision Log	

Service Reference Card	
ID	**GENERIC_DOC_7**
Description	For each of the services that a product runs, document its characteristics with a reference card.
Mandatory	NO
Applicability	All products that need services for operation.

Input from Technology Provider	Documentation (or link) with requested documentation.
Pass/Fail Criteria	The document must exist and contain the following information for each service:

ServiceName	
Description	Description of the service
Init scripts	List of init scripts for the service, expected run levels
Daemons	List of daemons needed for the service
Configuration	List of configuration files used by the service
Logs	List of log files used by the service
Open ports	List of ports the service uses
Cron	List of crons used by the service
Other information	Any other relevant information about the service.

Related Information	
Revision Log	

Software License	
ID	**GENERIC_DOC_8**
Description	Products must have a compatible license for using them in the EGI Infrastructure
Mandatory	YES
Applicability	All products.

Input from Technology Provider	Product License (link or document).
Pass/Fail Criteria	Pass: if the license is available and is compatible with the EGI infrastructure. For Open Source products, compatible licenses are those accepted by the Open Source Initiative and categorized as "Popular and widely used or with strong communities": - Apache License, 2.0 (Apache-2.0) - BSD 3-Clause "New" or "Revised" license (BSD-3-Clause) - BSD 3-Clause "Simplified" or "FreeBSD" license (BSD-2-Clause) - GNU General Public License (GPL) - GNU Library or "Lesser" General Public License (LGPL) - MIT license (MIT) - Mozilla Public License 1.1 (MPL-1.1) - Common Development and Distribution License (CDDL-1.0) - Eclipse Public License (EPL-1.0) Other licenses accepted by the Open Source Initiative and listed as "Special Purpose" are compatible with the infrastructure (when applicable): - Educational Community License - IPA Font License (IPA) - NASA Open Source Agreement 1.3 (NASA-1.3) - Open Font License 1.1 (OFL-1.1) Any other license, and non Open Source products will be evaluated by the verification team in coordination with the Operations Community.
Related Information	Open Source Initiative Licenses by Category: http://www.opensource.org/licenses/category
Revision Log	V2: Moved from Software Release to documentation.

Release changes testing	
ID	**GENERIC_DOC_9**
Description	Changes in a release of a product must be tested.
Mandatory	NO
Applicability	All Products.

Input from Technology Provider	Tests (or documentation for the test results) for relevant changes described in the product release notes, including bug fixes and any new features.
Pass/Fail Criteria	Pass if the TP provides documentation of the tests performed to certify the release quality. The documentation *should* describe tests (and tests results) for all the changes included, especially bug fixes. The granularity of the testing documentation will be determined per release basis. In the case of missing tests, the verifier will decide if the provided information is enough to trust quality of the changes introduced in the software.
Related Information	MS503: Software Provisioning Process
Revision Log	V2: Better specification of the pass/fail criteria. Moved to documentation criteria V3: improvement of the pass/fail criteria. V4: better wording after IGE review, turned into NOT mandatory.

2 SOFTWARE DISTRIBUTION

Source Code Availability	
ID	**GENERIC_DIST_1**
Description	Open Source Products should provide their source code.
Mandatory	NO
Applicability	All Open Source Products.

Input from Technology Provider	Source code repository or source distribution of product with building documentation.
Pass/Fail Criteria	Open source products **must** publicly offer their source code and the license with the binaries. Build documentation (or link to it) should be available. Ideally, automatic or continuous build procedures exist.
Related Information	
Revision Log	V2: Changed ID (previously GENERIC_REL_2) V4: Merged GENERIC_DIST_1 and GENERIC_DIST_2 & Turned into not mandatory

Binary Distribution	
ID	**GENERIC_DIST_3**
Description	Products must be available in the native packaging format of the supported platform.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Binary distribution of product in the native packaging format of the supported platform (RPM, DEB, …)
Pass/Fail Criteria	- Binary packages using the standard packaging format of the OS (i.e. RPM, DEB...) must be provided for all the supported OS and/or architectures. - Packages **must** be signed by the TP - Packages *should* follow OS packaging policies (e.g. names of packages, use of filesystem hierarchy, init scripts). Any deviance from the policies must be documented. - Second level dependencies (i.e. software not provided by the TP in their repository) **must** be provided by the OS distribution or standard OS repositories (EPEL in SL5 & SL6). In the case of needing a different version for a specific package or packages from other repositories, the verifier will decide whether to accept or not the packages depending on the reason given for such dependencies on external packages.
Related Information	Verification reports from EMI release 1. #1357: Middleware use standard file locations GGUS #82417: https://ggus.eu/ws/ticket_info.php?ticket=82417
Revision Log	V2: Turn to mandatory, better description to avoid problems found in verification. Changed ID (previously GENERIC_REL_5) V4: Added requirement for signed packages.

3 SOFTWARE FEATURES

Backwards Compatibility	
ID	**GENERIC_SOFT_1**
Description	Minor/Revision releases of a product must be backwards compatible.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Products must maintain backwards compatibility between releases of the same major version. Ideally, TP provides tests to assure the backwards compatibility of the product.
Pass/Fail Criteria	All the changes in a minor or revision release *must* be backward compatible (test should be done with previous releases of clients within the same major version). Any new features should not introduce changes in the previous features.
Related Information	MS503: Software Provisioning Process IGE QC
Revision Log	

New features testing	
ID	**GENERIC_SOFT_2**
Description	Verification should cover testing of new features and bug fixes.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Release notes with changes in the software. The verifier will review each of the changes and check its correctness (whenever possible)
Pass/Fail Criteria	New features and bug fixes specified in the release notes work as documented. Some new features may not be tested if they are not relevant to the main capability of the product.
Related Information	MS503: Software Provisioning Process IGE QC
Revision Log	

4 SERVICE CRITERIA

4.1 Service Management

UMD products should have mechanisms for managing them, monitoring their status and tracing actions they perform on the system. Ideally, these should be also available remotely, allowing operators to react timely to problems in the infrastructure. This generic criteria for services is the minimum set of service related

Service control and status	
ID	**GENERIC_SERVICE_1**
Description	Services run by the product must provide a mechanism for starting, stopping and querying the status of the services.
Mandatory	YES
Applicability	All products that use services for operations.

Input from Technology Provider	Start/stop mechanism for each of the services following OS conventions. Ideally, provide a test suite for the mechanism as described below.	
Test Description	**Pre-condition**	Service is started
	Test	Start service
	Expected Outcome	No action taken, show a message stating the service is already started.
	Pre-condition	Service is stopped
	Test	Start service
	Expected Outcome	Service is started, show a message when it is started.
	Pre-condition	Service is started
	Test	Stop service
	Expected Outcome	Service is stopped, show a message stating the service is stopped.
	Pre-condition	Service is stopped
	Test	Stop service
	Expected Outcome	No action taken, show a message stating the service is already stopped.
	Pre-condition	Service is stopped
	Test	Check service status
	Expected Outcome	Show a message stating the service is stopped.

Test Description	**Pre-condition**	Service is started
	Test	Check service status
	Expected Outcome	Show a message stating the service is started.
Pass/Fail Criteria	Services run by the product must provide a mechanism for starting, stopping and querying the status of the services following the OS init scripts conventions (e.g. for Linux Distributions, check http://refspecs.freestandards.org/LSB_3.1.0/LSB-Core-generic/LSB-Core-generic/iniscrptact.html). They must work properly in **all** the cases described above. If the OS provides tools for configuring the services (chkconfig in RH based distros), these *should* work out of the box with the init scripts of the services	
Related Information	#2274: Service under RH following SystemV init system #1201: Homogeneity in service control.	
Revision Log	V3: Added related information, fix test conditions.	

4.2 Service logs

Log Files	
ID	**GENERIC_SERVICE_2**
Description	All services should create log files where the service administrator can trace most relevant actions taken.
Mandatory	YES
Applicability	All products that use services for operations.

Input from Technology Provider	List of logs generated by the service (the reference card of service should already include them)
Pass/Fail Criteria	List of logs is provided. They should follow the OS conventions for location and format so they can be treated with the standard tools of the OS (log rotation, collection with syslog, …)
Related Information	This criterion may be further specialized in the specific criteria for each product/capability determining which information must be logged or number/types of logs. #1357: Middleware use standard file locations
Revision Log	V2. Review of the criteria. V4: Added related information

4.3 Service Monitoring

All services in the EGI Infrastructure should provide monitoring probes that can be executed automatically by the EGI monitoring framework (based in Nagios). The probes should check the service responsiveness and correctness (good replies for typical requests).

Particular monitoring probes are defined at the Specific Quality Criteria document for Operations tools The probes that apply to all capabilities (generic probes) are identified as MON_PROBE_GENERIC_*xx*. For specific capabilities there might exist other probes that are described in the same document.

4.4 Service Accounting

All services in the EGI Infrastructure should provide ways of recording the use of resources within the infrastructure. The Accounting Capability described in the Operations Capabilities Criteria document specifies the criteria for the different appliances.

4.5 Availability, Reliability and Scalability.

The EGI Infrastructure depends on the uninterrupted performance of the installed software. All products should provide a reliable operation and should be able to handle growing amounts of work in a graceful manner. Specific criteria for the availability, reliability or scalability of appliances may be also defined in the criteria documents for each of the capabilities.

Service Reliability	
ID	**GENERIC_SERVICE_3**
Description	Services must maintain a good performance and reliability over long periods of time with normal operation.
Mandatory	NO
Applicability	All products that use services for operations.

Input from Technology Provider	Long running unattended operation test measuring performance of the product.	
Test Description	**Pre-condition**	Product is properly configured.
	Test	Start service and measure performance during operations.
	Expected Outcome	No significant performance degradation is observed in the system.
Pass/Fail Criteria	Service must not show performance degradation during a 3-day period. The most important parameters to check are: • stable memory usage • throughput and/or response times remain stable during the period of activity (they should be as good or better than at the beginning of the test for similar requests)	
Related Information		
Revision Log	V2: detailed pass/fail criteria	

Service Robustness	
ID	**GENERIC_SERVICE_4**
Description	Services should not produce unexpected results or become uncontrollable when taxed beyond normal capacity.
Mandatory	NO
Applicability	All products that use services for operations.

Input from Technology Provider	Assure that the services taxed beyond normal capacity do not produce unexpected results or become uncontrollable.
Pass/Fail Criteria	Services taxed beyond normal capacity: • should not become unresponsive to normal start/stop operations • must be able to start after a forceful stop • must not expose (potentially sensitive) memory contents to other processes • must not leave sensitive data in world-readable files • must not accept connections that would be refused under normal operating conditions
Related Information	TST_2 from IGE Quality Assurance.
Revision Log	

4.6 Service Configuration

Automatic Configuration	
ID	**GENERIC_SERVICE_5**
Description	Products that provide tools for configuration (yaim) that covers typical deployments must assure tools work as documented.
Mandatory	NO
Applicability	Products with automatic configuration tools

Input from Technology Provider	Tests of the automatic configuration tool (yaim) in typical deployment scenario.
Pass/Fail Criteria	Pass if the product can be configured as documented with the provided tool. Resulting configuration must prepare the product for operation without extra manual configuration steps (unless clearly documented).
Related Information	Yaim: https://twiki.cern.ch/twiki/bin/view/EGEE/YAIM UMD 1.0.0 Verification Reports.
Revision Log	V3: Removed the requirement for keeping manual configurations.

Default Password Configuration	
ID	**GENERIC_SERVICE_6**
Description	Products should not use default passwords. If the service needs a password, it must be generated randomly or force the admin to introduce one.
Mandatory	YES
Applicability	All products with passwords.

Input from Technology Provider	Configuration should never have default passwords. If there is an automated configuration generator (e.g. yaim) it must request the user to set one or generate a random one.
Pass/Fail Criteria	No default passwords are used for configuration of services.
Related Information	SVG Advisory 1414: https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1414
Revision Log	

Default Configuration	
ID	**GENERIC_SERVICE_7**
Description	Default configuration of the service should be *usable*.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Documentation on the default values of any optional configuration parameters. Default values for those values reasonable for the normal operation of the service in a standard installation.
Pass/Fail Criteria	Pass if the documentation of the default values of the optional configuration parameters is available and the service runs with those default values (in a standard installation).
Related Information	VOMS mass user suspension (RT #3585)
Revision Log	

5 SECURITY

World Writable Files	
ID	**GENERIC_SEC_1**
Description	Products must not create world-writable files or directories.
Mandatory	YES
Applicability	All products.

Input from Technology Provider	World-writable files and directories are dangerous since they allows anyone to modify them, several vulnerabilities in recent years have been due to world writable files and directories being present when they should not be. Technology Provider must assure that they software do not produce world writable files in order to prevent new vulnerabilities being introduced in the future. Ideally a test that checks that those files do not exist should be provided.	
Test Description	**Pre-condition**	Service correctly configured and started
	Test	Check the existence of world writable or unowned files in the system.
	Expected Outcome	No world writable or unowned files exist.
Pass/Fail Criteria	The product should not create world-writable files or directories. If any world-writable files are needed for the normal operation of the service, these should be documented. Logs and config files **must** not be world-writable.	
Related Information	Proposed by the EGI SVG RAT to prevent new vulnerabilities in the future.	
Revision Log	V1.3 Changed test description. V4: improved pass/fail criteria.	

Passwords in world readable files	
ID	**GENERIC_SEC_3**
Description	Service password must not be stored in world readable files.
Mandatory	YES
Applicability	All products with passwords.

Input from Technology Provider	If the product uses passwords stored in files, those files must not be world readable.
Pass/Fail Criteria	No passwords are stored in world readable files.
Related Information	SVG Advisory 1414: https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1414
Revision Log	

6 MISCELLANEOUS

Bug Tracking System	
ID	**GENERIC_MISC_1**
Description	TP must enrol as 3rd level support in the EGI Helpdesk.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Technology Providers must enrol in GGUS as 3rd level support for the products verified by the Quality Assurance team of EGI. Any further integration with TP-specific bug tracking software is entirely up to the Technology Provider.
Pass/Fail Criteria	Pass if Technology Provider enlisted as 3rd level support in GGUS.
Related Information	IGE QC
Revision Log	

7 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.

7.1 Authentication Credentials

X.509 Certificate support	
ID	**AUTHN_CRED_1**
Description	Primary authentication token within the infrastructure is the X.509 certificate and its proxy derivatives.
Mandatory	YES
Applicability	Authentication Appliances.

Input from Technology Provider	Support for X.509 certificate (and proxy derivatives) as credential token for authentication.
Pass/Fail Criteria	Pass if the appliance is able to use X.509 certificates as authentication token. The appliance *should* also support proxy derivatives.
Related Information	UMD Roadmap [R 1]
Revision Log	

SHA-2 Certificate support	
ID	**AUTHN_CRED_2**
Description	SHA-2 certificates should be accepted by middleware.
Mandatory	NO
Applicability	Authentication Appliances.

Input from Technology Provider	Support for certificates and proxies with SHA-2 cryptographic hash functions.
Pass/Fail Criteria	Pass if the appliance is able to use SHA-2 certificates as authentication token. Information on how to get and test with SHA-2 certificates is available at [R 2]
Related Information	UMD Roadmap [R 1] Support for SHA2 proxies RT #3078
Revision Log	

RFC Proxy support	
ID	**AUTHN_CRED_3**
Description	RFC proxies should be accepted by middleware.
Mandatory	NO
Applicability	Authentication Appliances that

Input from Technology Provider	Support for RFC proxies as credential tokens for authentication.
Pass/Fail Criteria	Pass if the appliance is able to use RFC proxies as authentication token. Information on how to create RFC proxies is available at [R 2]
Related Information	UMD Roadmap [R 1]
Revision Log	

7.2 Authentication Protocols

TLS/SSLv3 Support	
ID	**AUTHN_PROTO_1**
Description	TLS/SSLv3/v2 with client-side authentication must be supported.
Mandatory	YES
Applicability	Authentication Appliances.

Input from Technology Provider	Support for accessing resources through protocols that are secured using SSL or TLS (e.g. plain socket, or https connections). If the component exposes a WebService that requires authentication, it should use the X.509 certificates/proxies with the https protocol.
Pass/Fail Criteria	Pass if the product uses SSL or TLS for accessing it. For the current releases of UMD, products still using GSI authentication (with httpg for WebServices) may be accepted, this exception may be dropped 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 V4: changed from AUTH_IFACE_1 to AUTH_PROTO_1.

8 AUTHORISATION

8.1 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	**Pre-condition**	Policy repository available.
	Test	List policies
	Expected Outcome	List of stored policies.
Pass/Fail Criteria	Pass if the test suite passes	
Related Information	UMD Roadmap [R 1] Argus [R 37]	
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	Pass if the administrator is able to configure the use of (remote) policy repositories: disabling, enabling and establishing an order for them.
Related Information	UMD Roadmap [R 1] Argus [R 37]
Revision Log	

8.2 Policy Definition

8.2.1 Central policy management (Argus)

(un) Banning Policies	
ID	**AUTHZ_ PCYDEF_1**
Description	Administrators must be able to define policies that ban users or groups of users.
Mandatory	YES
Applicability	Authorisation Appliances with PAP

Input from Technology Provider	Support for banning different users (defined by a DN) or group of users defined by certain attributes (e.g. role/group attributes, FQANs); also support re-establishing already existing banning.	
Test Description	**Pre-condition**	Policy repository available. Banning policy for user/group not defined
	Test	Define ban policy for user/group
	Expected Outcome	Ban policy for user/group stored in policy repository.
	Pre-condition	Policy repository available. Banning policy for user/group defined
	Test	Unban policy for user/group
	Expected Outcome	Ban policy for user/group 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 37]	
Revision Log	V4: Removed explicit FQAN references.	

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 XACML or a simplified equivalent.	
Mandatory	YES	
Applicability	Authorisation Appliances with PAP	

Input from Technology Provider	Support for policy definitions with different users (usually defined by a DN) or group of users defined by certain attributes (e.g. role/group attributes, FQANs); both *allow* and *deny* 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 users and or groups of users.	
Related Information	UMD Roadmap [R 1] Argus [R 37]	
Revision Log	V4: Removed FQAN references.	

8.3 Policy Enforcement

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 (or any other role/group attributes schema agreed), 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 role/group attributes if available. For gridmap based mapping, new entry in grid map is created.
	Pre-condition	Configured system. Previous mapping for user existing.
	Test	Accepted authorisation.
	Expected Outcome	GID/UID of the previous mapping returned.
Pass/Fail Criteria	Pass if the mapping is performed as defined in the AuthZ appliance (e.g according to a gridmapfile). The use of pool accounts is desirable, although the criteria can pass if not supported. The verifier may accept other mapping mechanisms after discussion within the verification team.	
Related Information	UMD Roadmap [R 1] Argus [R 37]	
Revision Log	V4: removed FQAN references, relaxed pool account support.	

9 INFORMATION MODEL

9.1 Information Model Schema

GlueSchema Support	
ID	**INFOMODEL_SCHEMA_1**
Description	Resource information exchanged in the EGI Infrastructure must conform to GlueSchema.
Mandatory	YES
Applicability	Information Model Appliances

Input from Technology Provider	Resource information published by Information Discovery Appliances must conform to the GlueSchema v1.3.	
Test Description	**Pre-condition**	None.
	Test	Check that information published conforms to GlueSchema 1.3. The suggested tool for testing the conformance is the GlueValidator [R 26]
	Expected Outcome	Information conforms to GlueSchema.
Pass/Fail Criteria	Information published must be available in GlueSchema v1.3 Ideally the Technology Provider should assure this by a test suite of the appliances.	
Related Information	UMD Roadmap [R 1] GlueSchema v1.3 [R 24] GlueValidator [R 26]	
Revision Log	V2: Merged INFOMODEL_SCHEMA_* into this criterion. Rephrasing. V4: Added reference to Glue Validator	

Middleware Version Information	
ID	**INFOMODEL_SCHEMA_2**
Description	The middleware version must be published in the resource information.
Mandatory	NO
Applicability	Information Model Appliances

Input from Technology Provider	Resource information published by Information Discovery Appliances must include the version of the middleware.
Pass/Fail Criteria	Middleware version of service is published correctly by the service.
Related Information	Requirement #1378
Revision Log	

GlueSchema 2.0 Support	
ID	**INFOMODEL_SCHEMA_3**
Description	Resource information exchanged in the EGI Infrastructure must conform to GlueSchema.
Mandatory	NO
Applicability	Information Model Appliances

Input from Technology Provider	Resource information published by Information Discovery Appliances should conform to the GlueSchema v2.0	
Test Description	**Pre-condition**	None.
	Test	Check that information published conforms to GlueSchema 2.0. The suggested tool for testing the conformance is the GlueValidator [R 26]
	Expected Outcome	Information conforms to GlueSchema.
Pass/Fail Criteria	Information published must be available in GlueSchema v2.0 Ideally the Technology Provider should assure this by a test suite of the appliances.	
Related Information	UMD Roadmap [R 1] GlueSchema v2.0 [R 25] GlueValidator [R 26]	
Revision Log		

10 MONITORING PROBES

The Monitoring Capability executes a set of probes defined by the operations community. These probes *should* be provided by the TP for each product.

10.1 Service Probes

Certificate Lifetime Probe	
ID	**MON_PROBE_GENERIC_1**
Description	Provide a monitoring probe that assures that the host certificate lifetime for the service is valid.
Mandatory	NO
Applicability	All products that use host certificates

Input from Technology Provider	Certificate Validity Probe. The probe should only use the public interface of the service and run integrated in the monitoring infrastructure of EGI
Pass/Fail Criteria	The QC will pass if the TP provides with the service a probe for checking the certificate lifetime. This probe may be provided also indirectly as part of other probes.
Related Information	
Revision Log	V1.1 Added probe description. V2: Simplified description

Service Probe	
ID	**MON_PROBE_GENERIC_2**
Description	Provide monitoring probes that test the functionality of the service
Mandatory	NO
Applicability	All Services

Input from Technology Provider	Monitoring probe that tests that the service provides the expected functionality. The probe should only use the public interface of the service and run integrated in the monitoring infrastructure of EGI. The exact tests to perform for each service are determined by the operations community. For the current probes specification check the SAM documentation [R 32]
Pass/Fail Criteria	Probes must exist, they must be integrated with the EMI monitoring infrastructure and provide the expected functionality.
Related Information	SAM documentation [R 32]
Revision Log	

11 REFERENCES

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

R 23	DORII (Deployment of Remote Instrumentation Infrastructure) Project: http://www.dorii.eu/
R 24	GlueSchema Specification v1.3: http://glueschema.forge.cnaf.infn.it/Spec/V13
R 25	GlueSchema Specification v2.0: http://www.ogf.org/documents/GFD.147.pdf
R 26	Glue Validator: https://tomtools.cern.ch/confluence/display/IS/GLUEValidator
R 27	JMS (Java Message Service Specification) 1.1: http://www.oracle.com/technetwork/java/jms/index.html
R 28	AMQP (Advanced Message Queuing Protocol): http://www.amqp.org/confluence/display/AMQP/Advanced+Message+Queuing+Protocol
R 29	OASIS WS-Notification: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn
R 30	Nagios Config Generator: https://tomtools.cern.ch/confluence/display/SAM/NCG
R 31	My EGI portal: https://tomtools.cern.ch/confluence/display/SAM/MyEGI
R 32	SAM Probes Documentation: https://tomtools.cern.ch/confluence/display/SAM/Probes
R 33	Accounting Portal: http://accounting.egi.eu/
R 34	GridSite Delegation Protocol: http://www.gridsite.org/wiki/Delegation_protocol
R 35	Globus Delegation Service: http://www.globus.org/toolkit/docs/4.0/security/delegation/
R 36	European Policy Management Authority for Grid Authentication (EuGridPMA): http://www.eugridpma.org/
R 37	ARGUS Authorization Service: https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework
R 38	XACML: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
R 39	Hydra encrypted file storage: https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS
R 40	gLite FTS: https://twiki.cern.ch/twiki/bin/view/EGEE/GLiteFTS
R 41	SRM v2.2: http://www.ggf.org/documents/GFD.129.pdf
R 42	S2 Test: http://s-2.sourceforge.net/
R 43	SRM-Tester: https://sdm.lbl.gov/twiki/bin/view/Software/SRMTester/WebHome
R 44	Lcg-utils: http://grid-deployment.web.cern.ch/grid-deployment/documentation/LFC_DPM/lcg_util/
R 45	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 46	Open Cloud Computing Interface WG, OGF, http://www.ggf.org/gf/group_info/view.php?group=occi-wg
R 47	Virtualization Management (VMAN), DMTF http://www.dmtf.org/standards/vman
R 48	StratusLab http://stratuslab.eu/
R 49	StratusLab MarketPlace Technical Note TN-Marketplace (V3.0)