



# EGI-InSPIRE

## UMD QUALITY CRITERIA v5

---

Document identifier:	EGI-QC-V5-SE.doc
Date:	<b>18/04/2013</b>
Document Link:	<a href="https://documents.egi.eu/document/1153">https://documents.egi.eu/document/1153</a>

---

### Abstract

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



### 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
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

<b>1</b>	<b>Documentation.....</b>	<b>5</b>
	GENERIC_DOC_1.....	5
	GENERIC_DOC_2.....	6
	GENERIC_DOC_3.....	7
	GENERIC_DOC_4.....	8
	GENERIC_DOC_5.....	9
	GENERIC_DOC_6.....	10
	GENERIC_DOC_7.....	11
	GENERIC_DOC_8.....	12
	GENERIC_DOC_9.....	13
<b>2</b>	<b>Software Distribution .....</b>	<b>15</b>
	GENERIC_DIST_1.....	15
	GENERIC_DIST_3.....	16
<b>3</b>	<b>Software Features .....</b>	<b>17</b>
	GENERIC_SOFT_1.....	17
	GENERIC_SOFT_2.....	18
<b>4</b>	<b>Service Criteria .....</b>	<b>19</b>
<b>4.1</b>	<b>Service Management.....</b>	<b>19</b>
	GENERIC_SERVICE_1.....	19
<b>4.2</b>	<b>Service logs.....</b>	<b>21</b>
	GENERIC_SERVICE_2.....	21
<b>4.3</b>	<b>Service Monitoring .....</b>	<b>21</b>
<b>4.4</b>	<b>Service Accounting .....</b>	<b>21</b>
<b>4.5</b>	<b>Availability, Reliability and Scalability.....</b>	<b>22</b>
	GENERIC_SERVICE_3.....	22
	GENERIC_SERVICE_4.....	23
	GENERIC_SERVICE_6.....	24
	GENERIC_SERVICE_7.....	25
<b>5</b>	<b>Security.....</b>	<b>26</b>
	GENERIC_SEC_1.....	26
	GENERIC_SEC_2.....	27
	GENERIC_SEC_3.....	28
<b>6</b>	<b>Miscellaneous .....</b>	<b>29</b>
	GENERIC_MISC_1.....	29
<b>7</b>	<b>Authentication.....</b>	<b>30</b>
<b>7.1</b>	<b>Authentication Credentials.....</b>	<b>30</b>
	AUTHN_CRED_1.....	30
	AUTHN_CRED_2.....	31
	AUTHN_CRED_3.....	32
<b>7.2</b>	<b>Authentication Protocols.....</b>	<b>33</b>
	AUTHN_PROTO_1.....	33
<b>7.3</b>	<b>Delegation Interface.....</b>	<b>34</b>
	AUTHN_DELEG_1.....	34
<b>8</b>	<b>Authorisation.....</b>	<b>36</b>
<b>8.1</b>	<b>Policy Definition.....</b>	<b>36</b>
	8.1.1 Service Based Authorisation (Not Using Argus).....	36



AUTHZ_PCYDEF_3 .....	36
AUTHZ_PCYDEF_4 .....	37
<b>8.2 Policy Enforcement .....</b>	<b>38</b>
AUTHZ_PEP_2 .....	38
AUTHZ_PEP_3 .....	39
<b>9 Information Model.....</b>	<b>40</b>
<b>9.1 Information Model Schema.....</b>	<b>40</b>
INFOMODEL_SCHEMA_1.....	40
INFOMODEL_SCHEMA_2.....	41
INFOMODEL_SCHEMA_3.....	42
<b>10 File Access.....</b>	<b>43</b>
<b>10.1 File Access Interface .....</b>	<b>43</b>
FILEACC_API_1.....	43
FILEACC_API_2.....	44
<b>11 File Transfer.....</b>	<b>45</b>
<b>11.1 File Transfer Interfaces.....</b>	<b>45</b>
FILETRANS_API_1.....	45
FILETRANS_API_2.....	46
FILETRANS_API_3.....	47
<b>12 Storage Management .....</b>	<b>48</b>
<b>12.1 SRM Interface .....</b>	<b>48</b>
STORAGE_API_1.....	48
STORAGE_API_2.....	49
<b>12.2 Storage Device Support .....</b>	<b>50</b>
STORAGE_DEVICE_1.....	50
STORAGE_DEVICE_2.....	51
STORAGE_DEVICE_3.....	52
STORAGE_DEVICE_4.....	53
<b>13 Monitoring Probes.....</b>	<b>54</b>
<b>13.1 Service Probes .....</b>	<b>54</b>
MON_PROBE_GENERIC_1 .....	54
MON_PROBE_GENERIC_2 .....	55
13.1.1 File Access Capability Probes.....	56
MON_PROBE_STORAGE_1 .....	56
<b>14 Client Tools.....</b>	<b>58</b>
<b>14.1 Generic client tools criteria.....</b>	<b>58</b>
CLIENT_TOOLS_1 .....	58
CLIENT_TOOLS_2 .....	59
<b>15 References .....</b>	<b>60</b>

## 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.

<b>Functional Description</b>	
<b>ID</b>	<b>GENERIC_DOC_1</b>
<b>Description</b>	All products must provide a document with a brief functional description of the product.
<b>Mandatory</b>	NO
<b>Applicability</b>	All products
<b>Input from Technology Provider</b>	Document (or link) with a general description of the product that includes: <ul style="list-style-type: none"><li>• Purpose of the product</li><li>• Capabilities meet by the product</li></ul>
<b>Pass/Fail Criteria</b>	The document should exist and contain the requested information.
<b>Related Information</b>	
<b>Revision Log</b>	V2: clarified the required documentation



<b>Release Notes</b>	
<b>ID</b>	<b>GENERIC_DOC_2</b>
<b>Description</b>	All products must provide a document with the release notes.
<b>Mandatory</b>	YES
<b>Applicability</b>	All products
<b>Input from Technology Provider</b>	Document (or link) with release notes of the product. They must include major the changes in the product: bug fixes, new features.
<b>Pass/Fail Criteria</b>	The document should exist and contain the requested information.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>User Documentation</b>	
<b>ID</b>	<b>GENERIC_DOC_3</b>
<b>Description</b>	All products must provide a document describing how to use it.
<b>Mandatory</b>	NO
<b>Applicability</b>	All products with end-user tools and services.
<b>Input from Technology Provider</b>	Document (or link) with user guide describing the functionality of the software and how to use it.
<b>Pass/Fail Criteria</b>	The document should exist and contain the requested information.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>Online help (man pages)</b>	
<b>ID</b>	<b>GENERIC_DOC_4</b>
<b>Description</b>	All products with end user command line tools must include man pages or online help.
<b>Mandatory</b>	NO
<b>Applicability</b>	All products with command line tools.
<b>Input from Technology Provider</b>	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)
<b>Pass/Fail Criteria</b>	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 <b>must</b> be mutually consistent (describe the same set of options and their meaning).
<b>Related Information</b>	GGUS ticket # 73214
<b>Revision Log</b>	V3: Tighten wording to avoid situations as described in GGUS #73214



<b>API Documentation</b>	
<b>ID</b>	<b>GENERIC_DOC_5</b>
<b>Description</b>	Public API of product/appliances must be documented.
<b>Mandatory</b>	NO
<b>Applicability</b>	All products with public API.
<b>Input from Technology Provider</b>	Documentation (or link) of the API of the product. The documentation <i>should</i> cover all the existing public functionality of the API.
<b>Pass/Fail Criteria</b>	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.
<b>Related Information</b>	
<b>Revision Log</b>	V2: review of the description

<b>Administrator Documentation</b>	
<b>ID</b>	<b>GENERIC_DOC_6</b>
<b>Description</b>	Products must provide an administrator guide describing installation, configuration and operation of the system.
<b>Mandatory</b>	NO
<b>Applicability</b>	All products managed by an administrator.
<b>Input from Technology Provider</b>	Documentation (or link) with requested documentation.
<b>Pass/Fail Criteria</b>	The document should exist and contain the requested information.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>Service Reference Card</b>																			
<b>ID</b>	<b>GENERIC_DOC_7</b>																		
<b>Description</b>	For each of the services that a product runs, document its characteristics with a reference card.																		
<b>Mandatory</b>	NO																		
<b>Applicability</b>	All products that need services for operation.																		
<b>Input from Technology Provider</b>	Documentation (or link) with requested documentation.																		
<b>Pass/Fail Criteria</b>	<p>The document must exist and contain the following information for each service:</p> <table border="1"> <thead> <tr> <th colspan="2"><b>ServiceName</b></th> </tr> </thead> <tbody> <tr> <td>Description</td> <td>Description of the service</td> </tr> <tr> <td>Init scripts</td> <td>List of init scripts for the service, expected run levels</td> </tr> <tr> <td>Daemons</td> <td>List of daemons needed for the service</td> </tr> <tr> <td>Configuration</td> <td>List of configuration files used by the service</td> </tr> <tr> <td>Logs</td> <td>List of log files used by the service</td> </tr> <tr> <td>Open ports</td> <td>List of ports the service uses</td> </tr> <tr> <td>Cron</td> <td>List of crons used by the service</td> </tr> <tr> <td>Other information</td> <td>Any other relevant information about the service.</td> </tr> </tbody> </table>	<b>ServiceName</b>		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.
<b>ServiceName</b>																			
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.																		
<b>Related Information</b>																			
<b>Revision Log</b>																			

<b>Software License</b>	
<b>ID</b>	<b>GENERIC_DOC_8</b>
<b>Description</b>	Products must have a compatible license for using them in the EGI Infrastructure
<b>Mandatory</b>	YES
<b>Applicability</b>	All products.
<b>Input from Technology Provider</b>	Product License (link or document).
<b>Pass/Fail Criteria</b>	<p>Pass: if the license is available and is compatible with the EGI infrastructure.</p> <p>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”:</p> <ul style="list-style-type: none"> <li>- Apache License, 2.0 (Apache-2.0)</li> <li>- BSD 3-Clause "New" or "Revised" license (BSD-3-Clause)</li> <li>- BSD 3-Clause "Simplified" or "FreeBSD" license (BSD-2-Clause)</li> <li>- GNU General Public License (GPL)</li> <li>- GNU Library or "Lesser" General Public License (LGPL)</li> <li>- MIT license (MIT)</li> <li>- Mozilla Public License 1.1 (MPL-1.1)</li> <li>- Common Development and Distribution License (CDDL-1.0)</li> <li>- Eclipse Public License (EPL-1.0)</li> </ul> <p>Other licenses accepted by the Open Source Initiative and listed as “Special Purpose” are compatible with the infrastructure (when applicable):</p> <ul style="list-style-type: none"> <li>- Educational Community License</li> <li>- IPA Font License (IPA)</li> <li>- NASA Open Source Agreement 1.3 (NASA-1.3)</li> <li>- Open Font License 1.1 (OFL-1.1)</li> </ul> <p>Any other license, and non Open Source products will be evaluated by the verification team in coordination with the Operations Community.</p>
<b>Related Information</b>	Open Source Initiative Licenses by Category: <a href="http://www.opensource.org/licenses/category">http://www.opensource.org/licenses/category</a>
<b>Revision Log</b>	V2: Moved from Software Release to documentation.

<b>Release changes testing</b>	
<b>ID</b>	<b>GENERIC_DOC_9</b>
<b>Description</b>	Changes in a release of a product must be tested.
<b>Mandatory</b>	NO
<b>Applicability</b>	All Products.
<b>Input from Technology Provider</b>	Tests (or documentation for the test results) for relevant changes described in the product release notes, including bug fixes and any new features.
<b>Pass/Fail Criteria</b>	<p>Pass if the TP provides documentation of the tests performed to certify the release quality. The documentation <i>should</i> describe tests (and tests results) for all the changes included, especially bug fixes.</p> <p>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.</p>
<b>Related Information</b>	MS503: Software Provisioning Process
<b>Revision Log</b>	<p>V2: Better specification of the pass/fail criteria. Moved to documentation criteria</p> <p>V3: improvement of the pass/fail criteria.</p> <p>V4: better wording after IGE review, turned into NOT mandatory.</p>



## 2 SOFTWARE DISTRIBUTION

Source Code Availability	
<b>ID</b>	<b>GENERIC_DIST_1</b>
<b>Description</b>	Open Source Products should provide their source code.
<b>Mandatory</b>	NO
<b>Applicability</b>	All Open Source Products.
<b>Input from Technology Provider</b>	Source code repository or source distribution of product with building documentation.
<b>Pass/Fail Criteria</b>	Open source products <b>must</b> 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.
<b>Related Information</b>	
<b>Revision Log</b>	V2: Changed ID (previously GENERIC_REL_2) V4: Merged GENERIC_DIST_1 and GENERIC_DIST_2 & Turned into not mandatory

<b>Binary Distribution</b>	
<b>ID</b>	<b>GENERIC_DIST_3</b>
<b>Description</b>	Products must be available in the native packaging format of the supported platform.
<b>Mandatory</b>	YES
<b>Applicability</b>	All Products.
<b>Input from Technology Provider</b>	Binary distribution of product in the native packaging format of the supported platform (RPM, DEB, ...)
<b>Pass/Fail Criteria</b>	<ul style="list-style-type: none"> <li>- 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.</li> <li>- Packages <b>must</b> be signed by the TP</li> <li>- Packages <i>should</i> follow OS packaging policies (e.g. names of packages, <u>use of filesystem hierarchy</u>, init scripts). Any deviance from the policies must be documented.</li> <li>- Second level dependencies (i.e. software not provided by the TP in their repository) <b>must</b> be provided by the OS distribution or standard OS repositories (EPEL in SL5 &amp; 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.</li> </ul>
<b>Related Information</b>	Verification reports from EMI release 1. #1357: Middleware use standard file locations GGUS #82417: <a href="https://ggus.eu/ws/ticket_info.php?ticket=82417">https://ggus.eu/ws/ticket_info.php?ticket=82417</a>
<b>Revision Log</b>	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	
<b>ID</b>	<b>GENERIC_SOFT_1</b>
<b>Description</b>	Minor/Revision releases of a product must be backwards compatible.
<b>Mandatory</b>	YES
<b>Applicability</b>	All Products.
<b>Input from Technology Provider</b>	Products must maintain backwards compatibility between releases of the same major version. Ideally, TP provides tests to assure the backwards compatibility of the product.
<b>Pass/Fail Criteria</b>	All the changes in a minor or revision release <i>must</i> 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.
<b>Related Information</b>	MS503: Software Provisioning Process IGE QC
<b>Revision Log</b>	

<b>New features testing</b>	
<b>ID</b>	<b>GENERIC_SOFT_2</b>
<b>Description</b>	Verification should cover testing of new features and bug fixes.
<b>Mandatory</b>	YES
<b>Applicability</b>	All Products.
<b>Input from Technology Provider</b>	Release notes with changes in the software. The verifier will review each of the changes and check its correctness (whenever possible)
<b>Pass/Fail Criteria</b>	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.
<b>Related Information</b>	MS503: Software Provisioning Process IGE QC
<b>Revision Log</b>	

## 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	
<b>ID</b>	<b>GENERIC_SERVICE_1</b>
<b>Description</b>	Services run by the product must provide a mechanism for starting, stopping and querying the status of the services.
<b>Mandatory</b>	YES
<b>Applicability</b>	All products that use services for operations.

<b>Input from Technology Provider</b>	Start/stop mechanism for each of the services following OS conventions. Ideally, provide a test suite for the mechanism as described below.						
<b>Test Description</b>	<table border="0"> <tr> <td><b>Pre-condition</b></td> <td>Service is started</td> </tr> <tr> <td><b>Test</b></td> <td>Start service</td> </tr> <tr> <td><b>Expected Outcome</b></td> <td>No action taken, show a message stating the service is already started.</td> </tr> </table>	<b>Pre-condition</b>	Service is started	<b>Test</b>	Start service	<b>Expected Outcome</b>	No action taken, show a message stating the service is already started.
	<b>Pre-condition</b>	Service is started					
	<b>Test</b>	Start service					
	<b>Expected Outcome</b>	No action taken, show a message stating the service is already started.					
	<table border="0"> <tr> <td><b>Pre-condition</b></td> <td>Service is stopped</td> </tr> <tr> <td><b>Test</b></td> <td>Start service</td> </tr> <tr> <td><b>Expected Outcome</b></td> <td>Service is started, show a message when it is started.</td> </tr> </table>	<b>Pre-condition</b>	Service is stopped	<b>Test</b>	Start service	<b>Expected Outcome</b>	Service is started, show a message when it is started.
	<b>Pre-condition</b>	Service is stopped					
	<b>Test</b>	Start service					
	<b>Expected Outcome</b>	Service is started, show a message when it is started.					
	<table border="0"> <tr> <td><b>Pre-condition</b></td> <td>Service is started</td> </tr> <tr> <td><b>Test</b></td> <td>Stop service</td> </tr> <tr> <td><b>Expected Outcome</b></td> <td>Service is stopped, show a message stating the service is stopped.</td> </tr> </table>	<b>Pre-condition</b>	Service is started	<b>Test</b>	Stop service	<b>Expected Outcome</b>	Service is stopped, show a message stating the service is stopped.
	<b>Pre-condition</b>	Service is started					
	<b>Test</b>	Stop service					
	<b>Expected Outcome</b>	Service is stopped, show a message stating the service is stopped.					
<table border="0"> <tr> <td><b>Pre-condition</b></td> <td>Service is stopped</td> </tr> <tr> <td><b>Test</b></td> <td>Stop service</td> </tr> <tr> <td><b>Expected Outcome</b></td> <td>No action taken, show a message stating the service is already stopped.</td> </tr> </table>	<b>Pre-condition</b>	Service is stopped	<b>Test</b>	Stop service	<b>Expected Outcome</b>	No action taken, show a message stating the service is already stopped.	
<b>Pre-condition</b>	Service is stopped						
<b>Test</b>	Stop service						
<b>Expected Outcome</b>	No action taken, show a message stating the service is already stopped.						
<table border="0"> <tr> <td><b>Pre-condition</b></td> <td>Service is stopped</td> </tr> <tr> <td><b>Test</b></td> <td>Check service status</td> </tr> <tr> <td><b>Expected Outcome</b></td> <td>Show a message stating the service is stopped.</td> </tr> </table>	<b>Pre-condition</b>	Service is stopped	<b>Test</b>	Check service status	<b>Expected Outcome</b>	Show a message stating the service is stopped.	
<b>Pre-condition</b>	Service is stopped						
<b>Test</b>	Check service status						
<b>Expected Outcome</b>	Show a message stating the service is stopped.						

<b>Test Description</b>	<b>Pre-condition</b> Service is started <b>Test</b> Check service status <b>Expected Outcome</b> Show a message stating the service is started.
<b>Pass/Fail Criteria</b>	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 <a href="http://refspecs.freestandards.org/LSB_3.1.0/LSB-Core-generic/LSB-Core-generic/inisrptact.html">http://refspecs.freestandards.org/LSB_3.1.0/LSB-Core-generic/LSB-Core-generic/inisrptact.html</a> ). They must work properly in <b>all</b> the cases described above. If the OS provides tools for configuring the services (chkconfig in RH based distros), these <i>should</i> work out of the box with the init scripts of the services
<b>Related Information</b>	#2274: Service under RH following SystemV init system #1201: Homogeneity in service control.
<b>Revision Log</b>	V3: Added related information, fix test conditions.

## 4.2 Service logs

Log Files	
<b>ID</b>	<b>GENERIC_SERVICE_2</b>
<b>Description</b>	All services should create log files where the service administrator can trace most relevant actions taken.
<b>Mandatory</b>	YES
<b>Applicability</b>	All products that use services for operations.
<b>Input from Technology Provider</b>	List of logs generated by the service (the reference card of service should already include them)
<b>Pass/Fail Criteria</b>	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, ...)
<b>Related Information</b>	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
<b>Revision Log</b>	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.

<b>Service Reliability</b>	
<b>ID</b>	<b>GENERIC_SERVICE_3</b>
<b>Description</b>	Services must maintain a good performance and reliability over long periods of time with normal operation.
<b>Mandatory</b>	NO
<b>Applicability</b>	All products that use services for operations.
<b>Input from Technology Provider</b>	Long running unattended operation test measuring performance of the product.
<b>Test Description</b>	<p><b>Pre-condition</b> Product is properly configured.</p> <p><b>Test</b> Start service and measure performance during operations.</p> <p><b>Expected Outcome</b> No significant performance degradation is observed in the system.</p>
<b>Pass/Fail Criteria</b>	<p>Service must not show performance degradation during a 3-day period. The most important parameters to check are:</p> <ul style="list-style-type: none"> <li>• stable memory usage</li> <li>• 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)</li> </ul>
<b>Related Information</b>	
<b>Revision Log</b>	V2: detailed pass/fail criteria

<b>Service Robustness</b>	
<b>ID</b>	<b>GENERIC_SERVICE_4</b>
<b>Description</b>	Services should not produce unexpected results or become uncontrollable when taxed beyond normal capacity.
<b>Mandatory</b>	NO
<b>Applicability</b>	All products that use services for operations.
<b>Input from Technology Provider</b>	Assure that the services taxed beyond normal capacity do not produce unexpected results or become uncontrollable.
<b>Pass/Fail Criteria</b>	Services taxed beyond normal capacity: <ul style="list-style-type: none"> <li>• should not become unresponsive to normal start/stop operations</li> <li>• must be able to start after a forceful stop</li> <li>• must not expose (potentially sensitive) memory contents to other processes</li> <li>• must not leave sensitive data in world-readable files</li> <li>• must not accept connections that would be refused under normal operating conditions</li> </ul>
<b>Related Information</b>	TST_2 from IGE Quality Assurance.
<b>Revision Log</b>	

<b>Default Password Configuration</b>	
<b>ID</b>	<b>GENERIC_SERVICE_6</b>
<b>Description</b>	Products should not use default passwords. If the service needs a password, it must be generated randomly or force the admin to introduce one.
<b>Mandatory</b>	YES
<b>Applicability</b>	All products with passwords.
<b>Input from Technology Provider</b>	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.
<b>Pass/Fail Criteria</b>	No default passwords are used for configuration of services.
<b>Related Information</b>	SVG Advisory 1414: <a href="https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1414">https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1414</a>
<b>Revision Log</b>	



<b>Default Configuration</b>	
<b>ID</b>	<b>GENERIC_SERVICE_7</b>
<b>Description</b>	Default configuration of the service should be <i>usable</i> .
<b>Mandatory</b>	YES
<b>Applicability</b>	All Products.
<b>Input from Technology Provider</b>	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.
<b>Pass/Fail Criteria</b>	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).
<b>Related Information</b>	VOMS mass user suspension (RT #3585)
<b>Revision Log</b>	

## 5 SECURITY

World Writable Files	
<b>ID</b>	<b>GENERIC_SEC_1</b>
<b>Description</b>	Products must not create world-writable files or directories.
<b>Mandatory</b>	YES
<b>Applicability</b>	All products.
<b>Input from Technology Provider</b>	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.
<b>Test Description</b>	<p><b>Pre-condition</b> Service correctly configured and started</p> <p><b>Test</b> Check the existence of world writable or unowned files in the system.</p> <p><b>Expected Outcome</b> No world writable or unowned files exist.</p>
<b>Pass/Fail Criteria</b>	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 <b>must</b> not be world-writable.
<b>Related Information</b>	Proposed by the EGI SVG RAT to prevent new vulnerabilities in the future.
<b>Revision Log</b>	V1.3 Changed test description. V4: improved pass/fail criteria.

<b>Directory Traversal Attacks testing</b>	
<b>ID</b>	<b>GENERIC_SEC_2</b>
<b>Description</b>	Products should assure that directory traversal exploits are not possible using their interfaces. Special care must be taken to products exposing part of the file system (e.g. file access capabilities) and web services.
<b>Mandatory</b>	YES
<b>Applicability</b>	All products with previous known Directory Traversal exploits (See list at related information), any other product <i>should</i> also include this kind of testing.
<b>Input from Technology Provider</b>	A directory traversal (or path traversal) consists in exploiting insufficient security validation/sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs. The Technology Provider should test that directory traversal attacks are not possible using the product interface. Products that need to run as root user, must have special care in this case of attacks, since they may give access to whole file system.
<b>Test Description</b>	<p><b>Pre-condition</b> Service correctly configured and started</p> <p><b>Test</b> Try to exploit directory traversal in product</p> <p><b>Expected Outcome</b> No directory traversal succeeds.</p>
<b>Pass/Fail Criteria</b>	Test for directory traversal exploiting do not successfully access the file system.
<b>Related Information</b>	Advisory-SVG-2011-1569 ( <a href="https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1569">https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1569</a> )
<b>Revision Log</b>	

<b>Passwords in world readable files</b>	
<b>ID</b>	<b>GENERIC_SEC_3</b>
<b>Description</b>	Service password must not be stored in world readable files.
<b>Mandatory</b>	YES
<b>Applicability</b>	All products with passwords.
<b>Input from Technology Provider</b>	If the product uses passwords stored in files, those files must not be world readable.
<b>Pass/Fail Criteria</b>	No passwords are stored in world readable files.
<b>Related Information</b>	SVG Advisory 1414: <a href="https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1414">https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1414</a>
<b>Revision Log</b>	

## 6 MISCELLANEOUS

<b>Bug Tracking System</b>	
<b>ID</b>	<b>GENERIC_MISC_1</b>
<b>Description</b>	TP must enrol as 3 <sup>rd</sup> level support in the EGI Helpdesk.
<b>Mandatory</b>	YES
<b>Applicability</b>	All Products.
<b>Input from Technology Provider</b>	Technology Providers must enrol in GGUS as 3 <sup>rd</sup> 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.
<b>Pass/Fail Criteria</b>	Pass if Technology Provider enlisted as 3 <sup>rd</sup> level support in GGUS.
<b>Related Information</b>	IGE QC
<b>Revision Log</b>	

## 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

<b>X.509 Certificate support</b>	
<b>ID</b>	<b>AUTHN_CRED_1</b>
<b>Description</b>	Primary authentication token within the infrastructure is the X.509 certificate and its proxy derivatives.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authentication Appliances.
<b>Input from Technology Provider</b>	Support for X.509 certificate (and proxy derivatives) as credential token for authentication.
<b>Pass/Fail Criteria</b>	Pass if the appliance is able to use X.509 certificates as authentication token. The appliance <i>should</i> also support proxy derivatives.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>SHA-2 Certificate support</b>	
<b>ID</b>	<b>AUTHN_CRED_2</b>
<b>Description</b>	SHA-2 certificates should be accepted by middleware.
<b>Mandatory</b>	NO
<b>Applicability</b>	Authentication Appliances.
<b>Input from Technology Provider</b>	Support for certificates and proxies with SHA-2 cryptographic hash functions.
<b>Pass/Fail Criteria</b>	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]
<b>Related Information</b>	UMD Roadmap [R 1] Support for SHA2 proxies RT #3078
<b>Revision Log</b>	

<b>RFC Proxy support</b>	
<b>ID</b>	<b>AUTHN_CRED_3</b>
<b>Description</b>	RFC proxies should be accepted by middleware.
<b>Mandatory</b>	NO
<b>Applicability</b>	Authentication Appliances that
<b>Input from Technology Provider</b>	Support for RFC proxies as credential tokens for authentication.
<b>Pass/Fail Criteria</b>	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]
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	



## 7.2 Authentication Protocols

TLS/SSLv3 Support	
<b>ID</b>	<b>AUTHN_PROTO_1</b>
<b>Description</b>	TLS/SSLv3/v2 with client-side authentication must be supported.
<b>Mandatory</b>	YES
<b>Applicability</b>	Authentication Appliances.
<b>Input from Technology Provider</b>	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.
<b>Pass/Fail Criteria</b>	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, <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 V4: changed from AUTH_IFACE_1 to AUTH_PROTO_1.

### 7.3 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>	Delegation implementation that includes all functionality of the GridSite or Globus 4 interfaces. Correct handling for erroneous input.
<b>Pass/Fail Criteria</b>	Pass if the delegation interface is tested and works as expected. Appliances must support at least <b>one</b> of the following interfaces: GridSite delegation or Globus 4 delegation.
<b>Related Information</b>	UMD Roadmap [R 1] GridSite Delegation [R 34] Globus Delegation [R 35]
<b>Revision Log</b>	V2: Merged AUTHN_DELEG_1 & 2.



## 8 AUTHORISATION

### 8.1 Policy Definition

#### 8.1.1 Service Based Authorisation (Not Using Argus)

<b>Ban User/Group of users</b>	
<b>ID</b>	<b>AUTHZ_PCYDEF_3</b>
<b>Description</b>	Administrators must be able to define policies that ban users (black list).
<b>Mandatory</b>	NO
<b>Applicability</b>	Authorisation Appliances without PAP (Argus)
<b>Input from Technology Provider</b>	Support for banning of single user (defined by a DNs) or by a set of users (defined by role/group attributes or FQANs).
<b>Test Description</b>	<b>Pre-condition</b> Configured system.
	<b>Test</b> Ban policy for user/group. Test access for user/group.
	<b>Expected Outcome</b> Ban policy is correctly enforced.
	<b>Pre-condition</b> Configured system. Banning policy for user/group defined
	<b>Test</b> Unban user/group. Test access for user/group.
	<b>Expected Outcome</b> User/group is allowed.
<b>Pass/Fail Criteria</b>	Pass if the banning policies can be defined and enforced at least for users, ideally support role/groups attributes for defining policies.
<b>Related Information</b>	
<b>Revision Log</b>	V4: better wording, not mandatory since for some service only white list policies can be defined.

<b>Allowed users definition</b>	
<b>ID</b>	<b>AUTHZ_PCYDEF_4</b>
<b>Description</b>	Administrators must be determine which users/groups are allowed in the system
<b>Mandatory</b>	YES
<b>Applicability</b>	Authorisation Appliances without PAP
<b>Input from Technology Provider</b>	Support for allowing users/groups of users in the system. Support for defining allowed users (determined by DNs) or groups (defined by a set of role/group attributes or FQANs).
<b>Test Description</b>	<p><b>Pre-condition</b> Configured system.</p> <p><b>Test</b> Allow user/group access into system. Test access for user/group.</p> <p><b>Expected Outcome</b> User/group is allowed in the system.</p>
<b>Pass/Fail Criteria</b>	Pass if the banning policies can be defined and enforced at least for individual users, ideally support role/groups attributes for defining policies.
<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) V4: reviewed wording

## 8.2 Policy Enforcement

User Mapping	
<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>	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.
<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 role/group attributes if available. For gridmap based mapping, 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 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.
<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 37]
<b>Revision Log</b>	V4: removed FQAN references, relaxed pool account support.

<b>Integration with authorisation appliances (ARGUS)</b>	
<b>ID</b>	<b>AUTHZ_PEP_3</b>
<b>Description</b>	Services should be able to use external authorisation appliance (ARGUS)
<b>Mandatory</b>	NO
<b>Applicability</b>	Services requiring authorisation
<b>Input from Technology Provider</b>	Support for using an authorization appliance that applies the authorization policies and returns a mapping to a local account. The preferred authorization appliance is ARGUS.
<b>Pass/Fail Criteria</b>	Pass if the service is able to get authorization and authentication from correctly configured authorization appliance (ARGUS)
<b>Related Information</b>	UMD Roadmap [R 1] Argus [R 37]
<b>Revision Log</b>	

## 9 INFORMATION MODEL

### 9.1 Information Model Schema

GlueSchema Support	
<b>ID</b>	<b>INFOMODEL_SCHEMA_1</b>
<b>Description</b>	Resource information exchanged in the EGI Infrastructure must conform to GlueSchema.
<b>Mandatory</b>	YES
<b>Applicability</b>	Information Model Appliances
<b>Input from Technology Provider</b>	Resource information published by Information Discovery Appliances must conform to the GlueSchema v1.3.
<b>Test Description</b>	<p><b>Pre-condition</b> None.</p> <p><b>Test</b> Check that information published conforms to GlueSchema 1.3. The suggested tool for testing the conformance is the GlueValidator [R 26]</p> <p><b>Expected Outcome</b> Information conforms to GlueSchema.</p>
<b>Pass/Fail Criteria</b>	Information published must be available in GlueSchema v1.3 Ideally the Technology Provider should assure this by a test suite of the appliances.
<b>Related Information</b>	UMD Roadmap [R 1] GlueSchema v1.3 [R 24] GlueValidator [R 26]
<b>Revision Log</b>	V2: Merged INFOMODEL_SCHEMA_* into this criterion. Rephrasing. V4: Added reference to Glue Validator



<b>Middleware Version Information</b>	
<b>ID</b>	<b>INFOMODEL_SCHEMA_2</b>
<b>Description</b>	The middleware version must be published in the resource information.
<b>Mandatory</b>	NO
<b>Applicability</b>	Information Model Appliances
<b>Input from Technology Provider</b>	Resource information published by Information Discovery Appliances must include the version of the middleware.
<b>Pass/Fail Criteria</b>	Middleware version of service is published correctly by the service.
<b>Related Information</b>	Requirement #1378
<b>Revision Log</b>	

<b>GlueSchema 2.0 Support</b>	
<b>ID</b>	<b>INFOMODEL_SCHEMA_3</b>
<b>Description</b>	Resource information exchanged in the EGI Infrastructure must conform to GlueSchema.
<b>Mandatory</b>	NO
<b>Applicability</b>	Information Model Appliances
<b>Input from Technology Provider</b>	Resource information published by Information Discovery Appliances should conform to the GlueSchema v2.0
<b>Test Description</b>	<p><b>Pre-condition</b> None.</p> <p><b>Test</b> Check that information published conforms to GlueSchema 2.0. The suggested tool for testing the conformance is the GlueValidator [R 26]</p> <p><b>Expected Outcome</b> Information conforms to GlueSchema.</p>
<b>Pass/Fail Criteria</b>	Information published must be available in GlueSchema v2.0 Ideally the Technology Provider should assure this by a test suite of the appliances.
<b>Related Information</b>	UMD Roadmap [R 1] GlueSchema v2.0 [R 25] GlueValidator [R 26]
<b>Revision Log</b>	

## 10 FILE ACCESS

Provides an abstraction that allows a file to be stored on or retrieved from a storage device (e.g. tape, disk, distributed file system, etc.) for use elsewhere in the infrastructure.

### 10.1 File Access Interface

POSIX Read file access	
<b>ID</b>	<b>FILEACC_API_1</b>
<b>Description</b>	Provide genuine POSIX read file access.
<b>Mandatory</b>	NO
<b>Applicability</b>	File Access Interface.
<b>Input from Technology Provider</b>	Support for the POSIX read file access: opening and reading files.
<b>Test Description</b>	<p><b>Pre-condition</b> POSIX access configured and available for user.</p> <p><b>Test</b> POSIX read file operations tests.</p> <p><b>Expected Outcome</b> POSIX file operations work as documented. Log of operations</p>
<b>Pass/Fail Criteria</b>	Pass if POSIX access to files is provided.
<b>Related Information</b>	UMD Roadmap [R 1] #1386: EMI Data clients should be able to offer the file:// protocol to SRM
<b>Revision Log</b>	V2: changed to READ only access, and not mandatory.

<b>POSIX Write file access</b>	
<b>ID</b>	<b>FILEACC_API_2</b>
<b>Description</b>	Provide genuine POSIX write file access.
<b>Mandatory</b>	NO
<b>Applicability</b>	File Access Interface.
<b>Input from Technology Provider</b>	Support for the POSIX file access: open (creating files), and write/append operations on files.
<b>Test Description</b>	<p><b>Pre-condition</b> POSIX access configured and available for user.</p> <p><b>Test</b> POSIX file write operations tests.</p> <p><b>Expected Outcome</b> POSIX file operations work as documented. Log of operations</p>
<b>Pass/Fail Criteria</b>	Pass if POSIX write access to files is provided.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

## 11 FILE TRANSFER

### 11.1 File Transfer Interfaces

GridFTP File Access	
<b>ID</b>	FILETRANS_API_1
<b>Description</b>	Provide gridFTP access for reading data.
<b>Mandatory</b>	YES
<b>Applicability</b>	GridFTP File Transfer Appliances.
<b>Input from Technology Provider</b>	Support for reading and writing data from the Storage Resource using gridFTP.
<b>Test Description</b>	<p><b>Pre-condition</b> Valid credentials.</p> <p><b>Test</b> Transfer files via gridFTP protocol (both read and write operations)</p> <p><b>Expected Outcome</b> Files can be transferred. Log of operations</p>
<b>Pass/Fail Criteria</b>	Pass if gridFTP access to files is provided.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>HTTPS File Access</b>	
<b>ID</b>	<b>FILETRANS_API_2</b>
<b>Description</b>	Provide HTTP(S) access for reading data.
<b>Mandatory</b>	YES
<b>Applicability</b>	HTTPS File Transfer Appliances.
<b>Input from Technology Provider</b>	Support for reading data from the Storage Resource using http(s)
<b>Test Description</b>	<p><b>Pre-condition</b> Valid credentials.</p> <p><b>Test</b> Transfer files via HTTP(s) protocol.</p> <p><b>Expected Outcome</b> Files can be transferred. Log of operations</p>
<b>Pass/Fail Criteria</b>	Pass if HTTP(s) read access to files is provided.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

<b>WebDAV File Access</b>	
<b>ID</b>	<b>FILETRANS_API_3</b>
<b>Description</b>	Provide WebDAV access for data.
<b>Mandatory</b>	YES
<b>Applicability</b>	WebDAV File Transfer Appliances.
<b>Input from Technology Provider</b>	Support for reading and writing data from the Storage Resource using WebDAV.
<b>Test Description</b>	<p><b>Pre-condition</b> Valid credentials.</p> <p><b>Test</b> Transfer files via WebDAV protocol (both read and write operations)</p> <p><b>Expected Outcome</b> Files can be transferred. Log of operations</p>
<b>Pass/Fail Criteria</b>	Pass if WebDAV read access to files is provided.
<b>Related Information</b>	UMD Roadmap [R 1]
<b>Revision Log</b>	

## 12 STORAGE MANAGEMENT

### 12.1 SRM Interface

SRM API Support	
<b>ID</b>	<b>STORAGE_API_1</b>
<b>Description</b>	Storage Management Appliances must provide support for SRM2.2 specification.
<b>Mandatory</b>	YES
<b>Applicability</b>	Storage Management Appliances
<b>Input from Technology Provider</b>	Valid SRM v2.2 API implementation, any deviations from the API implementation should be documented. Ideally, also provide a complete test suite and results for the API support
<b>Test Description</b>	<p><b>Pre-condition</b> Valid user credentials.</p> <p><b>Test</b> Test SRMv2.2 functionality, with correct/incorrect input and with valid and invalid credentials. Use S2 [R 42] test suite for reference.</p> <p><b>Expected Outcome</b> Log of all the operations performed. All the documented functions work as documented.</p>
<b>Pass/Fail Criteria</b>	Pass if SRM v2.2 support is provided (as tested with S2 test suite). If the API is not completely supported, this should be documented.
<b>Related Information</b>	UMD Roadmap [R 1] SRM v2.2 [R 41]
<b>Revision Log</b>	V3: Improved wording



<b>LCG-UTILS test</b>	
<b>ID</b>	<b>STORAGE_API_2</b>
<b>Description</b>	Test Storage Management Appliances with the lcg-utils commands.
<b>Mandatory</b>	YES
<b>Applicability</b>	Storage Management Appliances
<b>Input from Technology Provider</b>	Support for lcg-utils [R 44] commands, documentation of any possible incompatibilities with other Appliances.
<b>Test Description</b>	<p><b>Pre-condition</b> Valid user credentials.</p> <p><b>Test</b> Test lcg-utils commands, with correct/incorrect input and with valid and invalid credentials. An example test suite is available at [R 45]</p> <p><b>Expected Outcome</b> Log of all the operations performed. All the documented functions work as documented.</p>
<b>Pass/Fail Criteria</b>	Pass if lcg-utils commands can be executed correctly against the Storage Management Appliance. In the case of incompatibilities or collateral effects they must be documented.
<b>Related Information</b>	Although all Storage Management Appliances should use SRM [R 41] protocol, deficiencies in the protocol description had lead to different implementations and results. This tests intends to harmonize results at least when using lcg-utils, and until a complete and better description of SRM protocol and desired results is reached.
<b>Revision Log</b>	V3: Added reference

## 12.2 Storage Device Support

The Storage Management Capability provide an abstraction to a Storage Device, these QC refer to the interaction of the Storage Management Capability implementation with the underlying storage device. Storage Management Capabilities are expected to support the most common file systems and storage devices used in the current EGI infrastructure.

<b>Information retrieval</b>	
<b>ID</b>	<b>STORAGE_DEVICE_1</b>
<b>Description</b>	The Storage Management Capability must be able to provide information from the underlying storage and make it available to an Information Discovery Appliance.
<b>Mandatory</b>	YES
<b>Applicability</b>	Storage Management Appliances
<b>Input from Technology Provider</b>	Information retrieval mechanisms that generate the Storage Element related entities of the current UMD Information Model Capability (GlueSchema 1.3/GlueSchema 2) using the actual information of the underlying available storage.
<b>Test Description</b>	<p><b>Pre-condition</b> Configured system.</p> <p><b>Test</b> Retrieve current status from storage.</p> <p><b>Expected Outcome</b> All the mandatory Storage Element related entities of GlueSchema using the <b>actual</b> information are generated.</p>
<b>Pass/Fail Criteria</b>	Pass if the information retrieval mechanisms are able to generate the requested information.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>Fine grained authorization</b>	
<b>ID</b>	<b>STORAGE_DEVICE_2</b>
<b>Description</b>	The Storage Management Capability must allow the implementation of a fine-grained authorization policy based on VO roles and enforce it (if defined).
<b>Mandatory</b>	NO
<b>Applicability</b>	Storage Management Appliances
<b>Input from Technology Provider</b>	Support for fine-grained authorization policy based on VO roles. Such authorization policy can be configured and applied to the full directory tree of the storage area or just to a fraction of the storage area directory tree.
<b>Test Description</b>	<p><b>Pre-condition</b> Configured system with a storage resource area directory tree with different authorization permissions along the directory tree for different VO roles.</p> <p><b>Test</b> Test I/O storage operations (write, copy, delete files) using SRM interface and LCG-UTILS in a storage space area directory using different VO roles in the FQAN.</p> <p><b>Expected Outcome</b> Log of the operation is performed. A user with a valid credential and invoking an authorized VO role should be able to write/delete or read/copy files from a given storage area, according to the defined policies.</p>
<b>Pass/Fail Criteria</b>	Pass if a user can interact with the storage area tree in compliance with the defined fine-grained authorization policy based on the user VO roles.
<b>Related Information</b>	
<b>Revision Log</b>	

Space reservations	
<b>ID</b>	<b>STORAGE_DEVICE_3</b>
<b>Description</b>	The Storage Management Capability must allow the implementation of (virtual or real) reserved space areas as storage space tokens
<b>Mandatory</b>	NO
<b>Applicability</b>	Storage Management Appliances
<b>Input from Technology Provider</b>	Support for (virtual or real) storage space reservations enabled as storage space tokens. Interactions with the storage areas represented by a given space token must be enforced to respect the defined fine-grained authorization policy. The storage resource information system must reflect the existence of storage space tokens (if configured).
<b>Test Description</b>	<p><b>Pre-condition</b> Configured system with (virtual or real) storage space reservations enabled as storage space tokens.</p> <p><b>Test</b> Retrieve current status from the storage space token area.</p> <p><b>Expected Outcome</b> All the mandatory Storage Element related entities of GlueSchema using the <b>actual</b> information for the storage space token area are generated.</p>
	<p><b>Pre-condition</b> Configured system with (virtual or real) storage space reservations enabled as storage space tokens.</p> <p><b>Test</b> Test I/O storage operations (write files, copy files, delete files) using SRM interface and LCG-UTILS in a storage space reservation area using a valid and invalid credential.</p> <p><b>Expected Outcome</b> Log of the operation is performed. A user with a valid credential should be able to copy and retrieve files from the storage space token area.</p>
<b>Pass/Fail Criteria</b>	Pass if a user can interact with the storage space token area in compliance with the fine-grained authorization policies (STORAGE_DEVICE_2); if the storage space token area information is updated in the storage information system; and if all operations are properly logged.
<b>Related Information</b>	
<b>Revision Log</b>	

<b>Checksum</b>	
<b>ID</b>	<b>STORAGE_DEVICE_4</b>
<b>Description</b>	The Storage Management Capability must support Adler32 checksum calculation and store the checksum value for a given file.
<b>Mandatory</b>	NO
<b>Applicability</b>	Storage Management Appliances
<b>Input from Technology Provider</b>	Support for storing/retrieving/listing a file in a storage resource through the SRM interface or LCG-UTILS enabling the checksum computation.
<b>Test Description</b>	<p><b>Pre-condition</b> Configured system with checksum computation option enabled.</p> <p><b>Test</b> Test storing/retrieving/listing a file in a storage resource through the SRM interface or LCG-UTILS enabling the checksum computation.</p> <p><b>Expected Outcome</b> Files checksum values are computed while storing a file. The checksum values are computed and compared at source and destiny to detect file corruptions. The checksum value for a file is accessible via SRM interface or LCG-UTILS listing functions.</p>
<b>Pass/Fail Criteria</b>	Pass if a user is able to store/retrieve/list a file in a storage resource through SRM interface or LCG-UTILS, and that the checksum value for the file was corrected computed and delivered.
<b>Related Information</b>	
<b>Revision Log</b>	

## 13 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.

### 13.1 Service Probes

Certificate Lifetime Probe	
<b>ID</b>	<b>MON_PROBE_GENERIC_1</b>
<b>Description</b>	Provide a monitoring probe that assures that the host certificate lifetime for the service is valid.
<b>Mandatory</b>	NO
<b>Applicability</b>	All products that use host certificates
<b>Input from Technology Provider</b>	Certificate Validity Probe. The probe should only use the public interface of the service and run integrated in the monitoring infrastructure of EGI
<b>Pass/Fail Criteria</b>	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.
<b>Related Information</b>	
<b>Revision Log</b>	V1.1 Added probe description. V2: Simplified description

<b>Service Probe</b>	
<b>ID</b>	<b>MON_PROBE_GENERIC_2</b>
<b>Description</b>	Provide monitoring probes that test the functionality of the service
<b>Mandatory</b>	NO
<b>Applicability</b>	All Services
<b>Input from Technology Provider</b>	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]
<b>Pass/Fail Criteria</b>	Probes must exist, they must be integrated with the EMI monitoring infrastructure and provide the expected functionality.
<b>Related Information</b>	SAM documentation [R 32]
<b>Revision Log</b>	

The criteria described in the next sections make reference to probes that are used by the EGI Operations community to monitor the Infrastructure. The specific appliances must support the execution of these probes.

### 13.1.1 File Access Capability Probes

SRM Probes	
<b>ID</b>	MON_PROBE_STORAGE_1
<b>Description</b>	Provide monitoring probes that test the functionality of SRM.
<b>Mandatory</b>	YES
<b>Applicability</b>	Storage Management Appliances
<b>Input from Technology Provider</b>	SRM probes as described at: <a href="https://tomtools.cern.ch/confluence/display/SAM/SRM">https://tomtools.cern.ch/confluence/display/SAM/SRM</a> .
<b>Pass/Fail Criteria</b>	Probes must exist and behave as expected in the probe documentation.
<b>Related Information</b>	SAM documentation [R 32]
<b>Revision Log</b>	





## 14 CLIENT TOOLS

### 14.1 Generic client tools criteria

<b>Command line options coherency</b>	
<b>ID</b>	<b>CLIENT_TOOLS_1</b>
<b>Description</b>	Client commands for the same product should have a coherent set of options.
<b>Mandatory</b>	NO
<b>Applicability</b>	Client Tools
<b>Input from Technology Provider</b>	Client command tools for a given product with coherent options between them (e.g. configuration file is always specified with <code>-c</code> option, vo with <code>-vo</code> option) Ideally, coherency with other product command line clients.
<b>Pass/Fail Criteria</b>	All the command tools for a given product must have a coherent command line options. Semantically common options for two commands must have the same syntax.
<b>Related Information</b>	Requirement #1780
<b>Revision Log</b>	

<b>Error Messages</b>	
<b>ID</b>	<b>CLIENT_TOOLS_2</b>
<b>Description</b>	Error messages provided by the service should be clear and facilitate the solution of those errors by users or service administrators
<b>Mandatory</b>	NO
<b>Applicability</b>	Client tools.
<b>Input from Technology Provider</b>	Any error in the client tools must produce a clear error message. A possible solution/cause for it should be given.
<b>Pass/Fail Criteria</b>	<p>Pass if the errors provided by the client tools always produce a descriptive message. Errors without any message (unless a quiet option is specified) will make the criterion to fail.</p> <p>Ideally the following info is also documented/shown for all errors:</p> <ul style="list-style-type: none"> <li>• Error code</li> <li>• Error source (internal module or remote resource (specify it explicitly))</li> <li>• Cause of error (syntax error, module malfunctioning, configuration problem, network error, other (specify it explicit))</li> <li>• Type (critical, informative)</li> <li>• Possible solution</li> </ul>
<b>Related Information</b>	Requirements gathered in MS305 related to resubmission of jobs, and information provided in error messages.
<b>Revision Log</b>	

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

<b>R 23</b>	DORII (Deployment of Remote Instrumentation Infrastructure) Project: <a href="http://www.dorii.eu/">http://www.dorii.eu/</a>
<b>R 24</b>	GlueSchema Specification v1.3: <a href="http://glueschema.forge.cnaf.infn.it/Spec/V13">http://glueschema.forge.cnaf.infn.it/Spec/V13</a>
<b>R 25</b>	GlueSchema Specification v2.0: <a href="http://www.ogf.org/documents/GFD.147.pdf">http://www.ogf.org/documents/GFD.147.pdf</a>
<b>R 26</b>	Glue Validator: <a href="https://tomtools.cern.ch/confluence/display/IS/GLUEValidator">https://tomtools.cern.ch/confluence/display/IS/GLUEValidator</a>
<b>R 27</b>	JMS (Java Message Service Specification) 1.1: <a href="http://www.oracle.com/technetwork/java/jms/index.html">http://www.oracle.com/technetwork/java/jms/index.html</a>
<b>R 28</b>	AMQP (Advanced Message Queuing Protocol): <a href="http://www.amqp.org/confluence/display/AMQP/Advanced+Message+Queuing+Protocol">http://www.amqp.org/confluence/display/AMQP/Advanced+Message+Queuing+Protocol</a>
<b>R 29</b>	OASIS WS-Notification: <a href="https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn">https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn</a>
<b>R 30</b>	Nagios Config Generator: <a href="https://tomtools.cern.ch/confluence/display/SAM/NCG">https://tomtools.cern.ch/confluence/display/SAM/NCG</a>
<b>R 31</b>	My EGI portal: <a href="https://tomtools.cern.ch/confluence/display/SAM/MyEGI">https://tomtools.cern.ch/confluence/display/SAM/MyEGI</a>
<b>R 32</b>	SAM Probes Documentation: <a href="https://tomtools.cern.ch/confluence/display/SAM/Probes">https://tomtools.cern.ch/confluence/display/SAM/Probes</a>
<b>R 33</b>	Accounting Portal: <a href="http://accounting.egi.eu/">http://accounting.egi.eu/</a>
<b>R 34</b>	GridSite Delegation Protocol: <a href="http://www.gridsite.org/wiki/Delegation_protocol">http://www.gridsite.org/wiki/Delegation_protocol</a>
<b>R 35</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 36</b>	European Policy Management Authority for Grid Authentication (EuGridPMA): <a href="http://www.eugridpma.org/">http://www.eugridpma.org/</a>
<b>R 37</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 38</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>
<b>R 39</b>	Hydra encrypted file storage: <a href="https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS">https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS</a>
<b>R 40</b>	gLite FTS: <a href="https://twiki.cern.ch/twiki/bin/view/EGEE/GLiteFTS">https://twiki.cern.ch/twiki/bin/view/EGEE/GLiteFTS</a>
<b>R 41</b>	SRM v2.2: <a href="http://www.ggf.org/documents/GFD.129.pdf">http://www.ggf.org/documents/GFD.129.pdf</a>
<b>R 42</b>	S2 Test: <a href="http://s-2.sourceforge.net/">http://s-2.sourceforge.net/</a>
<b>R 43</b>	SRM-Tester: <a href="https://sdm.lbl.gov/twiki/bin/view/Software/SRMTester/WebHome">https://sdm.lbl.gov/twiki/bin/view/Software/SRMTester/WebHome</a>
<b>R 44</b>	Lcg-utils: <a href="http://grid-deployment.web.cern.ch/grid-deployment/documentation/LFC_DPM/lcg_util/">http://grid-deployment.web.cern.ch/grid-deployment/documentation/LFC_DPM/lcg_util/</a>
<b>R 45</b>	Lcg-utils test suite: <a href="http://glite.cvs.cern.ch/cgi-">http://glite.cvs.cern.ch/cgi-</a>

	<a href="http://bin/glite.cgi/org.glite.testsuites.ctb/UI/tests/test-lcg-utils.sh?view=markup">bin/glite.cgi/org.glite.testsuites.ctb/UI/tests/test-lcg-utils.sh?view=markup</a>
<b>R 46</b>	Open Cloud Computing Interface WG, OGF, <a href="http://www.ggf.org/gf/group_info/view.php?group=occi-wg">http://www.ggf.org/gf/group_info/view.php?group=occi-wg</a>
<b>R 47</b>	Virtualization Management (VMAN), DMTF <a href="http://www.dmtf.org/standards/vman">http://www.dmtf.org/standards/vman</a>
<b>R 48</b>	StratusLab <a href="http://stratuslab.eu/">http://stratuslab.eu/</a>
<b>R 49</b>	StratusLab MarketPlace Technical Note TN-Marketplace (V3.0)