



EGI-InSPIRE

UMD QUALITY CRITERIA v5

Document identifier:	EGI-QC-V5-VOMS.doc
Date:	19/04/2013
Document Link:	https://documents.egi.eu/document/1153

Abstract

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



Copyright notice

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

Document Log

Issue	Date	Comment	Author/Partner
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.....	5
	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
	GENERIC_DOC_10.....	14
	GENERIC_DOC_11.....	15
2	Software Distribution	16
	GENERIC_DIST_1.....	16
	GENERIC_DIST_3.....	17
3	Software Features	18
	GENERIC_SOFT_1.....	18
	GENERIC_SOFT_2.....	19
4	Service Criteria	20
4.1	Service Management.....	20
	GENERIC_SERVICE_1.....	20
4.2	Service logs.....	22
	GENERIC_SERVICE_2.....	22
4.3	Service Monitoring	22
4.4	Service Accounting	22
4.5	Availability, Reliability and Scalability.....	23
	GENERIC_SERVICE_3.....	23
	GENERIC_SERVICE_4.....	24
4.6	Service Configuration	25
	GENERIC_SERVICE_6.....	25
	GENERIC_SERVICE_7.....	26
5	Security.....	27
	GENERIC_SEC_1.....	27
	GENERIC_SEC_3.....	28
6	Miscellaneous.....	29
	GENERIC_MISC_1.....	29
7	Authentication.....	30
7.1	Authentication Credentials.....	30
	AUTHN_CRED_1.....	30
	AUTHN_CRED_2.....	31
	AUTHN_CRED_3.....	32
7.2	Authentication Protocols.....	33
	AUTHN_PROTO_1.....	33
8	Attribute Authority.....	34
8.1	Attribute Authority Interface.....	34
	ATTAUTH_IFACE_1.....	34



ATTAUTH_IFACE_2	35
ATTAUTH_IFACE_3	36
ATTAUTH_IFACE_4	37
8.2 VO management.....	38
ATTAUTH_MGMT_1	38
ATTAUTH_MGMT_2	39
ATTAUTH_MGMT_3	40
ATTAUTH_MGMT_4	42
ATTAUTH_MGMT_5	43
ATTAUTH_MGMT_6	44
8.3 VO Management Web Interface (VOMS-Admin)	45
ATTAUTH_WEB_1	45
ATTAUTH_WEB_2	46
ATTAUTH_WEB_3	47
ATTAUTH_WEB_4	48
ATTAUTH_WEB_5	49
9 Information Model.....	50
9.1 Information Model Schema.....	50
INFOMODEL_SCHEMA_1	50
INFOMODEL_SCHEMA_2	51
INFOMODEL_SCHEMA_3	52
10 Monitoring Probes	53
10.1 Service Probes	53
MON_PROBE_GENERIC_1	53
MON_PROBE_GENERIC_2	54
11 Client Tools.....	55
11.1 Generic client tools criteria.....	55
CLIENT_TOOLS_1	55
CLIENT_TOOLS_2	56
12 References	57

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: <ul style="list-style-type: none">• 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 <i>should</i> 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	<p>The document must exist and contain the following information for each service:</p> <table border="1"> <thead> <tr> <th colspan="2">ServiceName</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>	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.
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	<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"> - 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) <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"> - Educational Community License - IPA Font License (IPA) - NASA Open Source Agreement 1.3 (NASA-1.3) - Open Font License 1.1 (OFL-1.1) <p>Any other license, and non Open Source products will be evaluated by the verification team in coordination with the Operations Community.</p>
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	<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>
Related Information	MS503: Software Provisioning Process
Revision Log	<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>

Database Schema Documentation	
ID	GENERIC_DOC_10
Description	Database schemas changes must be documented.
Mandatory	YES
Applicability	All Products that make use of a database backends.
Input from Technology Provider	Documentation (or link) with description of the database schema used by the product. If there are schema changes between releases (minor or major upgradeable from previous major), also include documentation of those changes and scripts for migration to the new schema.
Pass/Fail Criteria	Pass if any database schema changes are documented and a migration path is provided via a script or with detailed instructions. The database schema documentation should be also available.
Related Information	VOMS mass user suspension (RT #3585)
Revision Log	

Policy changes	
ID	GENERIC_DOC_11
Description	Documentation of changes that may affect underlying policies.
Mandatory	YES
Applicability	All Products that implement EGI policies
Input from Technology Provider	Documentation (or link) of any changes introduced in the product that may affect any underlying policies (e.g. procedure for VOMS membership renewal) implemented by the service.
Pass/Fail Criteria	If a new release of a product introduces changes in its configuration options, management interfaces or any other feature that affects the implementation of underlying policies, those changes and their effects must be documented.
Related Information	VOMS mass user suspension (RT #3585)
Revision Log	

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	<ul style="list-style-type: none"> - 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 <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. - 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 <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.
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	<table border="0"> <tr> <td>Pre-condition</td> <td>Service is started</td> </tr> <tr> <td>Test</td> <td>Start service</td> </tr> <tr> <td>Expected Outcome</td> <td>No action taken, show a message stating the service is already started.</td> </tr> </table>	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 started					
	Test	Start service					
	Expected Outcome	No action taken, show a message stating the service is already started.					
	<table border="0"> <tr> <td>Pre-condition</td> <td>Service is stopped</td> </tr> <tr> <td>Test</td> <td>Start service</td> </tr> <tr> <td>Expected Outcome</td> <td>Service is started, show a message when it is started.</td> </tr> </table>	Pre-condition	Service is stopped	Test	Start service	Expected Outcome	Service is started, show a message when it is started.
	Pre-condition	Service is stopped					
	Test	Start service					
	Expected Outcome	Service is started, show a message when it is started.					
	<table border="0"> <tr> <td>Pre-condition</td> <td>Service is started</td> </tr> <tr> <td>Test</td> <td>Stop service</td> </tr> <tr> <td>Expected Outcome</td> <td>Service is stopped, show a message stating the service is stopped.</td> </tr> </table>	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 started					
	Test	Stop service					
	Expected Outcome	Service is stopped, show a message stating the service is stopped.					
<table border="0"> <tr> <td>Pre-condition</td> <td>Service is stopped</td> </tr> <tr> <td>Test</td> <td>Stop service</td> </tr> <tr> <td>Expected Outcome</td> <td>No action taken, show a message stating the service is already stopped.</td> </tr> </table>	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	Stop service						
Expected Outcome	No action taken, show a message stating the service is already stopped.						
<table border="0"> <tr> <td>Pre-condition</td> <td>Service is stopped</td> </tr> <tr> <td>Test</td> <td>Check service status</td> </tr> <tr> <td>Expected Outcome</td> <td>Show a message stating the service is stopped.</td> </tr> </table>	Pre-condition	Service is stopped	Test	Check service status	Expected Outcome	Show a message stating the service is stopped.	
Pre-condition	Service is stopped						
Test	Check service status						
Expected Outcome	Show a message stating the service is stopped.						

Test Description	<p>Pre-condition Service is started</p> <p>Test Check service status</p> <p>Expected Outcome Show a message stating the service is started.</p>
Pass/Fail Criteria	<p>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.</p> <p>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</p>
Related Information	<p>#2274: Service under RH following SystemV init system</p> <p>#1201: Homogeneity in service control.</p>
Revision Log	<p>V3: Added related information, fix test conditions.</p>

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	<p>Pre-condition Product is properly configured.</p> <p>Test Start service and measure performance during operations.</p> <p>Expected Outcome No significant performance degradation is observed in the system.</p>
Pass/Fail Criteria	<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"> • 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: <ul style="list-style-type: none"> • 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

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 <i>usable</i> .
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	<p>Pre-condition Service correctly configured and started</p> <p>Test Check the existence of world writable or unowned files in the system.</p> <p>Expected Outcome No world writable or unowned files exist.</p>
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 3 rd level support in the EGI Helpdesk.
Mandatory	YES
Applicability	All Products.
Input from Technology Provider	Technology Providers must enrol in GGUS as 3 rd 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 3 rd 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 <i>should</i> 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, <u>this exception may be dropped</u> in future releases of the criterion.
Related Information	UMD Roadmap [R 1]
Revision Log	V2: Added GSI (httpg) exception for products that have not yet transitioned V4: changed from AUTH_IFACE_1 to AUTH_PROTO_1.

8 ATTRIBUTE AUTHORITY

8.1 Attribute Authority Interface

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

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

Proxy Destroy							
ID	ATTAUTH_IFACE_3						
Description	Users must be able to destroy a previously created proxy.						
Mandatory	YES						
Applicability	Attribute Authority Appliances						
Input from Technology Provider	Support for proxy destroy.						
Test Description	<table border="0"> <tr> <td>Pre-condition</td> <td>Valid user proxy</td> </tr> <tr> <td>Test</td> <td>Destroy user proxy.</td> </tr> <tr> <td>Expected Outcome</td> <td>Proxy is destroyed.</td> </tr> </table>	Pre-condition	Valid user proxy	Test	Destroy user proxy.	Expected Outcome	Proxy is destroyed.
Pre-condition	Valid user proxy						
Test	Destroy user proxy.						
Expected Outcome	Proxy is destroyed.						
Pass/Fail Criteria	Proxy is destroyed, no operations requiring a proxy can be done with it.						
Related Information	UMD Roadmap [R 1]						
Revision Log							

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

8.2 VO management

VO Creation	
ID	ATTAUTH_MGMT_1
Description	The service administrator must be able to create new VOs in the service.
Mandatory	YES
Applicability	Attribute Authority Appliances
Input from Technology Provider	Support for the creation of VOs, correct handling of incorrect input.
Test Description	Pre-condition Administrator privileges in VO service. Configured service. Test Create a new VO Expected Outcome New database is created and initialized.
	Pre-condition Administrator privileges in VO service. Configured service. Existent VO name Test Create a VO with already existent name. Expected Outcome No action performed, warning message issued.
Pass/Fail Criteria	Pass if the administrator is able to create VOs for all the supported underlying databases.
Related Information	UMD Roadmap [R 1]
Revision Log	

VO Administrators	
ID	ATTAUTH_MGMT_2
Description	The service administrator must be able to define who has VO administrator privileges.
Mandatory	YES
Applicability	Attribute Authority Appliances
Input from Technology Provider	Support for adding VO administrators, managing incorrect input.
Test Description	Pre-condition Administrator privileges in VO service. Configured service. User certificate of new admin. Test Define VO administrator with user certificate. Expected Outcome User is added as VO administrator.
	Pre-condition Administrator privileges in VO service. Configured service. User certificate of already existent admin. Test Define VO administrator with user certificate. Expected Outcome No action performed, warning message is issued.
	Pre-condition Administrator privileges in VO service. Configured service. User certificate of new admin. Test Define VO administrator with user certificate for a nonexistent VO. Expected Outcome Error message stating that the VO is not existent.
Pass/Fail Criteria	Pass if the administrator is able to assign administrator privileges to other users.
Related Information	UMD Roadmap [R 1]
Revision Log	

VO Role/Group/Attribute Management	
ID	ATTAUTH_MGMT_3
Description	Authorized users must be able to define roles, groups and attributes and manage the users with those assigned.
Mandatory	YES
Applicability	Attribute Authority Appliances

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

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

VO User Management	
ID	ATTAUTH_MGMT_4
Description	Authorized users must be able to add and remove users to the VO
Mandatory	YES
Applicability	Attribute Authority Appliances
Input from Technology Provider	Support for adding/removing users to the VO.
Test Description	Pre-condition Authorized user to manage VO users. User to add to VO. Test Add user to VO Expected Outcome User is correctly added to the VO.
	Pre-condition Non-Authorized user to manage VO users. User to add to VO. Test Add user to VO Expected Outcome No action performed, issue error message.
	Pre-condition Authorized user to manage VO users. User to add to VO that already belongs to the VO. Test Add user to VO Expected Outcome No action performed, issue a warning message.
Pass/Fail Criteria	Pass if authorized users are able to add/remove other users for a given VO.
Related Information	UMD Roadmap [R 1]
Revision Log	

ACL Management	
ID	ATTAUTH_MGMT_5
Description	Authorized users must be able to change the different ACLs of the VO.
Mandatory	YES
Applicability	Attribute Authority Appliances
Input from Technology Provider	Support for changing ACLs of users of the VO.
Test Description	Pre-condition Authorized user to manage ACLs. Test Change ACL for a given user. Expected Outcome ACL is correctly changed.
	Pre-condition Non-Authorized user to manage ACLs. Test Change ACL for a given user. Expected Outcome No action performed, error message issued.
Pass/Fail Criteria	Pass if authorized users are able to manage the ACLs for other users for a given VO. The following list of ACLs is expected to be managed: <ul style="list-style-type: none"> • browse users of VO • management of groups • management of roles • management of attributes • management of ACL • add/remove users
Related Information	UMD Roadmap [R 1]
Revision Log	

User suspension notification	
ID	ATTAUTH_MGMT_6
Description	Users must get a notification about the suspension of their membership prior to the suspension
Mandatory	YES
Applicability	Attribute Authority Appliances
Input from Technology Provider	<p>The Attribute Authority appliance must send notifications to the users that are going to be suspended according to the EGI policies. This notification should be sent as an email warning about the membership expiration date and how to resign the VO AUP or any extra steps needed to successfully renew their membership.</p> <p>The notification must be sent in a configurable period before the expiration date (default value should be > 24h, e.g. 2 weeks)</p>
Pass/Fail Criteria	Pass if <ul style="list-style-type: none">•
Related Information	GGUS ticket #77913 RT ticket #3278
Revision Log	

8.3 VO Management Web Interface (VOMS-Admin)

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

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

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

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

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

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	<p>Pre-condition None.</p> <p>Test Check that information published conforms to GlueSchema 1.3. The suggested tool for testing the conformance is the GlueValidator [R 26]</p> <p>Expected Outcome Information conforms to GlueSchema.</p>
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	<p>Pre-condition None.</p> <p>Test Check that information published conforms to GlueSchema 2.0. The suggested tool for testing the conformance is the GlueValidator [R 26]</p> <p>Expected Outcome Information conforms to GlueSchema.</p>
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 CLIENT TOOLS

11.1 Generic client tools criteria

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

Error Messages	
ID	CLIENT_TOOLS_2
Description	Error messages provided by the service should be clear and facilitate the solution of those errors by users or service administrators
Mandatory	NO
Applicability	Client tools.
Input from Technology Provider	Any error in the client tools must produce a clear error message. A possible solution/cause for it should be given.
Pass/Fail Criteria	<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"> • Error code • Error source (internal module or remote resource (specify it explicitly)) • Cause of error (syntax error, module malfunctioning, configuration problem, network error, other (specify it explicit)) • Type (critical, informative) • Possible solution
Related Information	Requirements gathered in MS305 related to resubmission of jobs, and information provided in error messages.
Revision Log	

12 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_wsdaire.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)