



EGI-InSPIRE

UMD STORAGE CAPABILITIES QUALITY CRITERIA v3 DRAFT 1

Document identifier:	EGI-STORAGE-QC-V3-DRAFT1.docx
Date:	18/10/2011
Document Link:	https://documents.egi.eu/document/718

Abstract

This document describes the Quality Criteria for the Storage Capabilities identified in the UMD Roadmap.



Copyright notice

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

Document Log

Issue	Date	Comment	Author/Partner
1.0	19/01/2011	Reorganisation of criteria according to UMD Roadmap v2	Enol Fernández
1.1	04/02/2011	Added Storage Management	Álvaro Fernández
1.2	09/02/2011	Review of Criteria	Enol Fernández
2 DRAFT 1	10/05/2011	Update to new template and review of criteria	Enol Fernández / Mario David / Álvaro Fernández
2	03/08/2011	Review of storage criteria	E. Fernández / G. Borges
3 DRAFT 1	13/10/2011	First draft of release 3	Enol Fernández



TABLE OF CONTENTS

1	File Encryption/Decryption	4
1.1	Key Management	4
	FILECRYPT_KEY_1	4
	FILECRYPT_KEY_2	6
	FILECRYPT_KEY_3	7
1.2	File Encryption/Decryption	8
	FILECRYPT_FILE_1	8
	FILECRYPT_FILE_2	9
2	File Access	10
2.1	File Access Interface	10
	FILEACC_API_1	10
	FILEACC_API_2	11
3	File Transfer	12
3.1	File Transfer Interfaces	12
	FILETRANS_API_1	12
	FILETRANS_API_2	13
	FILETRANS_API_3	14
4	File Transfer Scheduling	15
4.1	File Transfer Channel Management	15
	FILETRANSFSCH_CHANNEL_1	15
	FILETRANSFSCH_CHANNEL_2	16
4.2	File Transfer Management	17
	FILETRANSFSCH_MGMT_1	17
	FILETRANSFSCH_MGMT_2	18
5	Storage Management	19
5.1	SRM Interface	19
	STORAGE_API_1	19
	STORAGE_API_2	20
5.2	Storage Device Support	21
	STORAGE_DEVICE_1	21
	STORAGE_DEVICE_2	22
	STORAGE_DEVICE_3	23
	STORAGE_DEVICE_4	24
5.3	Service availability, monitoring and error handling	25
	STORAGE_SERVICE_1	25
6	References	26

1 FILE ENCRYPTION/DECRYPTION

Criteria for the File Encryption/Decryption Capability are based on gLite Hydra [R 2] as reference implementation. A key handling interface will be described in future versions of the roadmap following input from the EGI Community.

1.1 Key Management

Key Registration	
ID	FILECRYPT_KEY_1
Description	Hydra appliances must allow registering and unregistering keys.
Mandatory	YES
Applicability	Hydra File Encryption/Decryption Appliances.
Input from Technology Provider	Support for key registration/unregistration.
Test Description	Pre-condition Keystore running accepted user credentials. Test Register key in server Expected Outcome Key is successfully registered
	Pre-condition Keystore running accepted user credentials. Test Register key in server specifying cipher and key length. Expected Outcome Key is successfully registered
	Pre-condition Keystore running previously registered key, accepted user credentials. Test Register key in server Expected Outcome Warning issued, no action taken.
	Pre-condition Keystore running previously registered key, accepted user credentials. Test Unregister key in server Expected Outcome Key is successfully unregistered
	Pre-condition Keystore running, non-registered key, accepted user credentials. Test Unregister key in server Expected Outcome Warning message issued, no action taken.
Pass/Fail Criteria	Pass if the registration and unregistration of keys in the appliance work as expected.



Related Information	Hydra [R 2]
Revision Log	V3: Improved wording.

Key and Password Splitting and Recombination	
ID	FILECRYPT_KEY_2
Description	Hydra appliances must provide functionality for generating, splitting and recombine keys and passwords.
Mandatory	YES
Applicability	Hydra File Encryption/Decryption Appliances.
Input from Technology Provider	Support for split and joining password and keys.
Test Description	Pre-condition Password/Key to split Test Split password/key. Expected Outcome Password is successfully splitted
	Pre-condition Whole set of Password/key splits Test Join splits Expected Outcome Password/key successfully joined.
	Pre-condition Minimum number of Password/key splits needed for joining. Test Join splits Expected Outcome Password/key successfully joined.
Pass/Fail Criteria	Pass if the split/join of password and keys functionality is provided. The tests should include different combination of number of parts and minimum number of parts needed for recombinations.
Related Information	Hydra [R 2]
Revision Log	V3: Improved wording.

Key ACL management	
ID	FILECRYPT_KEY_3
Description	Hydra appliances must allow the management of ACLs for a file/key.
Mandatory	YES
Applicability	Hydra File Encryption/Decryption Appliances.
Input from Technology Provider	Support for ACL management of keys and keys set.
Test Description	Pre-condition Key registered in server, user allowed to list ACLs of key Test List key ACLs Expected Outcome ACLs of file correctly shown.
	Pre-condition Key registered in server, user allowed to modify ACLs of key Test Set new ACL for key. Expected Outcome ACL changed correctly.
	Pre-condition Key registered in server, ACL of key set. Test Try allowed actions for ACL. Expected Outcome Actions are performed correctly
	Pre-condition Key registered in server, ACL of key set. Test Try non-allowed actions for ACL. Expected Outcome Actions are not allowed.
Pass/Fail Criteria	Pass if the ACLs can be listed and set. They are correctly enforced for actions.
Related Information	Hydra [R 2]
Revision Log	V3: Improved wording.

1.2 File Encryption/Decryption

File Encryption/Decryption	
ID	FILECRYPT_FILE_1
Description	Hydra appliances must provide encryption and decryption of files functionality.
Mandatory	YES
Applicability	Hydra File Encryption/Decryption Appliances.
Input from Technology Provider	Support for file encryption and decryption.
Test Description	<p>Pre-condition Existing file, key registered.</p> <p>Test Encrypt and decrypt existing file.</p> <p>Expected Outcome Result of the test is identical to original file.</p>
Pass/Fail Criteria	Pass if the encryption/decryption of files functionality is provided.
Related Information	Hydra [R 2]
Revision Log	V3: Improved wording.

File Encryption/Decryption into grid storage	
ID	FILECRYPT_FILE_2
Description	Hydra appliances must allow storage of encrypted files into grid storage system and the retrieval and decryption of those files.
Mandatory	YES
Applicability	Hydra File Encryption/Decryption Appliances.
Input from Technology Provider	Support for file encryption and decryption into grid storage (SRM).
Test Description	Pre-condition Existing file, available grid storage. Test Encrypt and store file into grid storage, retrieval and decryption of file. Expected Outcome Result of the test is identical to original file. Grid storage contains encrypted file.
	Pre-condition Encrypted file stored in grid storage. Test Retrieve file, decrypt file. Expected Outcome File is correctly retrieved and decrypted.
Pass/Fail Criteria	Pass if the encryption/decryption of files into grid storage functionality is provided.
Related Information	Hydra [R 2]
Revision Log	V3: Improved wording.

2 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.

2.1 File Access Interface

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

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

3 FILE TRANSFER

3.1 File Transfer Interfaces

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

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

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

4 FILE TRANSFER SCHEDULING

These criteria are defined taking gLite FTS [R 3] as reference implementation.

4.1 File Transfer Channel Management

Channel Management Operations	
ID	FILETRANSFSCH_CHANNEL_1
Description	FTS must allow administrators to add, drop and list channels for file transfers.
Mandatory	YES
Applicability	FTS File Transfer Scheduling Appliances.
Input from Technology Provider	Support for channel management operations: add, drop and list channels for various sites. Support for setting the channel configuration.
Test Description	Pre-condition Valid administrator credentials. Valid Site A and B. Test Add transfer channel from site A to site B Expected Outcome New transfer channel created.
	Pre-condition Valid administrator credentials. Existing channel Test Drop channel. Expected Outcome Channel is dropped.
	Pre-condition Valid administrator credentials. Test List available channels Expected Outcome List of available channels is shown.
	Pre-condition Valid administrator credentials. Existing channel. Test Set channel configuration (bandwidth, transfer limit per VO, ...) Expected Outcome Channel configuration is effectively changed.
Pass/Fail Criteria	Pass if administrator can manage the channels correctly.
Related Information	gLite FTS [R 3]
Revision Log	V3: Improved wording.

Channel Manager Control		
ID	FILETRANSFSCH_CHANNEL_2	
Description	FTS must allow administrators to control who is allowed or not to manage a channel.	
Mandatory	YES	
Applicability	FTS File Transfer Scheduling Appliances.	
Input from Technology Provider	Support for channel manager control operations: add/remove channel managers and listing current channels.	
Test Description	Pre-condition Valid administrator credentials. Existing channel. Credentials of user to add as manager Test Add user as manager of channel. Test privilege operations on channel with user. Expected Outcome Manager is added; privileged operations are performed correctly.	
	Pre-condition Valid administrator credentials. Existing channel. Test List channel managers Expected Outcome List of channel managers is returned	
	Pre-condition Valid administrator credentials. Existing channel. Existing manager of channel Test Remove channel manager. Test privilege operations on channel with user Expected Outcome Manager is removed; privileged operations are not performed.	
	Pass/Fail Criteria	Pass if administrator can list and change the channel managers. The manager access is correctly enforced.
	Related Information	gLite FTS [R 3]
	Revision Log	V3: Improved wording.

4.2 File Transfer Management

File Transfer Operation Management	
ID	FILETRANSFSCH_ MGMT _1
Description	FTS must allow users to create and manage file transfer operations.
Mandatory	YES
Applicability	FTS File Transfer Scheduling Appliances.
Input from Technology Provider	Support for submission, query and cancelling file transfer operations.
Test Description	Pre-condition FTS Service available; source and destination available; list of files to transfer; valid user credentials Test Create new file transfer job. Expected Outcome New file transfer job created. ID of job returned.
	Pre-condition Transfer job ID of a previously submitted job; valid user credentials. Test Check status of job. Expected Outcome Status of job returned.
	Pre-condition Transfer job ID of a previously submitted job; valid user credentials. Test Cancel job. Expected Outcome Job is cancelled.
	Pre-condition Transfer job ID of a previously submitted job; valid user credentials. Test Cancel job. Expected Outcome Job is cancelled.
Pass/Fail Criteria	Pass if users can create and manage transfer jobs.
Related Information	gLite FTS [R 3]
Revision Log	V3: Improved wording.

End to end file transfer operation	
ID	FILETRANSFSCH_ MGMT _2
Description	FTS must execute correctly file transfer operations.
Mandatory	YES
Applicability	FTS File Transfer Scheduling Appliances.
Input from Technology Provider	End-to-end file transfer operation are performed correctly, if errors are found they are clearly indicated.
Test Description	<p>Pre-condition FTS Service available; source and destination available; list of files to transfer; valid user credentials</p> <p>Test Create new file transfer job.</p> <p>Expected Outcome New file transfer job created and executed correctly.</p>
Pass/Fail Criteria	Pass if users can create jobs and the jobs are executed correctly.
Related Information	gLite FTS [R 3]
Revision Log	V3: Improved wording.

5 STORAGE MANAGEMENT

5.1 SRM Interface

SRM API Support	
ID	STORAGE_API_1
Description	Storage Management Appliances must provide support for SRM2.2 specification.
Mandatory	YES
Applicability	Storage Management Appliances
Input from Technology Provider	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
Test Description	<p>Pre-condition Valid user credentials.</p> <p>Test Test SRMv2.2 functionality, with correct/incorrect input and with valid and invalid credentials. Use S2 [R 5] test suite for reference.</p> <p>Expected Outcome Log of all the operations performed. All the documented functions work as documented.</p>
Pass/Fail Criteria	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.
Related Information	UMD Roadmap [R 1] SRM v2.2 [R 4]
Revision Log	V3: Improved wording

LCG-UTILS test	
ID	STORAGE_API_2
Description	Test Storage Management Appliances with the lcg-utils commands.
Mandatory	YES
Applicability	Storage Management Appliances
Input from Technology Provider	Support for lcg-utils [R 7] commands, documentation of any possible incompatibilities with other Appliances.
Test Description	<p>Pre-condition Valid user credentials.</p> <p>Test Test lcg-utils commands, with correct/incorrect input and with valid and invalid credentials. An example test suite is available at [R 8]</p> <p>Expected Outcome Log of all the operations performed. All the documented functions work as documented.</p>
Pass/Fail Criteria	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.
Related Information	<p>Although all Storage Management Appliances should use SRM [R 4] 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.</p> <p>http://glite.cvs.cern.ch/cgi-bin/glite.cgi/org.glite.testsuites.ctb/UI/tests/test-lcg-utils.sh?view=markup</p>
Revision Log	V3: Added reference

5.2 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.

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

Fine grained authorization	
ID	STORAGE_DEVICE_2
Description	The Storage Management Capability must allow the implementation of a fine-grained authorization policy based on VO roles and enforce it (if defined).
Mandatory	NO
Applicability	Storage Management Appliances
Input from Technology Provider	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.
Test Description	<p>Pre-condition Configured system with a storage resource area directory tree with different authorization permissions along the directory tree for different VO roles.</p> <p>Test 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>Expected Outcome 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>
Pass/Fail Criteria	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.
Related Information	
Revision Log	

Space reservations	
ID	STORAGE_DEVICE_3
Description	The Storage Management Capability must allow the implementation of (virtual or real) reserved space areas as storage space tokens
Mandatory	NO
Applicability	Storage Management Appliances
Input from Technology Provider	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).
Test Description	<p>Pre-condition Configured system with (virtual or real) storage space reservations enabled as storage space tokens.</p> <p>Test Retrieve current status from the storage space token area.</p> <p>Expected Outcome All the mandatory Storage Element related entities of GlueSchema using the actual information for the storage space token area are generated.</p>
	<p>Pre-condition Configured system with (virtual or real) storage space reservations enabled as storage space tokens.</p> <p>Test 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>Expected Outcome 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>
Pass/Fail Criteria	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.
Related Information	
Revision Log	

Checksum	
ID	STORAGE_DEVICE_4
Description	The Storage Management Capability must support Adler32 checksum calculation and store the checksum value for a given file.
Mandatory	NO
Applicability	Storage Management Appliances
Input from Technology Provider	Support for storing/retrieving/listing a file in a storage resource through the SRM interface or LCG-UTILS enabling the checksum computation.
Test Description	<p>Pre-condition Configured system with checksum computation option enabled.</p> <p>Test Test storing/retrieving/listing a file in a storage resource through the SRM interface or LCG-UTILS enabling the checksum computation.</p> <p>Expected Outcome 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>
Pass/Fail Criteria	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.
Related Information	
Revision Log	

5.3 Service availability, monitoring and error handling

Error Messages	
ID	STORAGE_SERVICE_1
Description	Error messages provided by the service should be clear and facilitate the solution of those errors.
Mandatory	NO
Applicability	Storage Management Appliances
Input from Technology Provider	Include in documentation, a list of possible errors and possible solution/cause for it. For errors that may reach the user, this list has to be exhaustive.
Pass/Fail Criteria	Will pass if the list of errors is documented and includes information about: <ul style="list-style-type: none"> • Error code • Error message (if applicable) • 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	Client Tools Criterion: CLIENT_TOOLS_2
Revision Log	V2: major restructuring of criterion.

6 REFERENCES

R 1	UMD roadmap: https://documents.egi.eu/public/ShowDocument?docid=100
R 2	Hydra encrypted file storage: https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS
R 3	gLite FTS: https://twiki.cern.ch/twiki/bin/view/EGEE/GLiteFTS
R 4	SRM v2.2: http://www.ggf.org/documents/GFD.129.pdf
R 5	S2 Test: http://s-2.sourceforge.net/
R 6	SRM-Tester: https://sdm.lbl.gov/twiki/bin/view/Software/SRMTester/WebHome
R 7	Lcg-utils: http://grid-deployment.web.cern.ch/grid-deployment/documentation/LFC_DPM/lcg_util/
R 8	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