



# EGI-InSPIRE

## UMD STORAGE CAPABILITIES QUALITY CRITERIA v2

---

Document identifier:	EGI-STORAGE-QC-V2.docx
Date:	<b>03/08/2011</b>
Document Link:	<a href="https://documents.egi.eu/document/346">https://documents.egi.eu/document/346</a>

---

### 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](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
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



## TABLE OF CONTENTS

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

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



<b>Related Information</b>	Hydra [R 2]
<b>Revision Log</b>	

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

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

## 1.2 File Encryption/Decryption

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



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

## 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	
<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>	

### 3 FILE TRANSFER

#### 3.1 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>	<b>Pre-condition</b> Valid credentials. <b>Test</b> Transfer files via gridFTP protocol (both read and write operations) <b>Expected Outcome</b> Files can be transferred. Log of operations
<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>	

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

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



## 4.2 File Transfer Management

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

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

## 5 STORAGE MANAGEMENT

### 5.1 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>	SRM v2.2 API implementation that covers all the specification. Deviations from the API . Ideally, provide a complete test suite and results for the API.
<b>Test Description</b>	<p><b>Pre-condition</b> Valid user credentials.</p> <p><b>Test</b> Test all SRMv2.2 documented functions, with correct/incorrect input and with valid and invalid credentials. S2 [R 5] or SRM-Tester [R 6] are already existing test suites that may be used.</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. If the API is not completely supported, this should be documented. The Appliance should pass the S2 test correctly.
<b>Related Information</b>	UMD Roadmap [R 1] SRM v2.2 [R 4]
<b>Revision Log</b>	

<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 7] 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.</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 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.
<b>Revision Log</b>	

## 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.

<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>	



### 5.3 Service availability, monitoring and error handling

Error Messages	
<b>ID</b>	<b>STORAGE_SERVICE_1</b>
<b>Description</b>	Error messages provided by the service should be clear and facilitate the solution of those errors.
<b>Mandatory</b>	NO
<b>Applicability</b>	Storage Management Appliances
<b>Input from Technology Provider</b>	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.
<b>Pass/Fail Criteria</b>	Will pass if the list of errors is documented and includes information about: <ul style="list-style-type: none"> <li>• Error code</li> <li>• Error message (if applicable)</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>	
<b>Revision Log</b>	V2: major restructuring of criterion.

## 6 REFERENCES

R 1	UMD roadmap: <a href="https://documents.egi.eu/public/ShowDocument?docid=100">https://documents.egi.eu/public/ShowDocument?docid=100</a>
R 2	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>
R 3	gLite FTS: <a href="https://twiki.cern.ch/twiki/bin/view/EGEE/GLiteFTS">https://twiki.cern.ch/twiki/bin/view/EGEE/GLiteFTS</a>
R 4	SRM v2.2: <a href="http://www.ggf.org/documents/GFD.129.pdf">http://www.ggf.org/documents/GFD.129.pdf</a>
R 5	S2 Test: <a href="http://s-2.sourceforge.net/">http://s-2.sourceforge.net/</a>
R 6	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>
R 7	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>