**EGI-InSPIRE**

UMD Storage Capabilities

Quality Criteria

v1.1

|  |  |
| --- | --- |
| Document identifier: | EGI-STORAGE-QC-V1.1.docx |
| Date: | 04/02/2011 |
| Document Link: | https://documents.egi.eu/document/240 |

|  |
| --- |
| 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 |

**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

3 File Transfer 11

3.1 File Transfer Interface 11

FILETRANS\_API\_1 11

FILETRANS\_API\_2 12

FILETRANS\_API\_3 13

4 File Transfer Scheduling 14

4.1 File Transfer Channel Management 14

FILETRANSFSCH\_CHANNEL\_1 14

FILETRANSFSCH\_CHANNEL\_2 16

4.2 File Transfer Management 17

FILETRANSFSCH\_MGMT\_1 17

5 Storage Management 18

5.1 SRM Interface 18

STORAGE\_API\_1 18

5.2 Storage Device Support 19

STORAGE\_ STORAGE\_1 19

5.3 Service availability, monitoring and error handling 21

STORAGE\_SERVICE\_1 21

6 References 22

# File Encryption/Decryption

Sensitive data needs to be stored securely. Before being stored in a remote file store the file may need to be encrypted and then on retrieval de-encrypted before use. The capability should also provide solutions relating to the storage of the keys needed to perform these tasks.

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

## Key Management

|  |  |  |
| --- | --- | --- |
| Key Registration | | |
| ID | | FILECRYPT\_KEY\_1 |
| Mandatory | | |
| Applicability | | Hydra implementations of the File Encryption/Decryption Capability |
| Related Requirements | | None |
|  | | |
| Description  The capability must allow registering and unregistering keys | | |
| Input from TP  Testsuite for the key registration/unregistration interface. | | |
| Test 1 | | |
| **Pre-condition** | Keystore running, accepted user credentials. | |
| **Test** | Register key in server | |
| **Expected Outcome** | Key is successfully registered | |
| Test 2 | | |
| **Pre-condition** | Keystore running, accepted user credentials. | |
| **Test** | Register key in server specifying cipher and key length. | |
| **Expected Outcome** | Key is successfully registered | |
| Test 3 | | |
| **Pre-condition** | Keystore running, previously registered key, accepted user credentials. | |
| **Test** | Register key in server | |
| **Expected Outcome** | Warning issued, no action taken. | |
| Test 4 | | |
| **Pre-condition** | Keystore running, previously registered key, accepted user credentials. | |
| **Test** | Unregister key in server | |
| **Expected Outcome** | Key is successfully unregistered | |
| Test 5 | | |
| **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 test is provided and passes. | | |
| Related Information | | |
| History | | |

|  |  |  |
| --- | --- | --- |
| Key and Password Splitting and Recombination | | |
| ID | | FILECRYPT\_KEY\_2 |
| Mandatory | | |
| Applicability | | Hydra implementations of the File Encryption/Decryption Capability |
| Related Requirements | | None |
|  | | |
| Description  The capability must provide functionality for generating, splitting and recombine keys and passwords | | |
| Input from TP  Testsuite for the split and joining password and keys. Test for different combination of number of parts and minimum number of parts needed for recombinations. | | |
| Test 1 | | |
| **Pre-condition** | Password/Key to split | |
| **Test** | Split password/key. | |
| **Expected Outcome** | Password is successfully splitted | |
| Test 2 | | |
| **Pre-condition** | Whole set of Password/key splits | |
| **Test** | Join splits | |
| **Expected Outcome** | Password/key successfully joined. | |
| Test 3 | | |
| **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 test is provided and passes. | | |
| Related Information | | |
| History | | |

|  |  |  |
| --- | --- | --- |
| Key ACL management | | |
| ID | | FILECRYPT\_KEY\_3 |
| Mandatory | | |
| Applicability | | Hydra implementations of the File Encryption/Decryption Capability |
| Related Requirements | | None |
|  | | |
| Description  The capability must allow the management of ACLs for a file/key. | | |
| Input from TP  Testsuite for the management of ACL, test for different permissions and users. | | |
| Test 1 | | |
| **Pre-condition** | Key registered in server, user allowed to list ACLs of key | |
| **Test** | List key ACLs | |
| **Expected Outcome** | ACLs of file correctly shown. | |
| Test 2 | | |
| **Pre-condition** | Key registered in server, user allowed to modify ACLs of key | |
| **Test** | Set new ACL for key. | |
| **Expected Outcome** | ACL changed correctly. | |
| Test 3 | | |
| **Pre-condition** | Key registered in server, ACL of key set. | |
| **Test** | Try allowed actions for ACL. | |
| **Expected Outcome** | Actions are performed correctly | |
| Test 4 | | |
| **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 test is provided and passes. | | |
| Related Information | | |
| History | | |

## File Encryption/Decryption

|  |  |  |
| --- | --- | --- |
| File Encryption/Decryption | | |
| ID | | FILECRYPT\_FILE\_1 |
| Mandatory | | |
| Applicability | | Hydra implementations of the File Encryption/Decryption Capability |
| Related Requirements | | None |
|  | | |
| Description  The capability must allow encryption and decryption of files. | | |
| Input from TP  Testsuite for the file encryption and decryption. | | |
| Test 1 | | |
| **Pre-condition** | Existing file, key registered. | |
| **Test** | Encrypt and decrypt existing file. | |
| **Expected Outcome** | Result of the test is identical to original file. | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

|  |  |  |
| --- | --- | --- |
| File Encryption/Decryption into grid storage | | |
| ID | | FILECRYPT\_FILE\_2 |
| Mandatory | | |
| Applicability | | Hydra implementations of the File Encryption/Decryption Capability |
| Related Requirements | | None |
|  | | |
| Description  The capability must allow storage of encrypted files into grid storage system and the retrieval and decryption of those files. | | |
| Input from TP  Testsuite for the file encryption and decryption into grid storage. | | |
| Test 1 | | |
| **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. | |
| Test 2 | | |
| **Pre-condition** | Encrpyted file stored in SRM. | |
| **Test** | Retrieve file, decrypt file. | |
| **Expected Outcome** | File is correctly retrieved and decrypted. | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

# 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.

## File Access Interface

|  |  |  |
| --- | --- | --- |
| POSIX File Access | | |
| ID | | FILEACC\_API\_1 |
| Mandatory | | |
| Applicability | | Storage Management Capabilities that include the File Access Interface |
| Related Requirements | | None |
|  | | |
| Description  Provide genuine POSIX file system through mounted file systems. | | |
| Input from TP  Testsuite for the POSIX file access. | | |
| Test Suite Description. | | |
| **Pre-condition** | POSIX access configured and available for user. | |
| **Test** | Complete POSIX file operations tests. | |
| **Expected Outcome** | POSIX file operations work as documented. Log of operations | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

# File Transfer

Files are stored at different physical locations within the production infrastructure and are frequently used at other locations. It is necessary for the files to be efficiently transferred over the international wide area networks linking the different resource centres.

## File Transfer Interface

|  |  |  |
| --- | --- | --- |
| GridFTP File Access | | |
| ID | | FILETRANS\_API\_1 |
| Mandatory | | |
| Applicability | | File Transfer Capability implementations |
| Related Requirements | | None |
|  | | |
| Description  Provide gridFTP access for reading data. | | |
| Input from TP  Test to check the capability to read and write data from the Storage Resource using gridFTP. | | |
| Test Suite Description. | | |
| **Pre-condition** | Valid credentials. | |
| **Test** | Transfer files via gridFTP protocol (both read and write operations) | |
| **Expected Outcome** | Files can be transferred. Log of operations | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

|  |  |  |
| --- | --- | --- |
| HTTPS File Access | | |
| ID | | FILETRANS\_API\_2 |
| Not Mandatory | | |
| Applicability | | File Transfer Capability implementations |
| Related Requirements | | None |
|  | | |
| Description  Provide HTTP(S) access for reading data. | | |
| Input from TP  Test to check the capability to read data from the Storage Resource using http(s) | | |
| Test Suite Description. | | |
| **Pre-condition** | Valid credentials. | |
| **Test** | Transfer files via HTTP(s) protocol. | |
| **Expected Outcome** | Files can be transferred. Log of operations | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

|  |  |  |
| --- | --- | --- |
| WebDAV File Access | | |
| ID | | FILETRANS\_API\_3 |
| Not Mandatory | | |
| Applicability | | File Transfer Capability implementations |
| Related Requirements | | None |
|  | | |
| Description  Provide WebDAV access for data. | | |
| Input from TP  Test to check the capability to read and write data from the Storage Resource using WebDAV. | | |
| Test Suite Description. | | |
| **Pre-condition** | Valid credentials. | |
| **Test** | Transfer files via WebDAV protocol (both read and write operations) | |
| **Expected Outcome** | Files can be transferred. Log of operations | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

# File Transfer Scheduling

These criteria are defined taking gLite FTS as reference implementation.

## File Transfer Channel Management

|  |  |  |
| --- | --- | --- |
| Channel Management Operations | | |
| ID | | FILETRANSFSCH\_CHANNEL\_1 |
| Mandatory | | |
| Applicability | | FTS implementations of the File Transfer Channel Capability |
| Related Requirements | | None |
|  | | |
| Description  FTS should allow administrator to add, drop and list channels for file transfers. | | |
| Input from TP  Test the channel management operations. | | |
| Test 1 | | |
| **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. | |
| Test 2 | | |
| **Pre-condition** | Valid administrator credentials. Existing channel | |
| **Test** | Drop channel. | |
| **Expected Outcome** | Channel is dropped. | |
| Test 3 | | |
| **Pre-condition** | Valid administrator credentials. | |
| **Test** | List available channels | |
| **Expected Outcome** | List of available channels is shown. | |
| Test 4 | | |
| **Pre-condition** | Valid administrator credentials. Existing channel. | |
| **Test** | Change channel configuration (bandwith, transfer limits per VO, …) | |
| **Expected Outcome** | Channel configuration is effectively changed. | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

|  |  |  |
| --- | --- | --- |
| Channel Manager Control | | |
| ID | | FILETRANSFSCH\_CHANNEL\_2 |
| Mandatory | | |
| Applicability | | FTS implementations of the File Transfer Channel Capability |
| Related Requirements | | None |
|  | | |
| Description  FTS should allow administrator to control who is allowed or not to manage a channel. | | |
| Input from TP  Test the channel manager control operations. | | |
| Test 1 | | |
| **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. | |
| Test 2 | | |
| **Pre-condition** | Valid administrator credentials. Existing channel. | |
| **Test** | List channel managers | |
| **Expected Outcome** | List of channel managers is returned | |
| Test 3 | | |
| **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 the test is provided and passes. | | |
| Related Information | | |
| History | | |

## File Transfer Management

|  |  |  |
| --- | --- | --- |
| File Transfer Operation Management | | |
| ID | | FILETRANSFSCH\_MGMT\_1 |
| Mandatory | | |
| Applicability | | FTS implementations of the File Transfer Channel Capability |
| Related Requirements | | None |
|  | | |
| Description  The FTS service must allow users to create and manage file transfer operations. | | |
| Input from TP  Testsuite for the submission, query and cancelling file transfer operations. | | |
| Test 1 | | |
| **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. | |
| Test 2 | | |
| **Pre-condition** | Transfer job ID of a previously submitted job; valid user credentials. | |
| **Test** | Check status of job. | |
| **Expected Outcome** | Status of job returned. | |
| Test 3 | | |
| **Pre-condition** | Transfer job ID of a previously submitted job; valid user credentials. | |
| **Test** | Cancel job. | |
| **Expected Outcome** | Job is cancelled. | |
| Test 4 | | |
| **Pre-condition** | Valid user credentials. | |
| **Test** | List jobs submitted by user. | |
| **Expected Outcome** | List of jobs is returned. | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

# Storage Management

The bandwidth linking resource sites is a resource that needs to be managed in the same way compute resources at a site are accessed through a job scheduler. By being able to schedule wide area data transfers, requests can be prioritised and managed. This would include the capability to monitor and restart transfers as required.

## SRM Interface

|  |  |  |
| --- | --- | --- |
| SRM API Testsuite | | |
| ID | | STORAGE\_API\_1 |
| Mandatory | | |
| Applicability | | Implementations of Storage Management Capability. |
| Related Requirements | | None |
|  | | |
| Description  The Storage Resource Management (SRM) [R 5] interface specification is a commonly adopted specification in this area that defines much of the functionality used in this area. The implementations of the Storage Management capability must provide a complete test suite for the SRM2.2 specification. | | |
| Input from TP  Execute a complete test suite for the SRM v2.2 that covers all the specification. S2 [R 6] or SRM-Tester [R 7] are already existing testsuites that may be used for that purpose.  Test erroneous of input and erroneous user authorization should be covered by the testsuite. | | |
| Test Suite Description | | |
| **Pre-condition** | Valid user credentials. | |
| **Test** | Test all SRMv2.2 documented functions, with correct/incorrect input and with valid and invalid credentials. | |
| **Expected Outcome** | Log of all the operations performed. All the documented functions work as documented. | |
| Pass/Fail Criteria  Pass if the testsuite is provided and passes. | | |
| Related Information | | |
| History | | |

## 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:

* list here!

|  |  |  |
| --- | --- | --- |
| Space Management | | |
| ID | | STORAGE\_ STORAGE\_1 |
| Mandatory | | |
| Applicability | | Implementations of Storage Management Capability. |
| Related Requirements | | None |
|  | | |
| Description  The space management functionality of the Storage Management Capability must be tested with the storage devices supported. | | |
| Input from TP  Test of space management functionality (for each of the supported storage devices):   * Reserve/release storage space * Update already reserved space. * Get information about space. | | |
| Test 1 | | |
| **Pre-condition** | Correctly configured system | |
| **Test** | Reserve space | |
| **Expected Outcome** | Space is reserved in the storage device | |
| Test 2 | | |
| **Pre-condition** | Correctly configured system, reserved space exists. | |
| **Test** | Release already reserved space | |
| **Expected Outcome** | Space is released in the storage device | |
| Test 3 | | |
| **Pre-condition** | Correctly configured system, reserved space exists. | |
| **Test** | Update already reserved space | |
| **Expected Outcome** | Space is updated in the storage device | |
| Test 4 | | |
| **Pre-condition** | Correctly configured system, reserved space exists. | |
| **Test** | Get information about reserved space. | |
| **Expected Outcome** | Reserved space information is returned. | |
| Test 4 MISSING ERROR TESTS! | | |
| **Pre-condition** | n | |
| **Test** | n | |
| **Expected Outcome** | n | |
| Pass/Fail Criteria  Pass if the test is provided and passes. | | |
| Related Information | | |
| History | | |

## Service availability, monitoring and error handling

|  |  |
| --- | --- |
| Error Messages | |
| ID | STORAGE\_SERVICE\_1 |
| Non Mandatory | |
| Applicability | Implementations of Storage Management Capability. Applicable for every service, and specially for the command line interface |
| Related Requirements |  |
|  | |
| Description  The error messages provided by the service should be clear and facilitate the solution of those errors. | |
| Input from TP  For every service a list of possible errors that can appear must be provided. In case of command line interface, this list has to be exhaustive to all the messages that a user can obtain from its usage.  The list of messages have to contain the following fields:   * Error code (if applicable) * Error message * 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) | |
| Pass/Fail Criteria  A complete list of errors per service is provided | |
| Related Information | |
| History | |

# References

|  |  |
| --- | --- |
|  | UMD roadmap: <https://documents.egi.eu/public/ShowDocument?docid=100> |
|  | Generic UMD Quality Criteria |
|  | Security Capabilities Quality Criteria |
|  | Operational Capabilities Quality Criteria |
|  | SRM v2.2: <http://www.ggf.org/documents/GFD.129.pdf> |
|  | S2 Test: <http://s-2.sourceforge.net/> |
|  | SRM-Tester: <https://sdm.lbl.gov/twiki/bin/view/Software/SRMTester/WebHome> |