# Table of Contents

# HydraTest Plan

## Service Description

Hydra is a distributed redundant keystore. The CERN twiki has a description and installation instructions. The available test can be found in the glite CVS.

## Features/Scenarios to be tested

These are the tests for the client side `glite-eds-*` and `glite-ssss-*` commands and their parameters. There is also a test for the server to check that required services are running. The tests can be run with default parameters, or they can use specific parametes/environment variables as described in README. All tests require at least one voms proxy certificate. The hydra client and server can be installed on the same machine for the tests. If they are not, `hydra-server-test.sh` should be run on the server, the other tests on the client.

#### 'Service ping test' (implemented)

This test checks that all required services are configured and running on the server.

##### Normal workflow - correct input

This service has no input. The test prints output for each succesful subtest, and a final success confirmation.

##### Pass/Fail Criteria

This test should pass if all required services are running, otherwise it should fail

##### Error workflow - erroneous input

N/A

##### Pass/Fail Criteria

N/A

#### 'SSSS-tools test' (implemented)

This test checks the glite-ssss-* tools that are a prerequisite for hydra to work. This test can optionally test that man pages are found if MAN_PAGE_CHECK is set (default).

##### Normal workflow - correct input

This test tests that keys can be generated, split and recombined using the glite-ssss* tools. It does the same tests for splitting passphrases.

##### Pass/Fail Criteria

This test should pass if all tests pass and glite-ssss-* commands behve as described. Otherwise the test fails.

##### Error workflow - erroneous input

This test does not test for erroneous input

#### Pass/Fail Criteria

N/A

#### 'Key registration test' (implemented)

This test depends on previous tests. The test tries to register and unregister keys in the hydra keystore. This test can optionally test that man pages are found if MAN_PAGE_CHECK is set (default).

#### Normal workflow - correct input

This test checks that keys can be registered to the hydra keystore, and removed from there. It also test specifying ciphers for the key.

#### Pass/Fail Criteria

This test should pass if all tests pass and keys can be registered and unregistered. Otherwise the test fails.

#### Error workflow - erroneous input

This test tries to register new keys with existing names, and unregister nonexisting keys.

#### Pass/Fail Criteria

This test should pass if all the checks return errors. Otherwise the test fails.

#### 'Crypt test' (implemented)

This test depends on previous tests. The test tries to en-/decrypt a file using the keys in the hydra keystore. This test can optionally test that man pages are found if MAN_PAGE_CHECK is set (default).

#### Normal workflow - correct input

This test tries to encrypt a file and checks that it's is encrypted. It also tries to decrypt a file, and checks that the decrypted file matches the original

#### Pass/Fail Criteria

This test should pass if all tests pass and files can be en-/decrypted succesfully. Otherwise the test fails.

#### Error workflow - erroneous input

This test does not test for erroneous input

#### Pass/Fail Criteria

N/A

#### 'ACL test' (implemented)

This test depends on previous tests. The test tries to change the ACL of keys in the keystore. This test can optionally test that man pages are found if MAN_PAGE_CHECK is set (default).

#### Normal workflow - correct input

This test tries to change the ACL's of keys in the keystore with different command line parameters. It then confirms that the keys have the correct new permissions. If two proxy certificates are available, ACL permissions are tested.

#### Pass/Fail Criteria

This test should pass if all tests pass and the ACLs can be set. In only one proxy certificate is available, the ACL permission tests are not run.

#### Error workflow - erroneous input

If two proxy certificates are available, ACL permission enforcing is tested. The test tries to modify a key with a non-privileged certificate.

#### Pass/Fail Criteria

This test should pass if ACLs can't be modified with an unprivileged certificate. In only one proxy certificate is available, the ACL permission enforcing test are not run.

### 'Chmod test' (implemented)

This test depends on previous tests. The test tries to change the `user`, `group` and `other` permissions of keys in the keystore. This test can optionally test that man pages are found if MAN_PAGE_CHECK is set (default).

#### Normal workflow - correct input

This test tries to modify the user, group and other permissions of keys with different command line parameters, and verifies that these are changed. If two proxy certificates are available, the group/other permissions are tested.

#### Pass/Fail Criteria

This test should pass if all tests pass and the chmod permissions can be set. If two proxy certificates are available, the chmod permission checks need to pass.

#### Error workflow - erroneous input

If two proxy certificates are available, the group/other permissions enforcing is tested with a non-privileged certificate.

#### Pass/Fail Criteria

This test should pass if permissions can't be modified with an unprivileged certificate. In only one proxy certificate is available, the permission enforcing test are not run.

### 'File storage and retrieval tests' (implemented)

This test depends on previous tests. The test tries to register, encrypt, retrieve and decrypt files. This test can optionally test that man pages are found if MAN_PAGE_CHECK is set (default).

#### Normal workflow - correct input

This test should try to register an encrypted file with the hydra client tools. This file should be retrieved an decrypted using both hydra tools and lcg tools. An encrypted file should also be saved using lcg tools and retrieved using glite tools.

#### Pass/Fail Criteria

This test should pass if all tests pass and the files can be stored and retrieved. Encrypted files need to differ from plaintext files, and decrypted files must match plaintext files

#### Error workflow - erroneous input

Erroneous input is not tested at this point. Erroneous input causes a failure immideately (e.g. false filename). For example giving the "wrong" decryption key as an argument for decryption is considered valid, but the decrypted file is naturally garbled.

#### Pass/Fail Criteria

N/A

# Features not to be tested

N/A

# Stress testing

There is a simple stress/performance testing script included. It spawns multiple threads to register/unregister keys, and reports how many keys were handled / second

# Hydra security testing

As security is a very critical part of the Hydra service, a security test should be done to both the client side and the server side.

### Hydra server security testing

The hydra server is more security-critical than the client. The server can be hosted by an unknown party, and it contains (parts of) encryption keys which can give access to classified data. The server is written in the Java language, which makes it resistant to some attacks (e.g. buffer overflow). The server can however be vulnerable to many other types of attacks, and here I try to identify the most critical parts of the software, and what should be checked.

Installation

- Tomcat is configured properly to use correct host certificate, any cerftificates + keys that are copied have the correct permissions on the filesystem.
- Access to created databases is given only to specified users
- Any files which contain passwords have restrictive filesystem permissions
- No passwords are left in installation (or other) logs

Server

- Client input is always verified
    - In every place, client input must be assumed to be malicious
    - All database inputs need to be sanitized
    - Resulting data from database queries should be verified as far as possible
    - Client certificate needs to be valid (CA, VO, expiry)
- In all operations the user is only authorized to access (/remove/modfify) what the ACL and permissions allow him/her to
- Multiple commands are handled in a way so that each command is authorized separately
- The database connection is handled securely if database is on another machine
    - No cleartext authentication or key(part) exchange (REQUIRED?)

### Hydra client security testing

The hydra client is run by the user so it is not as vulnerable as the server. The client handles encryption keys however, so their correct usage should be confirmed.

Client

- Key generation is done with specified ciphers and keylengths
- After key usage the memory area where the keys were is blanked or randomized.
- The client checks that the server has a valid certificate which matches the hostname

-- KalleHapponen - 04 Aug 2008

---

This topic: EGEE > HydraTestPlan
Topic revision: r11 - 2009-03-12 - KalleHapponen