QUANTINUUM

Quantum Origin and Thales Luna 7 HSM Installation Guide

Ubuntu 20.04

Version 1.0, April 2023

Contents

- INTRODUCTION 3
- ENVIRONMENT OVERVIEW: 4
- LUNA 7 HSM PARTITIONS 5
- RESEED CLIENT SERVER FILES 5
- HSM ORIGIN PARTITION OBJECTS 6
- INSTALLATION INSTRUCTIONS 6

Remove Existing Install 6

Install the Reseed Client 7

Prepare the Instance for Onboarding 8

Configure Reseed Client and Luna HSM 10

Start the Reseed Client Service 13

- VERIFYING NORMAL OPERATIONS – RESEED CLIENT 13
- VERIFYING NORMAL OPERATIONS – HSM AUDIT LOGS 14

INTRODUCTION

This document describes the installation instructions for the Reseed Client and other preparation needed for an HSM infrastructure. This document should serve as a baseline for production infrastructure deployed and can be referenced for future redeployment or if migration to other existing server infrastructure becomes necessary.

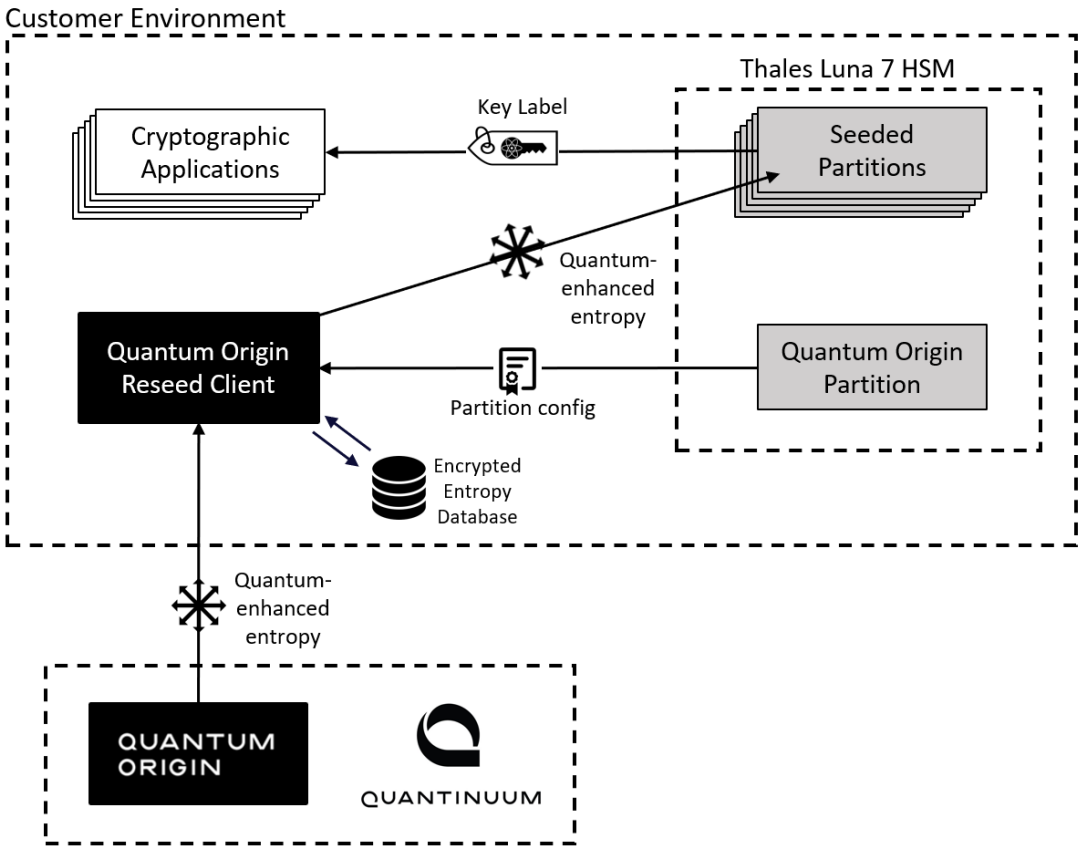
This installation guide assumes that the following dependencies are satisfied:

- Ubuntu Server 20.04 LTS is used for the deployment.
- Thales Luna 7 Network HSM running firmware 7.7.0+.
- The Thales HSM Client v10.3.0+, configured with the following components:
    - PKCS#11 (JCPROV PKCS#11 Java Wrapper).
    - FM Tools.
- Partitions have been defined on the Luna 7 HSM:
    - **Origin Partition** – secure data storage for the Reseed Client.
    - **Seeded Partition** – working HSM partition being seeded.
- Each Luna HSM partition being seeded has been configured and is accessible from LunaCM and the Thales PKCS#11 libraries.
- Credentials have been established for each partition for both the CO and CU users.

ENVIRONMENT OVERVIEW:

The Reseed Client is designed to retrieve verifiable quantum-derived entropy from the Quantum Origin Cloud (QOC) and make it available to the Thales Luna 7 HSM. Entropy is encrypted when in transit between the QOC and Reseed Client and between the Reseed Client and Thales Luna 7 HSM.

Entropy is continually seeded into the Luna 7 HSM, enhancing the quality of the HSM's onboard DRBG using the QOC. This results in the best possible keys, generated from a verifiable source of randomness, allowing all keys to be generated from a quantum process.



LUNA 7 HSM PARTITIONS

For the purpose of this guide, the following HSM partitions are defined. These partitions are referenced throughout the guide. In a customer environment, these names must be changed based on the partition labels used by the customer's environment.

Partition Label	Description
Origin_Partition	The Reseed Client data storage partition. This partition maintains data objects within it that are used by the Reseed Client to seed entropy into the Seeded Partitions.
Seeded_Partition1	An Application Partition that is being seeded with entropy by the Reseed Client
Seeded_Partition2	An Application Partition that is being seeded with entropy by the Reseed Client
Seeded_Partition3	An Application Partition that is being seeded with entropy by the Reseed Client

RESEED CLIENT SERVER FILES

The following files are defined for on the Reseed Client service instances on Ubuntu 20.04.

File	Location
QO CLI	`/usr/bin/qo_hsm_cli`
QO Reseed Service	`/usr/bin/qo_hsm_reseed_service`
Configuration File	`/etc/qo/reseed_service_config.yml`
Syslog	`/var/log/syslog`
Reseed Client Certificate	`/etc/qo/certs/client.crt.pem`
Reseed Client Private Key	`/etc/qo/certs/client.prv.pem`
On-Disk Entropy Database	`/var/lib/qo/reseed_service.sqlite`*****
Thales PKCS#11 Library	`/usr/safenet/lunaclient/lib/libCryptoki2_64.so`

***** The On-Disk Entropy Database **should never** be backed up or migrated between servers. If an Ubuntu server needs to be reprovisioned or migrated, the operator must not copy the database. An empty database is automatically created the first time the Reseed Client is started, if it does not exist on the system disk. Please ensure any automated backup or migration tools explicitly exclude the On-Disk Entropy Database or server from their operations, unless discussed with Quantinuum beforehand.

HSM ORIGIN PARTITION OBJECTS

The following objects are stored within the Origin Partition.

Object	Description
rsaWrappingKey_QOCS	RSA wrapping key for import of AES256 shared secrets
aesSharedSecret_QOCS	The AES256 Shared Secret that encrypts entropy between the QOC and the Reseed Client
seededPartition1_CO_Password	CO user password for Seeded_Partition1, used by the Reseed Client to login to the partition
seededPartition2_ CO_Password	CO user password for Seeded_Partition2, used by the Reseed Client to login to the partition
seededPartition3_ CO_Password	CO user password for Seeded_Partition3, used by the Reseed Client to login to the partition

INSTALLATION INSTRUCTIONS

The following instructions provide a step-by-step guide to installing the Reseed Client and configuring the HSM environment.

Remove Existing Install

If the system has been previously setup with a previous version of the Reseed Client, these steps will remove the previous version and make the system available for the new Reseed Client.

1. Disable and remove any existing Reseed Client installs.

```
$ sudo systemctl stop qo-hsm-reseed.service
```

2. Verify that the qo-hsm-reseed service has been stopped and is no longer running.

```
$ sudo systemctl status qo-hsm-reseed.service
● qo-hsm-reseed.service - Quantum Origin Hsm Reseed Service
  Loaded: loaded (/lib/systemd/system/qo-hsm-reseed.service; enabled; vendor
preset: enabled)
     Active: inactive (dead) since Thu 2023-01-26 23:22:24 UTC; 8min ago
    Process: 113197 ExecStart=/usr/bin/qo_hsm_reseed_service –
    config=/etc/qo/reseed_service_config.yml (code=killed, signal=>
   Main PID: 113197 (code=killed, signal=TERM)

Jan 26 23:22:24 ubuntu systemd[1]: Stopping Quantum Origin Hsm Reseed Service...
Jan 26 23:22:24 ubuntu systemd[1]: qo-hsm-reseed.service: Succeeded.
Jan 26 23:22:24 ubuntu systemd[1]: Stopped Quantum Origin Hsm Reseed Service.
```

3. Remove the existing Reseed Client package.

```
$ sudo apt remove qo-hsm-reseed-service
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
```

```
  qo-hsm-reseed-service
0 upgraded, 0 newly installed, 1 to remove and 33 not upgraded.
After this operation, 22.7 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 117574 files and directories currently installed.)
Removing qo-hsm-reseed-service (2.2.0) ...
```

4. Disable the service.

```
$ sudo systemctl disable qo-hsm-reseed.service
Removed /etc/systemd/system/multi-user.target.wants/qo-hsm-reseed.service.
```

Install the Reseed Client

1. Transfer the Reseed Client to the Ubuntu Server.

```
$ scp ~/qo_hsm_deb_Release-v*.*.*.tgz user@ubuntu:~/
qo_hsm_deb_Release-v*.*.*.tgz               100% 9428KB   7.1MB/s   00:01
```

2. Login to the Ubuntu Server and extract the files from both archives.

```
$ ssh user@ubuntu
user@ubuntu's password:
```

```
$ tar zxvf ./qo_hsm_deb_Release-v2.2.3.tgz
qo_hsm_deb_Release-v2.2.3/
qo_hsm_deb_Release-v2.2.3/qo-hsm-reseed-service_2.2.3_amd64.deb
LICENSE
```

3. Install the Reseed Client.

```
$ sudo apt install ~/qo_hsm_deb_Release-v2.2.3/qo-hsm-reseed-
service_2.2.3_amd64.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'qo-hsm-reseed-service' instead of './qo-hsm-reseed-
service_2.2.3_amd64.deb'
The following NEW packages will be installed:
  qo-hsm-reseed-service
0 upgraded, 1 newly installed, 0 to remove and 33 not upgraded.
Need to get 0 B/9,679 kB of archives.
After this operation, 22.7 MB of additional disk space will be used.
Get:1 /home/user/qo-hsm-reseed-service_2.2.3_amd64.deb qo-hsm-reseed-service
amd64 2.2.3 [9,679 kB]
Selecting previously unselected package qo-hsm-reseed-service.
(Reading database ... 117571 files and directories currently installed.)
Preparing to unpack .../qo-hsm-reseed-service_2.2.3_amd64.deb ...
Unpacking qo-hsm-reseed-service (2.2.3) ...
Setting up qo-hsm-reseed-service (2.2.3) ...
qo-hsm-reseed.service is a disabled or a static unit not running, not starting
it.
```

4. Add the current user to the qo group.

```
$ sudo addgroup user qo
Adding user `user' to group `qo' ...
Adding user user to group qo
Done.
```

Prepare the Instance for Onboarding

This section defines the configuration of the Reseed Client, establishing trust between the QOC and the Reseed Client and onboarding the client to authorize connectivity to the QOC. This process involves, the following steps:

- Generate TLS keypair and Certificates for the Reseed Client server.
  - You will need access to a CA to sign your request.
- Generate a wrapping keypair on the Luna HSM.
- Provide the server certificate and wrapping public key to Quantinuum.
- Install the Quantinuum-provided wrapped AES256 shared secret into the HSM.

1. Make a temporary certs folder in the home directory of the Ubuntu server.

```
$ mkdir ~/temp_certs/
```

2. Using OpenSSL, generate the TLS keypair and signing request.

```
$ openssl req -new                                                  \
     -newkey rsa:<2048/3072/4096>                                   \
     -nodes                                                         \
     -keyout ~/temp_certs/client.prv.pem                            \
     -out ~/temp_certs/client.req.pem                               \
     -sha256                                                        \
     -addext keyUsage=critical,digitalSignature,keyEncipherment     \
     -addext extendedKeyUsage=clientAuth

Generating a RSA private key
.............................................+++++
..................................................
..................................................
...+++++
writing new private key to '/etc/qo/certs/client.prv.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:State
Locality Name (eg, city) []:City
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organization
Organizational Unit Name (eg, section) []:Unit
Common Name (e.g. server FQDN or YOUR name) []:Client Cert
Email Address []:user@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Note: Update items in **bold** as required by your organization

3. Using `scp`, export the certificate signing request and have it signed with either a private CA controlled by your organization or have it signed with a public CA.

```
user@external_host:~/$ scp user@ubuntu:~/temp_certs/client.req.pem ~/
```

Have the CSR signed by a CA, generating an X.509 certificate.

4. Using `scp`, import the signed certificate to the Reseed Client server, saving it to the interim directory on the server.

```
$ scp ~/client.crt.pem user@ubuntu:~/temp_certs/client.crt.pem
```

5. Using the `qo_hsm_cli`, generate the wrapping key. This key will be used to securely transport the AES256 Shared Secret from Origin into the Thales Luna HSM.

```
$ qo_hsm_cli genrsa                                    \
    --primary_slot_token_label Origin_Partition        \
    --wrapkey_label rsaWrappingKey_QOCS                \
    --file ~/temp_certs/rsaWrappingKey_QOCS.pub.pem

[2023-02-03 14:05:29.463] [info] Starting...
Enter primary slot password: <ORIGIN_PARTITION_CO_PASSWORD>

[2023-02-03 14:05:35.701] [info] Loading PKCS11 Library at
/usr/safenet/lunaclient/lib/libCryptoki2_64.so
```

6. **Provide the following files to your contact at Quantinuum** for Onboarding to the QOC service. Use `scp` to export the files.
    - `rsaWrappingKey_QOCS.pub.pem`
    - `client.crt.pem`
    - The public or private CA tree that was used to sign `client.crt.pem`

```
user@external_host:~/$ scp user@ubuntu:~/temp_certs/rsaWrappingKey_QOCS.pub.pem
~/
user@external_host:~/$ scp user@ubuntu:~/temp_certs/client.crt.pem ~/
```

Your Quantinuum representative will authorize your client certificates for use with the QOC and generate a AES256 Shared Secret encrypted under the supplied wrapping key. Quantinuum staff may ask for an out-of-band verification of the public key hash, verifying the authenticity of the supplied public keys.

Configure Reseed Client and Luna HSM

This section provides details for the final configuration of the Reseed Client configuration files and Thales Luna 7 HSM.

1. Copy the provided wrapped secret provided by Quantinuum staff during the onboarding of your environment.

```
user@external_host:~/$ scp \
    ~/aesSharedSecret_QOCS.wrap
user@ubuntu:~/temp_certs/aesSharedSecret_QOCS.wrap
```

2. Inject the AES256 Shared Secret for each Reseed Client.

```
$ qo_hsm_cli load                                          \
    --primary_slot_token_label Origin_Partition           \
    --wrapkey_label rsaWrappingKey_QOCS                   \
    --secret_label aesSharedSecret_QOCS                   \
    --secret_file ~/temp_certs/aesSharedSecret_QOCS.wrap
[2023-02-03 16:01:55.595] [info] Starting...
Enter primary slot password: <ORIGIN_PARTITION_CO_PASSWORD>

[2023-02-03 16:02:02.337] [info] Loading PKCS11 Library at
/usr/safenet/lunaclient/lib/libCryptoki2_64.so
[2023-02-03 16:02:03.226] [info] Secret loaded with label aesSharedSecret_QOCS
```

3. Load the HSM Password for each Seeded Partition.

```
$ qo_hsm_cli password                                 \
    --primary_slot_token_label Origin_Partition    \
    --label seededPartition1_CO_Password

[2023-01-27 01:12:51.221] [info] Starting...
Enter primary slot password: <ORIGIN_PARTITION_CO_PASSWORD>
[2023-01-27 01:12:55.977] [info] Loading PKCS11 Library at
/usr/safenet/lunaclient/lib/libCryptoki2_64.so
Enter password to load: <SEEDED_PARTITION1_CO_PASSWORD>
[2023-01-27 01:12:58.186] [info] Password loaded

$ qo_hsm_cli password                                 \
    --primary_slot_token_label Origin_Partition    \
    --label seededPartition2_CO_Password

[2023-01-27 01:12:51.221] [info] Starting...
Enter primary slot password: <ORIGIN_PARTITION_CO_PASSWORD>
[2023-01-27 01:12:55.977] [info] Loading PKCS11 Library at
/usr/safenet/lunaclient/lib/libCryptoki2_64.so
Enter password to load: <SEEDED_PARTITION2_CO_PASSWORD>
[2023-01-27 01:12:58.186] [info] Password loaded

$ qo_hsm_cli password                                 \
    --primary_slot_token_label Origin_Partition    \
    --label seededPartition3_CO_Password

[2023-01-27 01:12:51.221] [info] Starting...
Enter primary slot password: <ORIGIN_PARTITION_CO_PASSWORD>
```

```
[2023-01-27 01:12:55.977] [info] Loading PKCS11 Library at
/usr/safenet/lunaclient/lib/libCryptoki2_64.so
Enter password to load: <SEEDED_PARTITION3_CO_PASSWORD>
[2023-01-27 01:12:58.186] [info] Password loaded
```

4. Copy all files from the interim directory to the `/etc/qo/certs` directory.

```
$ sudo mv ~/temp_certs/ /etc/qo/certs
```

5. Using a text editor, set the Origin configuration file. Make sure to do this for each /etc/qo/reseed_service_config.yml file on each Ubuntu server.

```
$ sudo vim /etc/qo/reseed_service_config.yml
api:
    auth:
        certificate: /etc/qo/certs/client.crt.pem
        private_key: /etc/qo/certs/client.prv.pem
        api_key: <API_KEY>
    url: https://<URL>.cambridgequantum.com/api/v1
    connect_timeout: 10
    request_timeout: 10
    batching: true

hsms:
  - primary_slot:
      # Origin Data Storage Partition
      token_label: Origin_Partition
      login_type: co
      password: <ORIGIN_PARTITION_CO_PASSWORD>

    partitions_to_seed:
      - token_label: Seeded_Partition1
        password_label: seededPartition1_CO_Password
      - token_label: Seeded_Partition2
        password_label: seededPartition2_CO_Password
      - token_label: Seeded_Partition3
        password_label: seededPartition3_CO_Password

    shared_secret_label: aesSharedSecret_QOCS

# Duplicate if seeding across multiple HSMs
#  - primary_slot:
#      # Origin Data Storage Partition
#      token_label: Origin_Partition
#      login_type: cu
#      password: <ORIGIN_PARTITION_CU_PASSWORD>
#
#    partitions_to_seed:
#      - token_label: Seeded_Partition1
#        password_label: seededPartition1_Password
#      - token_label: Seeded_Partition2
#        password_label: seededPartition2_Password
#      - token_label: Seeded_Partition3
#        password_label: seededPartition3_Password
#
#    shared_secret_label: aesSharedSecret_QOCS
```

```
service:
    seed_amount: 48                                          # Bytes
    seed_period: 10                                          # Seed interval, in
seconds
    cache_count: 43200                                       # max size = 43200
    service_id: server_name                                  # local server name
    p11_lib: /usr/safenet/lunaclient/lib/libCryptoki2_64.so
    database: /var/lib/qo/reseed_service.sqlite

logging:
    level: info
```

Note: The configuration file should be updated based on your configuration:

- **API_KEY**: The API key provided by Quantinuum during your onboarding.
- **URL**: The URL that was provided by Quantinuum and the region from which you will access the QOC.

6. Set the restrictive permissions on the /etc/qo directory, subdirectories, and files.

```
$ sudo chown -R qo:qo /etc/qo
$ sudo find /etc/qo -type d -exec chmod 750 {} +
$ sudo find /etc/qo -type f -exec chmod 640 {} +
```

Start the Reseed Client Service

Lastly, we need to run the Reseed Client service and verify successful operations.

1. Start the service.

```
$ sudo systemctl start qo-hsm-reseed.service
```

2. Verify that the service has started.

```
user@ubuntu:~$ sudo systemctl status qo-hsm-reseed.service
● qo-hsm-reseed.service - Quantum Origin Hsm Reseed Service
     Loaded: loaded (/lib/systemd/system/qo-hsm-reseed.service; disabled; vendor
preset: enabled)
     Active: active (running) since Fri 2023-01-27 01:49:49 UTC; 4s ago
   Main PID: 119506 (qo_hsm_reseed_s)
      Tasks: 3 (limit: 915)
     Memory: 5.0M
     Cgroup: /system.slice/qo-hsm-reseed.service
             └─119506 /usr/bin/qo_hsm_reseed_service --
config=/etc/qo/reseed_service_config.yml

Jan 27 01:49:49 ubuntu qo_hsm_reseed_service[119506]: [2023-01-27 01:49:49.374]
[info] Starting service...
Jan 27 01:49:49 ubuntu qo_hsm_reseed_service[119506]: [2023-01-27 01:49:49.920]
[info] Reseed thread starting
Jan 27 01:49:49 ubuntu qo_hsm_reseed_service[119506]: [2023-01-27 01:49:49.923]
[info] Cache thread starting
```

3. Set the primary Reseed Client instances to start when the system boots.

```
$ sudo systemctl enable qo-hsm-reseed.service
Created symlink /etc/systemd/system/multi-user.target.wants/qo-hsm-
reseed.service → /lib/systemd/system/qo-hsm-reseed.service.
```

VERIFYING NORMAL OPERATIONS – RESEED CLIENT

The Reseed Client actively logs to the /var/log/syslog file. Under normal conditions the log file will be frequently populated with the following message:

```
[info] Slot ID {} successfully seeded
```

```
[info] Slot index {} successfully seeded
```

```
[info] Slot labelled '{}' successfully seeded
```

This indicates that the specified slot is receiving entropy and successfully using it to seed the onboard Pseudorandom Number Generator (PRNG). Any absence on this line of the configured slot signals an issue with that slot. The system is also configured to log errors so that a Security Information and Event Management system (SIEM) can be configured to look for the following entries in the log file.

VERIFYING NORMAL OPERATIONS – HSM AUDIT LOGS

Under normal operating conditions the HSM will be logging seeding events in its own audit log. Audit log setup and usage is documented by Thales in their online documentation here. The specific log message during healthy operation will be in the following format:

```
<Seq#>,<Timestamp>,S/N <Partition S/N> session 5 Access <Session ID> operation
LUNA_SEED_RANDOM returned RC_OK(0x00000000)
```

For example:

```
3097786,23/01/23 12:06:06,S/N 1377551558176 session 5 Access c16747dd8a0b57f1
operation LUNA_SEED_RANDOM returned RC_OK(0x00000000)
```

The Thales Luna HSM (v7) has a series of errors that can be thrown that are related to seeding events. The below logs are relevant for seeding events.

HSM Error	Hex Code	PKCS#11 or SFNT Def
LUNA_RET_RNG_ERROR	0x00300003	CKR_DEVICE_ERROR
LUNA_RET_NO_RNG_SEED	0x00200015	CKR_DATA_INVALID