Quantis Appliance

Integration Guide

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Part Number: 000-000000-001, Rev. A

Release Date: June 2015

Contents

Preface

In a world where the technological landscape is being revolutionized by quantum physics, ID Quantique (IDQ) and Gemalto have teamed up to help their customers to guarantee long-term security of their data through quantum technology.

IDQ develops and commercializes random number generators based on quantum physics, which are used in several industries including government, security, banking, gaming and IT/ Telecom, where they have become a reference. The ID Quantique's QRNGs are NIST SP800-22 compliant, they have been independently certified by the Swiss national laboratory (METAS) and have been validated according to AIS 31 criteria from the German BSI.

Gemalto is a world leader in providing best in class Hardware Security Modules (HSM). Gemalto HSMs provide the highest level of security by storing cryptographic keys in hardware. HSMs provide a secure crypto foundation as the keys never leave the intrusion-resistant, tamper-evident, FIPS-validated appliance.

Even though Gemalto's current key generation is among the best in the market, adding external true random numbers will improve the existing key generation mechanism and it will elevate its quality to the next level.

Quantis Appliance has been selected and special features were developed to feed external entropy into Gemalto's existing internal random number generator. Quantis Appliance is a network-attached device, which securely generates and delivers high-quality random numbers for security and cryptographic applications.

The Quantis Appliance is designed for environments, where high availability is necessary. It can be inserted in, or removed from, an operating network with no impact on any other appliance, such as servers, switches and Hardware Security Modules (HSMs).

Scope

This document will describe the methodology of feeding the entropy into Gemalto's SafeNet Luna Network HSM 7 using Quantis Appliance.

The document will focus on how to set up the Quantis Appliance and will later describe in details the necessary commands to configure the Quantis Appliance to be used as an external entropy feeder to Gemalto's SafeNet Luna Network HSM 7.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

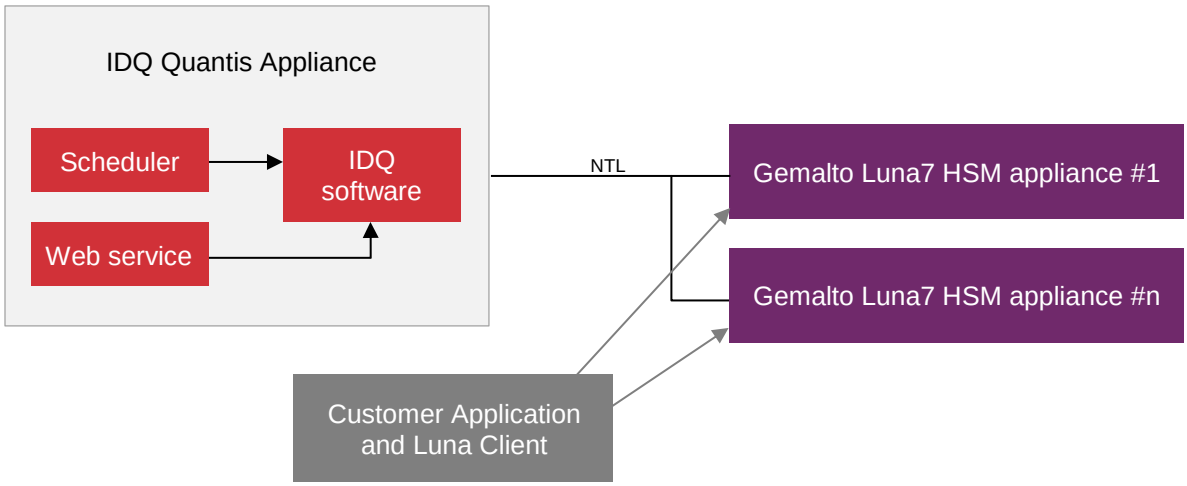
This chapter contains high level information to understand the integration of the Quantis Appliance with SafeNet Luna Network HSM 7.

Benefit

SafeNet Luna Network HSM 7 has an internal random generator which all cryptographic operations rely on. The entropy of the internal generator can be improved using an external quantum random generator. ID Quantique is the world leader in providing true random number generators. Quantis Appliance is a random number generator which has the ability to serve multiple applications simultaneously. It has also been designed to add external true randomness to the SafeNet Luna Network HSM 7 existing internal random number generator.

Overview

SafeNet Luna Network HSM 7 offers the abililty to provide an external seed through the PKCS11 interface of the Luna Client application. This client is installed in the Quantis Appliance.



The Quantis Appliance software offer 2 alternatives to provide randomness to the Luna client:

- **Automatic** reseeding can be done periodically using the Quantis Appliance scheduler.
- **On demand** reseeding can be done using a REST call to the web service.

Quantis Appliance Setup

This chapter contains information and steps to set up the IDQ Quantis Appliance to provide external seed for SafeNet Luna Network HSM 7.

Prerequisites

Before starting the installation, this document assumes:

- IDQ Quantis Appliance:
  - The quick start installation has been already done according to Quantis Appliance User Manual.
  - The Quantis Appliance is up and connected to the LAN.
  - The IP address is known.

- The Gemalto SafeNet Luna Network HSM 7:
  - The installation has been done according to Gemalto Configuration Guide document (document number 007-013576-002).
  - A dedicated partition is created and the credentials are known (name, password, slot and user type).
  - The system is up and connected to the LAN.
  - The IP address is known.
  - Administrator privileges in order to register the Quantis Appliance as client and assign it to a partition.

Configuration

Log in to the Quantis Appliance using the CLI:

```
qa login: cliUser
Password:
Last login: Fri Jul 21 16:48:18 on tty1
=====================================
*                                   *
*      ~~ Quantis Appliance CLI ~~     *
*                                   *
=====================================

Welcome to Quantis Appliance CLI
qa-cli>
```

Create the Network Trusted Link (NTL)

For all command related to the HSM refer to "*Create a Network Trust Link Between the Client and the Appliance*" section of the Configuration Guide document.

> **NOTE:** The following procedure (except the creation of the QA certificate) can be done for multiple HSMs or multiple partitions on the same HSM.

In this example we assume the next configuration:

- HSM IP address: 192.168.1.31
- Quantis Appliance IP address: 192.168.1.21

1. Retrieve the HSM certificate named *server.pem* through scp command.
2. Copy this certificate file to a USB memory drive.
3. Import the certificate on the Quantis Appliance and add the HSM in the server list.

```
qa-cli> ntl-hsm-cert-import --hsmCert=server.pem --hsmIp=192.168.1.31
Please insert media into USB port.
**** Press any key to continue ****
New server added to the list successfully
```

4. Create the QA certificate named *192.168.1.21.pem* and export it to a USB Memory drive

```
qa-cli> ntl-qa-cert-new
  New QA certificate created successfully for the NTL.
```

5. Optionally the certificate can be printed

```
qa-cli> ntl-qa-cert-show
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Ottawa, O=My company, CN=192.168.0.91
        Validity
            Not Before: Apr  5 14:08:38 2017 GMT
            Not After : Apr  4 14:08:38 2027 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=My company, CN=192.168.0.91
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d2:9e:1e:09:d4:6c:d4:96:32:0a:d0:7b:83:bc:
                    5c:8c:f6:67:89:8a:7d:37:84:df:22:f4:c4:d5:19:
                    08:ee:cc:98:8e:38:40:cf:8b:83:de:71:ca:45:1e:
                    b6:5b:96:1f:a4:f0:2a:21:c8:b4:10:b6:f2:d4:7f:
                    33:00:91:31:1e:2c:cf:31:7d:8b:d1:c9:5f:bd:e8:
                    85:7b:d1:4d:aa:d0:53:08:87:cd:3c:6b:be:b6:ec:
                    8b:28:36:cf:44:cd:c9:66:f5:7d:1c:3a:70:47:80:
                    fa:6c:97:d5:c6:35:fc:3b:e0:09:c8:55:fa:b9:cb:
                    21:51:8b:9b:90:dc:6c:8e:da:7a:57:d3:a5:4e:19:
                    21:ac:e7:c6:b4:83:5b:8b:d0:1c:28:25:c7:d2:d8:
                    85:f8:ef:bd:7f:15:e7:5e:9b:e6:e7:ab:6d:f6:20:
                    24:00:93:ff:27:3b:e2:04:01:bb:82:65:01:29:05:
                    0a:ec:00:c7:d3:93:4f:bf:93:40:3a:f2:e3:8d:0a:
                    00:d5:91:65:66:f3:72:6a:d0:ce:49:6e:b7:2b:81:
                    82:94:a0:38:c9:61:90:63:40:27:1c:c5:29:b8:94:
                    52:62:a8:0c:0f:ca:e3:79:4c:42:72:ae:18:e8:dc:
```

```
                    c9:b7:51:ad:bc:28:9c:cc:1c:a5:6d:ed:b2:2e:0e:
                    80:a9
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         b0:58:30:74:aa:15:52:a7:af:1f:91:83:27:a8:99:55:d3:27:
         42:3e:53:38:08:e6:60:2d:1f:be:32:b7:14:22:c2:25:e0:49:
         7b:46:3a:d5:ad:03:d8:6d:20:d4:43:58:97:47:1f:61:75:48:
         15:2a:9c:a1:7e:af:81:39:db:f1:73:ab:3c:ea:08:0e:be:10:
         2c:02:97:ad:f5:7f:96:a1:44:2c:d2:25:cb:b2:37:c6:3e:b0:
         cb:bb:a2:7f:bc:64:fa:f7:e4:09:7e:43:8a:f8:83:4c:a0:9b:
         4a:3b:ed:97:67:25:76:e2:96:e8:61:ce:fc:f1:b2:78:44:6b:
         f5:42:6f:b7:bb:8f:4a:00:d8:d2:78:59:bd:96:31:b1:d8:57:
         da:34:18:e7:96:9c:f6:7e:77:2d:f1:e7:9b:56:b6:b4:8e:fd:
         b0:09:89:3a:3e:4f:e3:fd:c4:90:5f:3f:78:86:7b:16:c3:2b:
         d3:b2:2c:31:a4:13:43:bd:f8:dd:ac:6d:bd:2e:ab:43:45:90:
         50:51:9a:a6:5b:15:68:90:12:09:aa:25:7c:3a:1e:0c:b7:10:
         d6:e2:78:5d:f2:94:c3:99:35:7c:c7:55:0c:45:6b:95:f6:70:
         7d:12:7b:9e:6e:72:91:9d:d0:e4:cc:ed:8e:38:e1:c8:e8:0d:
         5d:11:f5:de
```

```
qa-cli> ntl-qa-cert-export --name=192.168.1.21.pem
Please insert media into USB port.
**** Press any key to continue ****
Certificate saved successfully
```

6. Upload the QA certificate named *192.168.1.21.pem* in the HSM through a scp command.
7. Register the QA as a HSM client. For all command related to the HSM refer to "*Enable the Client to Access a Partition*" section of the configuration guide document.
8. Assign this client to a partition of the HSM.
9. Verify the NTL in the Quantis Appliance.

```
qa-cli> ntl-verify
The following SafeNet Luna Network HSM Slots/Partitions were found:
Slot    Serial #        Label
====    ========        =====
 1      65091001        MyPartition
```

NOTE: If the Quantis Appliance IP address or hostname are changed, this configuration must be done again.

Configure access to HSM partitions

On the Quantis Appliance type for each partition that you want to seed. The number of HSM may be limited by licensing.

```
qa-cli> hsm-conf-new --name=HSM1

  New HSM1 configuration created successfully.

qa-cli> hsm-conf-edit --name=HSM1 --partitionName=Partition1 --
partitionPwd=myPassword --slot=1 --userType=CKU_USER

  Configuration edited successfully.
```

```
qa-cli> hsm-conf-show --name=HSM1

  partitionName=Partition1

  partitionPwd=myPassword

  slot=1

  userType=CKU_USER
```

High Availability (HA) Mode

In HA Mode two configurations are possible:

- Configure each partitions of the HA group in the QA. In this case every HSM will have quantum entropy available at any time even if it is a passive one.
- Configure only the virtual slot of the HA group. In this case only the primary HSM will have quantum entropy.

Remark: the drawback of the second configuration is that for a short period of time (between 2 reseed) if the primary HSM change it will not have quantum entropy for the operations until the next automatic reseed. The drawback of the first configuration is that you have to configure all your HSM in the QA and some passive HSMs will be seeded too.

Reseed the HSM

The HSM can be reseeded automatically or on-demand. Each operation consists in feeding 256 random bits from the Quantis Appliance to the HSM.

- Automatic reseeding can be done periodically using the Quantis Appliance scheduler.
- On demand reseeding can be done using a REST call.

Configure automatic reseeding

The period can be defined as:

- 0 never, the scheduler is disabled, only on-demand reseeding.
- 1 to 9 minutes.

```
qa> hsm-conf-seed --period 1
  Seed period configured successfully.
```

On demand reseeding

Use the next REST call to reseed the HSM immediately.

```
https://QA-IpAddress/api/2.0/hsmseed?name=HSM1
```

Validate the reseeding

To check reseed of the HSM, retrieve the audit log of “HSM Management” type of the HSM.

More details to configure the Audit log can be found in the “*Configuring and Using Audit Logging*” section of the Configuration Guide document.

APPENDIX A

Quantis Appliance Command Line Interface Description

The command line interface allows configuring the Quantis Appliance.

Refer to the Quantis Appliance User Manual for general commands. This sections only describes the HSM related commands.

HSM Configure New

NAME **hsm-conf-new**

DESCRIPTION create a new HSM configuration.

ARGUMENT

--name	Define a name of the configuration

EXAMPLE

```
qa-cli> hsm-conf-new --name=HSM1
  New HSM1 configuration created successfully.
```

HSM Configure Edit

NAME **hsm-conf-edit**

DESCRIPTION Edit an HSM configuration.

ARGUMENT

--name	Specify the name of the configuration
--partitionName	Set the partition name as defined in the HSM
--partitionPwd	Set the partition password as defined in the HSM
--slot	Set the slot as return by the ntl-verify command
--userType	Define the type of user

EXAMPLE

```
qa-cli> hsm-conf-edit --name=HSM1 --partitionName=Partition1 --
partitionPwd=myPassword --slot=1 --userType=CKU_USER
  Configuration edited successfully.
```

HSM Configure New

NAME **hsm-conf-new**

DESCRIPTION create a new HSM configuration.

ARGUMENT

--name Specify the name of the configuration

EXAMPLE

```
qa-cli> hsm-conf-new --name=HSM1
  New HSM1 configuration created successfully.
```

HSM Configure Show

NAME **hsm-conf-show**

DESCRIPTION Display a HSM configuration.

ARGUMENT

--name Specify the name of the configuration

EXAMPLE

```
qa-cli> hsm-conf-show --name=HSM1
  partitionName=Partition1
  partitionPwd=myPassword
  slot=1
  userType=CKU_USER
```

HSM Configure Seed

NAME **hsm-conf-seed**

DESCRIPTION Define the period of time between 2 reseeding.

ARGUMENT

--period Define the period in minutes.

0: scheduler is disabled, only on-demand reseeding

1 to 9: time in minutes

EXAMPLE

```
qa> hsm-conf-seed --period 1
```

```
  Seed period configured successfully.
```

NTL HSM Certificate Import

NAME	**ntl-hsm-cert-import**
DESCRIPTION	Import a NTL HSM certificate in the Quantis Appliance from a USB Memory drive.
ARGUMENT	
--hsmCert	Set the filename of the certificate of a configured HSM
--hsmIp	Specify the IP address of an HSM to set the certificate

EXAMPLE

```
qa-cli> ntl-hsm-cert-import --hsmCert=server.pem --hsmIp=192.168.1.31
Please insert media into USB port.
**** Press any key to continue ****
New server added to the list successfully
```

NTL QA Certificate New

NAME	**ntl-qa-cert-new**
DESCRIPTION	Create a new Quantis Appliance certificate for the NTL.

EXAMPLE

```
qa-cli> ntl-qa-cert-new
  New QA certificate created successfully for the NTL.
```

NTL QA Certificate Show

NAME	**ntl-qa-cert-show**
DESCRIPTION	Display the Quantis Appliance certificate for the NTL.

EXAMPLE

```
qa-cli> ntl-qa-cert-show
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
```

```
Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=CA, ST=Ontario, L=Ottawa, O=My company, CN=192.168.0.91
    Validity
        Not Before: Apr  5 14:08:38 2017 GMT
        Not After : Apr  4 14:08:38 2027 GMT
    Subject: C=CA, ST=Ontario, L=Ottawa, O=My company, CN=192.168.0.91
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:d2:9e:1e:09:d4:6c:d4:96:32:0a:d0:7b:83:bc:
                5c:8c:f6:67:89:8a:7d:37:84:df:22:f4:c4:d5:19:
                08:ee:cc:98:8e:38:40:cf:8b:83:de:71:ca:45:1e:
                b6:5b:96:1f:a4:f0:2a:21:c8:b4:10:b6:f2:d4:7f:
                33:00:91:31:1e:2c:cf:31:7d:8b:d1:c9:5f:bd:e8:
                85:7b:d1:4d:aa:d0:53:08:87:cd:3c:6b:be:b6:ec:
                8b:28:36:cf:44:cd:c9:66:f5:7d:1c:3a:70:47:80:
                fa:6c:97:d5:c6:35:fc:3b:e0:09:c8:55:fa:b9:cb:
                21:51:8b:9b:90:dc:6c:8e:da:7a:57:d3:a5:4e:19:
                21:ac:e7:c6:b4:83:5b:8b:d0:1c:28:25:c7:d2:d8:
                85:f8:ef:bd:7f:15:e7:5e:9b:e6:e7:ab:6d:f6:20:
                24:00:93:ff:27:3b:e2:04:01:bb:82:65:01:29:05:
                0a:ec:00:c7:d3:93:4f:bf:93:40:3a:f2:e3:8d:0a:
                00:d5:91:65:66:f3:72:6a:d0:ce:49:6e:b7:2b:81:
                82:94:a0:38:c9:61:90:63:40:27:1c:c5:29:b8:94:
                52:62:a8:0c:0f:ca:e3:79:4c:42:72:ae:18:e8:dc:
                c9:b7:51:ad:bc:28:9c:cc:1c:a5:6d:ed:b2:2e:0e:
                80:a9
            Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
     b0:58:30:74:aa:15:52:a7:af:1f:91:83:27:a8:99:55:d3:27:
     42:3e:53:38:08:e6:60:2d:1f:be:32:b7:14:22:c2:25:e0:49:
     7b:46:3a:d5:ad:03:d8:6d:20:d4:43:58:97:47:1f:61:75:48:
     15:2a:9c:a1:7e:af:81:39:db:f1:73:ab:3c:ea:08:0e:be:10:
     2c:02:97:ad:f5:7f:96:a1:44:2c:d2:25:cb:b2:37:c6:3e:b0:
```

```
cb:bb:a2:7f:bc:64:fa:f7:e4:09:7e:43:8a:f8:83:4c:a0:9b:
4a:3b:ed:97:67:25:76:e2:96:e8:61:ce:fc:f1:b2:78:44:6b:
f5:42:6f:b7:bb:8f:4a:00:d8:d2:78:59:bd:96:31:b1:d8:57:
da:34:18:e7:96:9c:f6:7e:77:2d:f1:e7:9b:56:b6:b4:8e:fd:
b0:09:89:3a:3e:4f:e3:fd:c4:90:5f:3f:78:86:7b:16:c3:2b:
d3:b2:2c:31:a4:13:43:bd:f8:dd:ac:6d:bd:2e:ab:43:45:90:
50:51:9a:a6:5b:15:68:90:12:09:aa:25:7c:3a:1e:0c:b7:10:
d6:e2:78:5d:f2:94:c3:99:35:7c:c7:55:0c:45:6b:95:f6:70:
7d:12:7b:9e:6e:72:91:9d:d0:e4:cc:ed:8e:38:e1:c8:e8:0d:
5d:11:f5:de
```

NTL QA Certificate Export

NAME	**ntl-qa-cert-export**
DESCRIPTION	Export a NTL Quantis Appliance certificate to a USB Memory drive.
ARGUMENT	
--name	Set the filename of the NTL certificate

EXAMPLE

```
qa-cli> ntl-qa-cert-export --name=192.168.1.21.pem
Please insert media into USB port.
**** Press any key to continue ****
Certificate saved successfully
```