Quside

INTEGRATION GUIDE

Quside PCIe Daemon - Luna HSM

CONTENTS

REVISION HISTORY

Date	Version	Description
17/VI/2024	1.0.0	Initial version

1. Overview

Quside's PCIe Daemon (QPD) guarantees the maximum levels of foundational security for your Thales' Luna HSM Devices. QPD allows for a continuous provision of high-quality, continuously monitored quantum entropy to your HSM devices, always guaranteeing the presence of fresh entropy in your devices and, therefore, enabling the generation of quantum-seeded cryptographic keys within the HSM domain with the guarantee of not experiencing entropy starvation. This allows for quantum seeding of both current and Post Quantum Secure Algorithms provided with the Thales PQC Functional Module.
QPD is a driver for Quside Hardware devices that installs into the Linux machine hosting the Thales PCIe HSM device in the customer environment. It provides tightly bound and frequent reseeding to the Thales Luna HSM with quantum entropy. Luna HSM provides strong physical protection of secure assets, including keys, and should be considered a best practice for managing sensitive data. The combination of QPD and Luna HSM generates robust and mathematically proven keys for the encryption process.

2. Certified Platforms

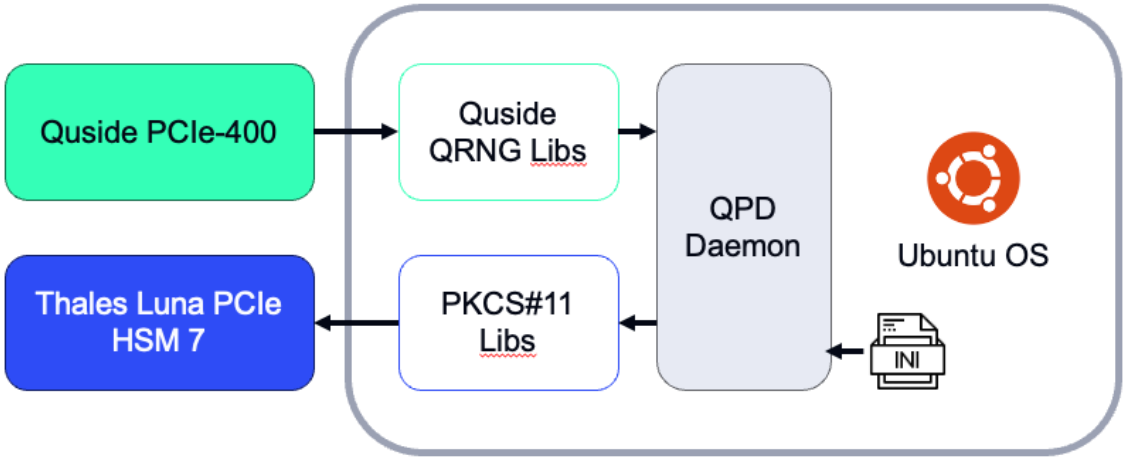
This integration is certified on the following platforms (minimum platform requirement listed):

HSM Type	Platforms Certified
Luna HSM 7	Quside PCIe Daemon (QPD)
LunaCM 10.7.0	Quside PCIe Daemon (QPD)

Luna HSM: Luna HSM devices are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. In this document, Luna HSM refers to the Luna PCIe HSM 7.

3. Solution Diagram

The following diagram illustrates a system architecture that integrates a Quside's QRNG device with a Thales® Luna™ PCIe HSM 7 on an Ubuntu 18 operating system.



The Quside PCIe-400 connects to the system through its Quside QRNG libraries. Simultaneously, the Thales Luna PCIe HSM 7 interfaces with the system using PKCS#11 libraries. The QPD Daemon manages the integration and operation of the QRNG with the HSM.

The system runs on the Ubuntu 18 OS, with configuration settings provided via an INI file used by the QPD Daemon for initialization and operational parameters.

4. Prerequisites

Before you proceed with any of the integrations described in this document, complete the following tasks:

Install the Quside Device

Please follow the instructions provided with your Quside PCIe device to install the card and verify its functionality. If any issues arise, please contact support@quside.odoo.com.

Configure Luna HSM

To configure Luna HSM:

1. Verify that the HSM is set up, initialized, provisioned, and ready for deployment.
2. Get a list of all partitions on the HSM that will be later used by the Quside PCIe Daemon (QPD), including one partition that is designated for use by QPD,
3. Initialize the Crypto Officer and Crypto User roles for the registered partition.

Note: Refer to Luna HSM documentation for detailed steps on initializing the partitions and assigning various user roles.

5. Installing Quside PCIe Daemon (QPD) on Linux

This document will go through the QPD install process for Linux. The Linux QPD automatically operates the extractor to feed entropy into the Luna HSM at a fixed interval. This allows HSM Luna to use quantum entropy to generate strong quantum-derived keys.

Installation

> Note: During this installation process, the reseed service is started automatically so that reseeding begins as soon as possible. To facilitate this, it is recommended that the required configuration file is placed at `/etc/quside/quside_luna_provider/config.ini` beforehand. If the configuration file is installed later, it will be necessary to restart the service with `sudo systemctl restart quside_luna_provider.service`.

The Linux kernel reseed client can be installed via the Debian package (DEB) with their install commands, e.g.:

```
sudo apt install quside-luna-provider
```

When installed, it does the following:

1. Installs a binary, `/usr/bin/quside_luna_provider_service`, which performs the reseeding.
2. Creates a sample file `/etc/quside/quside_luna_provider/config.ini`.
3. Creates a service called `quside_luna_provider.service`, which will run the QPD using the config file at `/etc/quside/quside_luna_provider/config.ini`. This file is required to operate the QPD.

Operation

When the service starts, it loads the configuration file and tests connectivity with the HSM device. Then, it rests for the configured period before waking up and reseeding the selected partition on the HSM at the specified reseed interval, as specified in the configuration file.

The service can be manually started by running:

```
sudo systemctl start quside_luna_provider.service
```

If this reseeding fails (for example, because Quside's PCIe is not calibrated yet), the service will log a critical error and exit. Please note that the service may be restarted multiple times according to your system configuration.

Reseed Configuration

The service requires a configuration file, `config.ini`, placed in the folder `/etc/quside/quside_luna_provider`.

```
# Amount of random numbers to seed at each interval
nRandomNumbers = 10240

# Interval between reseeds in seconds
sleepTime = 15

# Path to the PKCS#11 library
libraryPath = /usr/lib/libCryptoki2.so

# Slot number
slot = 3

# Password for the HSM
password = <ENTER PASSWORD>
```

Note that the service parses the configuration file only when it is started. If the configuration is modified, the service will need to be restarted with

```
sudo systemctl restart quside_luna_provider.service
```

Uninstallation

The service may be uninstalled by using the following commands:

```
sudo apt remove quside-luna-provider
```

Note that the configuration files will not be automatically removed. These may be removed manually if desired.

6. Quside User Support

If you require additional support or encounter technical issues, please contact Quside at support@quside.odoo.com. One of our customer support representatives will respond to your request as soon as possible.

Additional support documents for Quside's PCIe Device can also be requested from Quside at the same support address: support@quside.odoo.com.

www.quside.com