nShield Post-Quantum Software Development Kit

# PQSDK v1.1.0 Release Notes

10 April 2024

# Table of Contents

# 1. Introduction

These release notes apply to version 1.1.0 of the nShield Post-Quantum Software Development Kit (PQSDK). They contain information specific to this release such as new features, defect fixes, and known issues.

The Release Notes may be updated with issues that have become known after this release has been made available. Please check https://nshieldsupport.entrust.com/hc/en-us/sections/360001115837-Release-Notes for the latest version of this document.

Access to the Support Portal is available to customers under maintenance. Please contact Entrust nShield Technical Support at nshield.support@entrust.com to request an account.

# 2. Purpose of this release

The nShield Post-Quantum Cryptography (PQC) Software Development Kit provides an early look at quantum-resistant public-key cryptographic algorithms under consideration by NIST as part of the Post-Quantum Cryptography standardisation process.

The nShield Post-Quantum Software Development Kit contains the source code for a CodeSafe SEE machine enabling your nShield HSM to generate and use keys with post-quantum algorithms, as well as example Java code demonstrating how to interface with the SEE machine.

There are two main use-cases for using the CodeSafe PQSDK, which are:

- The 'PQC algorithm evaluator' is a CodeSafe developer (i.e. they are a 'Local Client'), who has the CodeSafe SDK and will be building a loadable PQSDK CodeSafe SEE machine onto their local HSM.
- The 'PQC algorithm evaluator' is not a CodeSafe developer (i.e. they are a 'Remote Client'), and will make a remote connection to an HSM (which has a working PQSDK CodeSafe SEE machine). Entrust (or another provider) takes the role of the Local Client (Admin), that is offering the 'PQSDK service' and managing the HSM.

The PQSDK provides the user with the opportunity to experiment with the use of PQC digital signature algorithms and signatures but at this moment the underlying Security World protection mechanisms still use classical (non Post-Quantum) crypto. It should not be used in an environment where a full post-quantum resistance security solution is required.

# 3. Features of nShield Post-Quantum Software Development Kit v1.1.0

The nShield Post-Quantum Software Development Kit is a source release, enabling modification and experimentation by the end user.

The nShield Post-Quantum Software Development Kit provides support for several candidates from the NIST Post-Quantum Cryptography standardisation process, including digital signature schemes (CRYSTALS-Dilithium, Falcon, SPHINCS+) and key encapsulation mechanisms (CRYSTALS-Kyber). See *Supported Post Quantum Algorithms* in the *PQSDK User Guide* for more information.

This release provides the following new features:

- nShield 5 support
- KEM support
- Installation changes to support new HSMs and client/developer split
- Key Import

# 4. Compatibility

## 4.1. Supported hardware

This release is targeted at deployments with any combination of the following nShield HSMs:

- nShield Solo XC (Base, Mid, High)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield 5s (Base, Mid, High)
- nShield 5c (Base, Mid, High)

## 4.2. Supported operating systems

This release has been tested for compatibility with the following operating systems:

- Red Hat Enterprise Linux 8 x64
- Additional mainstream x64 based Linux distributions other than the one listed above may be compatible, however Entrust cannot guarantee this compatibility.

## 4.3. Supported Security World Versions

The following tables show the supported configuration of firmware and software installations.

### 4.3.1. nShield Solo

| HSM Type | Firmware Version | Security World Version | CodeSafe Version |
|---|---|---|---|
| nShield 5s | v13.4.3 | v13.4.3 | v13.4.3 |
| nShield Solo XC | v12.72.1 | v12.70.4 | v12.70.4 |
| nShield Solo XC | v12.72.1 | v13.4.3 | v13.4.3 |

### 4.3.2. nShield Connect

| HSM Type | Image Version | Firmware Version | Security World Version | CodeSafe Version |
|---|---|---|---|---|
| nShield 5c | v13.4.3 | v13.4.3 | v13.4.3 | v13.4.3 |
| nShield Connect XC | v12.80.5 | v12.72.1 | v12.70.4 | v12.70.4 |
| nShield Connect XC | v12.80.5 | v12.72.1 | v13.4.3 | v13.4.3 |

Other combinations of Firmware, Security World software, and CodeSafe software may work but are not supported at this time.

# 5. Required licenses

Please use the Feature Enable Tool (FET) to set and view enabled features.

## 5.1. nShield XC

The Unrestricted SEE (`SEE Activation (EU+10)`) feature must be enabled on your HSM. Restricted SEE (`SEE Activation (Restricted)`) is not currently supported.

## 5.2. nShield 5

The SEE Activation, CodeSafe 5 (`SEE Activation, CodeSafe 5`) feature must be enabled on your HSM.

For more information, please refer to the latest nShield Security World documentation.