nShield Security World Release Information

nShield Licensing

21 January 2026

Table of Contents

This section defines the licensing model and permitted uses for the Entrust nShield hardware security modules (each an "HSM") and the HSM-related software ("HSM Software").

1. Permitted use

In this Licensing section, the term "Customer" means an Entrust customer who has purchased one or more HSMs, or an individual authorized by Customer to access components or features of the HSM or HSM Software ("Users").

HSMs and HSM Software are sold or licensed for internal Customer use (i.e. use for the Customer’s own business purposes). Customer may also grant access to Users who are employees of external contractors, but only to the extent that such Users are using HSMs and HSM Software on the Customer’s behalf in the operation or management of the Customer’s business.

Except as may be otherwise specified in an express license agreement signed by Entrust, neither Customer nor any User may use HSMs or HSM Software to set up or provide its own managed service for other companies (e.g. provision of HSM and HSM Software functionality as a "Managed Service Provider" or "Systems Integrator").

2. nShield HSMs

In the context of the HSMs, Customer will make certain choices as set out below:

1. Hardware model
2. Performance level/tier
3. Certification
4. Features
5. Add-ons and extras

2.1. Hardware model

1. **nShield Solo XC and nShield 5s (PCI-Express HSMs)** - nShield Solo XC and nShield 5s refer to the family of nShield PCI-Express (sometimes written as PCIe) form factors which are installed in a host computer/server. When ordering a PCIe variant of nShield, packaging will contain the desired hardware module, smartcard reader, additional accessories and essential documentation.
2. **nShield Connect XC, nShield 5c, and nShield 5c 10G** - nShield Connect and nShield 5c HSMs are stand-alone, network-attached devices that support one or more connected clients. The nShield 5c 10G is the nShield 5c variant offering 10G copper/fiber. There is an nShield 5c for 5G variant as part of a special bundle that includes the HSM + a number of accessories for 5G network deployments (smartcards, railkits, Remote Admin kit, SW and option packs). All nShield network appliance HSMs include: a card reader, 3 x Client licenses are by default, no Operator Cards are deployed by default with HSM. Separate smart card packs SKUs can be ordered separately.
3. **nShield Edge** - a physically secure, tamper resistant security device with integrated smart card reader that provides cryptographic functions for purposes such as Offline Public Key Infrastructure certificate authorities. It is attached to a host computer via USB.

2.2. Performance level/tier

Base/Mid/High - Customer selects the processing speed they would like for the HSM they have chosen. nShield datasheets providing the baseline transactional speed for most common algorithms (e.g.: RSA 4096, ECC 512, etc.)

Speed upgrades/Performance upgrades

Customer has the flexibility to upgrade the performance level of their HSM (Base/Mid) as an additional license (physical or electronic).

2.3. Certification

Customers may also select HSMs (or the related firmware) that are certified compliant with certain regimes as follows:

Common Criteria eIDAS

Compliance regime against which certain HSM firmware needs to be certified to fulfil the requirements of some use cases (e.g., remote signature). Note all Common Criteria orders ship from the United Kingdom with Tamper Evident Packaging.

FIPS 140

Organizations use the FIPS 140 standard to ensure that the hardware they select meets specific security requirements. The FIPS certification standard defines four increasing, qualitative levels of security:

Level 1 Requires production-grade equipment and externally tested algorithms.

Level 2 Adds requirements for physical tamper-evidence and role-based authentication. Software implementations must run on an Operating System approved to Common Criteria at EAL2.

Level 3 Adds requirements for physical tamper-resistance and identity-based authentication. There must also be physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module. Private keys can only enter or leave in encrypted form.

Level 4 This level makes the physical security requirements more stringent, requiring the ability to be tamper-active, erasing the contents of the device if it detects various forms of environmental attack.

The FIPS 140 standard technically allows for software-only implementations at level 3 or 4 but applies such stringent requirements that very few have been validated. For many organizations, requiring FIPS certification at FIPS 140 level 3 is a good compromise between effective security, operational convenience, and choice in the marketplace.

2.4. Features

Client licenses refer to the licensing system to control the number of application hosts that can consume an HSM in its network appliance form factor (nShield 5c, nShield 5c 10G or nShield Connect XC).

Network appliance HSMs include a default total of 3 client licenses allowing a maximum of 3 concurrent client connections. Additional client licenses are available for purchase to increase this limit. Licenses are applied to an individual HSM.

Note - Client licenses are perpetual HSM feature activations. The maximum amount that can be added to a single HSM is capped based on performance tier (B/M/H). Please refer to the product notes for more information.

License transfer fees - Licenses are typically linked to the serial of an HSM. These can be transferred from one unit to another under an appropriate license (and subject to the license transfer fee).

Additional soft client licenses - a default three (3) client licenses are provided at no extra cost. Additional client licenses are at an additional cost.

Enterprise Client license - In case the number of extra clients required is considerable (typi cally over 30) an enterprise license is available at a higher price to allow max number of clients permitted.

Enterprise Client license transfer fees - Licenses are typically linked to the serial of an HSM. These can be transferred from one unit to another under an appropriate license (and subject to the license transfer fee).

nShield Edge Developer Edition - for the nShield Edge only and refers to the lower cost of a unit sold for **development purposes only**. HSMs are to be used only for non-production use in support of development or engineering activities in support of development of applications or systems that will interact with the HSMs (in addition to this restriction, the standard terms and conditions, including restrictions, continue to apply).

Serialized tamper evident packaging - required for Common Criteria eIDAS certification (and some customers require it based on their own security requirements).

nShield Feature Activation - activates a specific function that is disabled on the HSM by default. e.g.: PQ algorithms for XC, CodeSafe, Elliptic curves etc…

- ISO S/Card Support Feature Activation
- Remote Operator Feature Activation (Per Unattended HSM)
- Korean Certificate-based Digital Signature Algorithm (KCDSA) Feature Activation
- Elliptic Curve Cryptography (ECC) Feature Activation
- Elliptic Curve Digital Signature Algorithm (ECDSA RNG) Feature Activation
- Post Quantum Activation

- CodeSafe Unrestricted Activation vs Restricted Activation vs Activation
- Unrestricted Activation feature allows the HSM to load and run a self-signed CodeSafe machine.
- Restricted Activation feature allows the HSM to load and run a CodeSafe machine that has been signed by an Entrust-trusted developer using the CodeSafe SDK).

Transferred Licenses - free transfer of licenses are only provided from end of support (EOS) HSMs to new HSMs, as long as Customer has an active support contract in place for the non-EOS new HSMs.

2.5. Add-ons and extras

The following items are subject to additional charge unless specifically included in a package:

- Additional client licenses and client activations
- Sub-assembly for remote admin kit (TVD/SW + instructions)
- nShield Remote Administration Kit includes:
  - Remote Administration Cards - custom smart cards equipped with a nShield applet
  - Trusted Verification Devices (TVDs)- nShield smart card readers used with Remote Administration Cards to create secure connection with the target HSM
  - Remote Administration Client (RAC) software - GIU tool running on client laptop or workstation to configure connection to HSM
- Optional Software Licenses/Option packs (see HSM Software section below for details)
- Professional Services
- Support Services
- nShield Accessories (replacement fans, spare fan trays, replacement PSU, keyboard, quick fit rack mounting kit, replacement battery, slide rail kits)
- Rack mounting rails (included with nShield 5c 10G, but otherwise extra)
- Any other nShield HSM parts and accessories

3. HSM software

5. Selection between electronic fulfillment (ISO) vs physical DVD for SW files vs smart-cards in the case of feature or speed license upgrades

3.1. Firmware and nShield Connect image

The nShield firmware and nShield Connect image is preloaded in the HSM (and will depend on hardware selection and proposed configurations). nShield Firmware & nShield Connect Image (ISO) contains the supported firmware and Connect images which allows for updating the HSM to later versions.

3.2. HSM-related software

- nShield Security World Software - client software required for managing and using the nShield HSM. Also contains the SDK to development software to use with the HSM libraries.
- KeySafe 5 - provides a centralized means to securely manage and monitor a distributed nShield HSM estate, including the creation and management of Security Worlds and associated resources (Softcards and Card Sets). The monitoring capability of KeySafe 5 is provided under an annual subscription license that is subject to an additional cost and requires a separate activation license.
- CodeSafe 5 (or earlier version CodeSafe) – a runtime environment on the HSM. Included in all HSMs.
- CodeSafe 5 (or earlier version CodeSafe) SDK is the toolkit to create and sign a CodeSafe Application. In order for a CodeSafe Application to be installed on an HSM, that HSM needs to have had an activation license (perpetual) installed (which is subject to an additional cost).

4. SDKs and APIs

- **CodeSafe** and **CodeSafe 5** - a runtime on the HSM
- **CodeSafe SDK** and **CodeSafe 5 SDK** - the toolkit to create and sign a CodeSafe machine (used to write a CodeSafe app).

This is the license to allow that signed CodeSafe machine to be executed by a specific HSM. It is linked to the serial of the unit.

4.1. Option packs

- **CIOP (Cloud Integration Option Pack)** - Integrates nShield HSMs with cloud services, allowing secure generation, storage, and management of keys used in sensitive cloud-hosted applications.
- **nCOP (Container Option Pack)** - Enables containerized environments with high assurance (FIPS/CC) HSMs.
- **nDSOP (Database Security Option Pack)** - Integration with Microsoft SQL Server using Microsoft's Extensible Key Management (EKM) API.
- **Web Services Option Pack** - Cloud-friendly, REST-like interface for high assurance nShield HSMs.
- **WS SQLEKM** - Integrates with SQL encryption key management to provides data-at-rest encryption for sensitive information held by Microsoft SQL Server.
- **nShield Post Quantum Option Pack (PQSDK - Post-Quantum Software Developer Kit)** - Leverages Entrust CodeSafe SDK and the `liboqs` open source library to provide quantum-resistant cryptographic algorithms to customers.

Transfer Entitlement for Option Packs - Customer may transfer their Option Packs from one HSM to another subject to a transfer fee.

5. Support services

Standard/Premium/Premium Plus

UK customers only - additional options:

- Premium Support with Office Hour onsite Replacement
- Premium Plus Support with Office Hour onsite Replacement
- Premium Plus Support + 24x7 On-site Replacement

Key Attestation Verifier - contact your account representative for more information on obtaining this software as there is a non-standard process involved.

6. Trade compliance

The HSMs and HSM Software contain cryptographic components which are subject to U.S. and U.K. export restrictions. Import and export rules in your jurisdiction may also apply.