nShield Security World

nShield Security World v13.6.12 Security Manual

22 August 2025

Table of Contents

1. Introduction

Good security practice requires procedural as well as technical measures to provide a comprehensive security environment for the protection of your cryptographic keys and data.

This guide provides advice to you on the secure operation of the product. It identifies procedural measures that should be deployed to support the secure operation of the nShield. The guidance should be used in the development of your Security Operating Procedures for your systems incorporating the nShield.

1.1. Who should read this document?

The guide should be used by the following people:

- Those responsible for the security policy and procedures for your systems incorporating the nShield
- Those responsible for commissioning the nShield
- Those responsible for administering the nShield
- Those responsible for auditing the nShield.

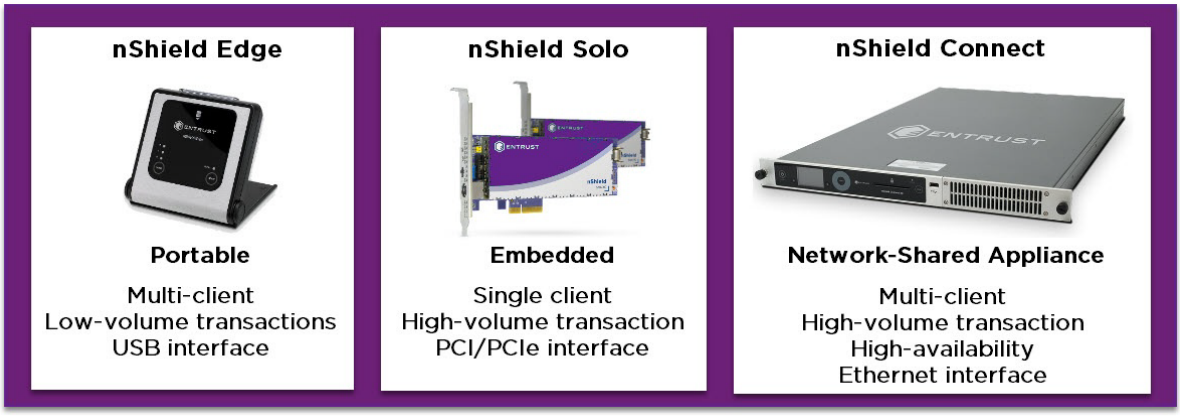
1.2. Products covered by this manual

- nShield Edge
- nShield Solo+
- nShield Solo XC
- nShield 5s
- nShield Connect+
- nShield Connect XC
- nShield 5c

1.3. Product security objective

The nShield range of products provide protection against technical and physical attacks on keys used to protect your data in use, in motion and at rest. This provides confidentiality, integrity and availability* of user data up to FIPS 140 Level 3 and Common Criteria version 3.1 revision 5 EAL 4+ (platform and version dependent) when deployed in accordance with the technical and procedural controls identified in the HSM and Security World product documentation and here in the *Security Manual*.

*Some availability threats can be mitigated by hosting a Security World across multiple Hardware Security Modules (HSMs).



1.4. Product selection

As part of the security product selection process, you must determine that the functionality delivered by any candidate product meets your requirements.

In this manual the terms module and HSM are both used to generically describe the nShield range of products.

1.5. Security manual authority and scope

The guide is advisory and its scope is limited to identifying good procedural practices for the secure operation of the product within your environment.

If there is any contradiction between the guidance that occurs in this manual and that found in the HSM and Security World product documentation, then the guidance found here takes precedence.

The scope of this manual is limited to security procedural guidance. The HSM and Security World product documentation provide guidance on how to implement the controls discussed in this Manual.

1.6. Related documents

- nShield v13.6.12 Hardware Install and Setup Guides
- nShield v13.6.12 HSM User Guide
- nShield Security World Software v13.6.12 Installation Guide

- nShield Security World v13.6.12 Management Guide
- nShield v13.6.12 Utilities Reference
- nShield Security World v13.6.12 Key Management Guide
- CodeSafe 5 v13.6.12 Developer Guide
- CodeSafe v13.6.12 Developer Guide
- keysafe5:intro.pdf
- *nShield Connect Physical Security Checklist*

1.7. Reference documents

- Ecrypt-CSA recommendations
- NIST SP 800-57 Part 1 Revision 5
- NIST SP800-131A Revision 1
- Net-SNMP
- NTP Vulnerabilities.

2. Supply and Transportation

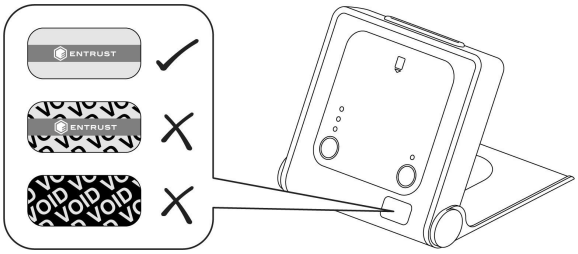
2.1. Trusted delivery

To help assure the integrity of the product during delivery a trusted courier service should be used that provides traceable delivery progress reporting and requires signed acceptance of delivery. Inspect the packaging for signs of tampering, for example, packing tape appears to have been removed or cut and then resealed. If tamper is detected, quarantine the package and notify your Security Officer in line with your Security Incident and Response procedures. Similar methods must be deployed by you for any further transportation of the product during its lifetime. If you utilize a protective marking scheme, the relevant protective marking must be deployed during transportation to provide the required level of integrity.

2.2. Tamper inspection

Upon receipt of the nShield HSM, it must be inspected for signs of tamper:

- nShield Edge: Inspect the USB cable and the nShield Edge before use. The inspection should cover the cable for signs of tampering, the fascia for signs of disfigurement and specifically the holographic tamper label in the tamper window shown below for the appearance of **VOID**.



The nShield Edge Developer Edition does not have a hologram and tamper window.

- nShield Solo: Examine the epoxy resin security coating (after removing the metal lid on nShield Solo XC) of the module for obvious signs of damage.
- Smart card reader: Examine the smartcard reader for signs of tamper and ensure it is directly plugged into the module or into the port provided by any appliance in which the module is integrated and the cable has not been tampered with.
- nShield Connect: The *nShield Connect Physical Security Checklist*, provided in the box with an nShield Connect and available in the document folder on the installation media provides details of the physical security checks required. Further guidance on physical

security checks can be found in [security-manual:physical-security]. Review the nShield Connect's tamper log for tamper alerts.

- See [security-manual:physical-security] for further guidance on the management of physical mechanisms provided to protect the product.

If a tamper is suspected then the unit must be quarantined to investigate the incident. The unit must not be deployed on the live system until its integrity can be verified. See the [security-manual:security-incident] for further guidance.

3. Environment

3.1. HSM function and architecture

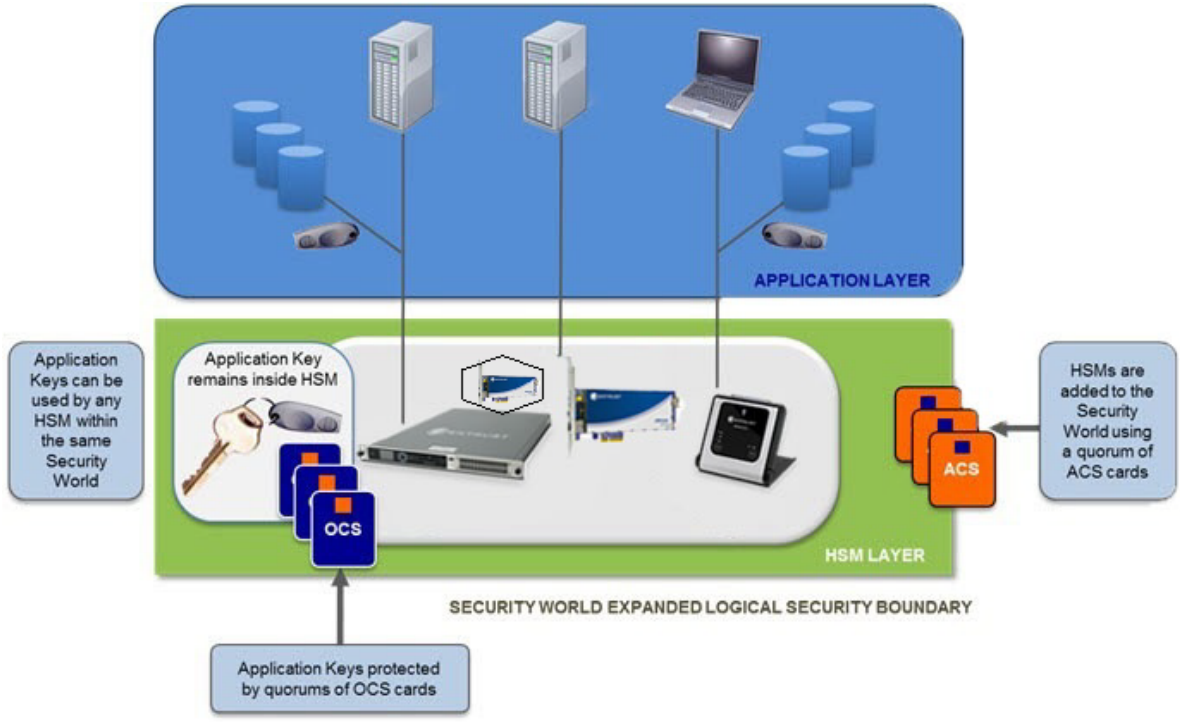
The nShield HSMs perform encryption, digital signing and key management on behalf of an extensive range of commercial and custom-built applications including Public Key Infrastructures (PKIs), identity management systems, application-level encryption and tokenization, SSL/TLS, and code signing.

nShield HSMs provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection and key, data and application encryption. They are available in three form factors to support a variety of deployment scenarios:

1. nShield Solo and 5s local FIPS 140 certified PCIe cards
2. nShield Connect and 5c network-attached appliances, that contain the nShield Solo or 5s FIPS 140 certified PCIe card along with surrounding networking and administration support facilities
3. nShield Edge FIPS 140 certified USB device

All nShield HSMs integrate with the nShield Security World architecture. This supports combinations of different nShield HSM models to build a unified ecosystem that delivers scalability, seamless failover and load balancing. The nShield Security World architecture supports a specialized key management framework that spans the nShield HSM range.

nShield HSMs all define the physical FIPS-certified security boundary or HSM Layer within which Application Keys, Control Keys and Infrastructure Keys are protected. Using quorums of Administrator Card Set (ACS) cards, Infrastructure Keys can be securely backed up and shared across multiple HSMs. When this is performed, HSMs that share the same Infrastructure Keys develop a common Security World that provides an expanded logical security boundary that extends beyond the physical HSM Layer and overlaps into the enterprise IT environment or Application Layer. The abstraction of Application Keys into Application Key Tokens enables these tokens to be stored outside the physical HSM and within the corporate IT environment.



The Security World technology makes sure that keys remain secure throughout their life cycle. Every key in the Security World is always protected by another key, even during recovery and replacement operations. Because the Security World is built around nShield key-management modules, keys are only ever available in plain text on secure hardware.

nShield Connect and nShield Solo HSMs also provide a secure environment for running sen sitive applications. The CodeSafe option lets you execute code within nShield boundaries, protecting your applications and the data they process. The CodeSafe area occurs outside of the module area that is FIPS 140 Level 2 and 3 approved.

The nShield HSM is used to protect sensitive keys, data and optionally applications. It can only operate securely if its environment provides the procedural security that it requires and if its security enforcing functions are utilized appropriately.

When configured correctly the nShield HSM provides encryption, digital signing and key management services in support of confidentiality and integrity requirements for your data. The nShield HSM is not designed to be completely resistant to denial of service attacks - these can be addressed by other aspects of the system design if warranted by the threat and impact assessments.

3.2. HSM environment controls

You must exercise due diligence to ensure that the environment within which the nShield HSMs are deployed is configured properly and is regularly examined as part of a comprehen

sive risk mitigation program to assess both logical and physical threats. The client's application and its environment must be protected from malware as they access the HSMs cryptographic services. Adequate logical and physical controls should be in place to ensure that malware is detected.

Your Security Procedures should identify the measures required to ensure the physical security (and counter any threats of theft or attack) of the nShield HSM, and associated host/client/Remote File System (RFS)/KeySafe 5 platforms, backup data, Security Information and Event Management (SIEM) collectors and card readers. Access to the nShield HSM, and associated host/client/RFS/KeySafe 5 platforms, backup data, SIEM collectors and card readers secure areas must: