nShield Key Attestation

nShield Key Attestation Verifier v1.0.2 Release Notes

30 January 2024

Table of Contents

1. Introduction

These release notes apply to version 1.0.2 of the nShield Key Attestation Verifier for Security World software. They contain information specific to this release, such as new features, defect fixes, and known issues.

This document will be updated if new issues become known after this release has been made available. Check https://nshieldsupport.entrust.com/hc/en-us/sections/360001115837-Release-Notes for the most up to date version of this document.

1.1. Purpose of this release

The new nShield Key Attestation Verifier (`nfkmattest`), provides a way for you to verify JSON bundles that contain the certificates and information about an nShield key and nShield HSM even if you do not have access to nShield HSMs. When the nShield Key Attestation Verifier is installed with the nShield Security World software and it has access to an nShield HSM, it can generate the JSON bundle that `nfkmattest` then can verify.

This version of the nShield Key Attestation Verifier addresses a number of issues with the previous release, see Fixed issues from previous release.

2. Features of nShield Key Attestation Verifier v1.0.2

2.1. Standalone installation

`nfkmattest` can be installed as a standalone installation with no need for an nShield HSM and Security World software. This allows third parties to verify cryptographically that a key is generated in the nShield HSM and cannot be exported in clear text. See the user guide for installation and usage information.

2.2. Security World software installation

`nfkmattest` can be installed with an nShield HSM and Software. This allows you to generate a key attestation bundle that can be forwarded to a third party to verify using the standalone installation of the `nfkmattest` tool. See the user guide for installation and usage information.

2.3. User documentation

The nShield Key Attestation Verifier release notes and user documentation are available at https://nshielddocs.entrust.com.

3. Compatibility

`nfkmattest` requires an nShield HSM with a KLF2 warrant to be able to generate a full key attestation bundle.

3.1. Supported operating systems

This release is supported on the following operating systems:

- Microsoft Windows Server 2019 x64
- Microsoft Windows Server 2022 x64
- Red Hat Enterprise Linux 9 x64
- Oracle Enterprise Linux 8 x64

3.2. Supported Security World versions

This release can be used with the following nShield Security World software installations:

- Security World v13.4

3.3. Supported hardware

This release can be installed as part of a Security World installation targeted at deployments with any combination of the following nShield HSMs:

- nShield 5s (Base, Mid, High)
- nShield 5c (Base, Mid, High)
- nShield Solo XC (Base, Mid, High)
- nShield Solo PCI Express (500+, and 6000+)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield Edge

4. Fixed issues from previous release

Reference	Description
NSE-61234	`nfkmattest` no longer returns `no such warrant` when creating an attestation bundle using an nShield Connect or an nShield Connect XC.
NSE-61031	Performing a standalone uninstall on Linux now prompts for confirmation before removing `/opt/nfast`.
NSE-60861	It is now possible to install the nShield Key Attestation Verifier alongside v13.4 Security World on Windows.

5. Known issues

Reference	Description
NSE-61073	Installing nShield Security World Software on top of a standalone installation of nShield Key Attestation Verifier is not a supported workflow.
NSE-60895	The `C:\Program Files\nCipher` folder is not removed following a standalone uninstall on Windows.