nShield Security World

nShield Trusted Verification Device v12.40 Installation Guide

04 March 2024

Contents

Chapter 1: Introduction

The nShield® Trusted Verification Device (TVD) is a USB connected smart card reader.

The nShield TVD connects to a laptop or work station. The TVD facilitates the authentication between the smart card and the HSM. The user is prompted to confirm the Electronic Serial Number (ESN) of the HSM being displayed on the nShield TVD.

Each time a smart card is inserted a new secure channel between smart card and HSM is established, when the smart card is removed the secure channel is shut down.

Chapter 2: Safety and security

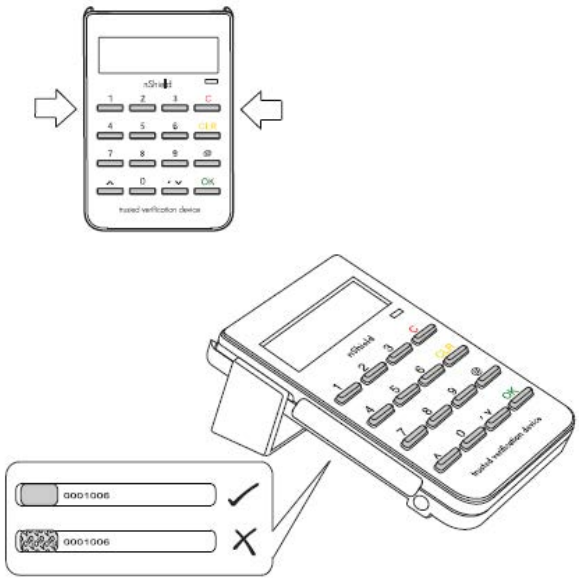
When the TVD is not being used it must be stored in a secure place.

Note: There are no user-serviceable parts inside the nShield TVD. Any attempt to dismantle the nShield TVD results in any remaining warranty cover, the maintenance and support agreement, or both being rendered void.

To help maintain security:

1. Always inspect the USB cable and the nShield TVD before use.
2. Make sure that the two nCipher tamper seals on the nShield TVD are undamaged before using the device, see Figure 1. If they are damaged the reader could have been tampered with. If this is the case please contact nCipher Support, https://help.ncipher.com
3. Never store or carry smart cards with the nShield TVD.

Figure 1. nCipher tamper seals



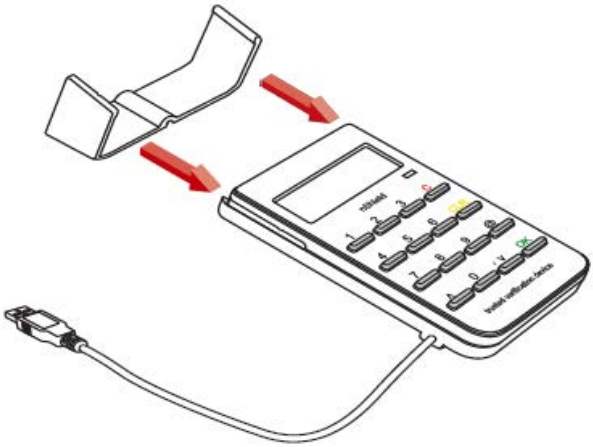
Chapter 3: Setting up the nShield Trusted Verification Device

Connecting the metal support bracket

Do the following:

1. Remove the nShield TVD and the metal stand from the packaging.
2. Slide the metal stand into the slots on either side of the TVD.
3. Route the USB cable through the groove in the base of the metal stand (if required).

Figure 2. Connecting the bracket to the nShield TVD



Software installation

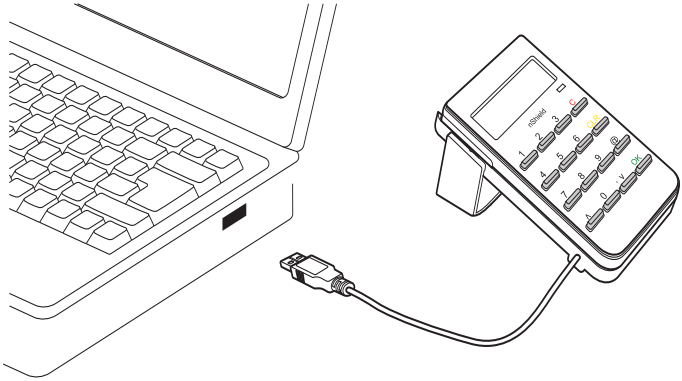
For software installation instructions, see the Remote Administration Client User Guide, which is available on the installation media.

Connecting an nShield TVD

Do the following:

1. Connect the nShield TVD to your computer, using the USB cable.
2. If your operating system detects the nShield TVD automatically, allow it to finish.

Figure 3. Connecting the nShield TVD to your computer



Note: Do not connect a nShield TVD to your computer with a smart card already inserted. The nShield TVD will not be recognised and the message **Please remove card** will be displayed on the nShield TVD. When the smart card is removed the message **Secoder 2 V2.2.1** will be displayed and the nShield TVD will be available.

Disconnecting and reconnecting the nShield TVD

After use, you can disconnect the nShield TVD from the computer's USB port, and then reconnect it when you next need to use it.

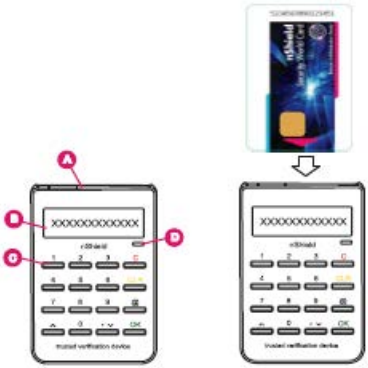
Note: Do not disconnect the nShield TVD or remove the smart card when data is being written to the inserted smart card.

Troubleshooting

If the nShield TVD does not function as expected, disconnect the nShield TVD, wait a few seconds, and then reconnect it. If this does not solve your problem, contact nCipher Support at help.ncipher.com

Chapter 4: Using the nShield Trusted Verification Device

Figure 4. The nShield TVD controls, card slot, and LED



Item	Description
A: Card slot	For inserting a smart card into the TVD, the chip on the card should face the user and inserted first into the card slot.
B: Display	Displays the ESN of the HSM.
C: Keypad	• 0 -9, CLR, ∧ and ∨: Not used • C: Used for canceling the current smart card verification • @: Can be used to show the firmware version and the name of the reader (status LED flashes at the same time) **Note:** Do not press the @ key when there is a smart card in the card slot because the time taken to display this information can cause the secure connection between smart card and HSM to be broken. • OK: Used to confirm the smart card verification and abort messages
D: Status LED	The status LED will flash when the TVD: • Is connected to a USB port • Requires the user to confirm a decision. For example, if the C button is pressed during a smart card verification the LED will flash and you will be asked to confirm the abort by pressing OK.

Chapter 5: Dimensions and operating temperatures

Parameter	Value
Dimensions	62 (w) x 95 (h) x 14 (d) mm
Weight	72g
Powered by USB host device	5V, 200 mA
Operating temperature	0 – 50 °C
Storage temperature	-10 – 50 °C
Operating and storage relative humidity	Maximum 90% non-condensing

Physical location considerations

nCipher nShield HSMs are certified to NIST FIPS 140-2 level 2 and 3. In addition to the intrinsic protection provided by an nShield HSM, customers 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 comprehensive risk mitigation program to assess both logical and physical threats. Applications running in the environment shall be authenticated to ensure their legitimacy and to thwart possible proliferation of malware that could infiltrate these as they access the HSMs' cryptographic services. The deployed environment must adopt 'defense in depth' measures and carefully consider the physical location to prevent detection of electromagnetic emanations that might otherwise inadvertently disclose cryptographic material.

When the TVD is not being used it must be stored in a secure place.