FORNETIX®
VaultCore™
HSM INTEGRATION WITH nCIPHER nSHIELD CONNECT XC GUIDE

Version 2.4

NOTICE

Fornetix LLC
5123 Pegasus Ct.
Suite X
Frederick, MD 21704
https://www.fornetix.com

The materials provided in this VaultCore™ HSM Integration With nCipher nShield Connect XC Guide, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for informational purposes only and is subject to change or withdrawal by Fornetix LLC ("Fornetix") without notice. The Documentation is proprietary information of Fornetix and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Fornetix.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Fornetix copyright notices, trademark notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Fornetix that all copies and partial copies of the Documentation have been returned to Fornetix or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, FORNETIX PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL FORNETIX BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF FORNETIX IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by this Notice.

Provided with "Restricted Rights." Use, duplication, or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Fornetix™ and VaultCore™ are registered trademarks of Fornetix IP LLC. All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Table of Contents

Conventions

Typeface	Use
Verdana Regular	• Normal text, headers, footers, TOC
Verdana Bold	• Something the user selects, types in. • Used for emphasis. • A command, an action that can be taken in the UI.
Verdana Bold (red)	• Used for **Note** and **Important** information segments headings for user awareness.
Verdana Bold Italic (blue)	• Additional information for the user related to a particular process.
Verdana Italic	• A field or column name, title of a button.
Courier New	• Commands and code examples.

1 Introduction

The VaultCore™ HSM Integration With nCipher nShield Connect XC Guide contains the necessary information to deploy a VaultCore™ Appliance connecting with a nCipher nShield Connect XC.

Note:
Due to a re-branding effort within Fornetix, the use of the following trademarked terms: "VaultCore™", "VC™", "Key Orchestration™" and "KO™" will be shown as "VaultCore", "VC", "Key Orchestration", and "KO" respectively in this manual. The trademarked terms associated Fornetix's 'Vault Core' shall replace the trademarked uses of Key Orchestration with Fornetix retaining all rights in regards to the use of its Trademarks. The term "nShield Connect XC" will be shown as "nShield Connect" in this manual going forward for ease of use.

Many layers of security are used within VC to prevent data breach, theft, or manipulation, but for those environments which require the highest levels of security, the integration of nShield Connect with VC adds an additional layer of security for the cryptographic information. The nShield Connect is used to store the master encryption key which is used to encrypt and decrypt all key material generated by VC. The encryption and decryption of the key material occurs within the crypto boundary of the nShield Connect.

Note that it is advisable that the integration with the HSM be performed directly after the initial configuration, in order to ensure that all cryptographic objects generated by VC are protected by the HSM.

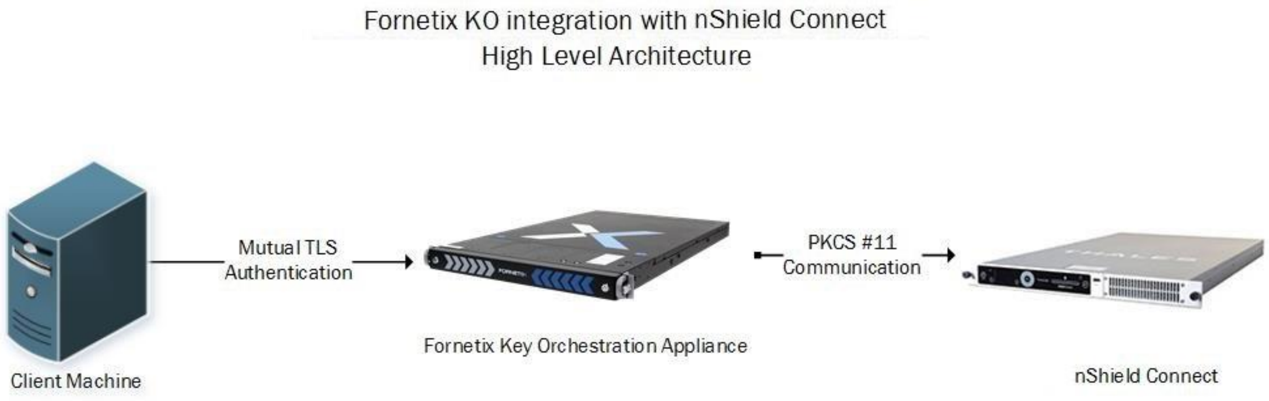

Fornetix KO integration with nShield Connect
High Level Architecture
Mutual TLS Authentication
PKCS #11 Communication
Client Machine
Fornetix Key Orchestration Appliance
nShield Connect

Figure 1. High-Level System Architecture

2 Preparation

The following is needed before proceeding with the deployment of VC.

2.1 VC Appliance

- VCVA500, VCVA2100, VC-1000, and/or VC-2000 running version 2.4.

2.2 KO Upgrade Package

- KO upgrade package containing Security World Software version 12.60.5.

2.3 KO License

- KO License file with HSM enabled
- KO License file with Clustering enabled (if configuring for disaster recovery)

2.4 nCipher nShield Connect XC

- nCipher nShield Connect +
    - 12.40.2 Security World Client
    - 12.40.2 Image
    - 2.61.2 FIPS Approved Firmware
- nCipher nShield Connect XC
    - 12.60.5 Security World Client
    - 12.60.2 Image
    - 12.50.11 FIPS Pending Firmware
- Remote File System must already be created
    - Server hosting the Remote File System has been created and configured
    - nShield Connect has been configured to use the Remote File System
- Security World must already be created
    - The PKCS #11 provider module must be installed
    - The following Security World types are supported:
        - FIPS 140-2 level 2
        - FIPS 140-2 level 3 (strictFIPS)
- Key to be used by the VC Appliance must already be created
    - Cryptographic algorithms supported:
        - AES
    - Cryptographic key lengths supported:
        - 128
        - 256
    - Key Application Types supported:

  - PKCS #11 (pkcs11)
- Key Protection Types supported:
  - Module-protected

3 nShield Connect Deployment Instructions

The following sections outline how to configure an nShield Connect and its associated Remote File System for integration with a VC Appliance. This is a minimum requirements installation; please see the **nShield Connect Installation Guide** and **nShield Connect User Guide** for full details on available configurations.

Note:
To use an existing nShield Connect deployment, start with Section 3.8 to create the key needed for the VC Appliance.

3.1 Allocate Server for Remote File System

The nShield Connect must have a Remote File System (RFS), which contains master copies of all the files that the HSM needs. This can be a physical server or a virtual machine.

Note:
Fornetix recommends use of a Linux-based operating system for the RFS.

3.2 Install Security World Software

Install the Security World software on the RFS server. These instructions assume the use of a Linux 64-bit operating system on the RFS server.

1. Login to the RFS server using an account with root permissions or sudo capabilities.

2. Create a temporary installation directory using this command:

```
sudo mkdir /tmp/ncipher
```

3. Copy the Linux installation files to the */tmp/ncipher* directory. The installation files are located in the "linux" directory on the Security World Software disk or digital download. Be sure to copy the entire "linux" directory.

4. Extract the software tar files:

```
tar -xvf /tmp/ncipher/linux/amd64/ctd.tar.gz -C /
tar -xvf /tmp/ncipher/linux/amd64/ctls.tar.gz -C /
tar -xvf /tmp/ncipher/linux/amd64/devref.tar.gz -C /
tar -xvf /tmp/ncipher/linux/amd64/hwsp.tar.gz -C /
tar -xvf /tmp/ncipher/linux/amd64/javasp.tar.gz -C /
tar -xvf /tmp/ncipher/linux/amd64/jd.tar.gz -C /
tar -xvf /tmp/ncipher/linux/amd64/ncsnmp.tar.gz -C /
tar -xvf /tmp/ncipher/linux/amd64/raserv.tar.gz -C /
```

5. Install the driver using the following command:

```
/opt/nfast/sbin/install
```

6. Confirm the installation of the driver was successful by using the *enquiry* command. The result should report that the mode is "operational."

```
/opt/nfast/bin/enquiry
```

7. You can now remove the installation files using this command:

```
sudo rm -rf /tmp/ncipher
```

For other operating systems and more detailed information, please see Chapter 4 of the **nShield Connect Installation Guide**.

3.3 Rack the nShield Connect and Connect Cables

1. Rack the nShield Connect and connect the cables by following the instructions outlined in Chapter 6 of the **nShield Connect Installation Guide**.

2. *Optional:* Connect a USB keyboard for entering passphrases for the Administrator Card Set.

3.4 Configure the Ethernet Interfaces on the nShield Connect

Configuring the nShield Connect's ethernet interfaces with the appropriate network settings is required. For detailed information about this process, please see Chapter 7 of the **nShield Connect Installation Guide**.

3.5 Configure Remote File System

For detailed information, please see Chapter 7, Subsection "Configuring the Remote File System (RFS)" of the **nShield Connect Installation Guide**.

1. The firewall must be configured to allow TCP connections on port 9004 in order to communicate with the nShield Connect.

2. Determine settings of the nShield Connect by using the *anonkneti* command:

```
/opt/nfast/bin/anonkneti nShield_Connect_IP
```

Note:
If communication is successful, the command returns the ESN and KeyHash to use in the command discussed below in **Step 3**.

3. Prepare for communication with the nShield Connect:

```
/opt/nfast/bin/rfs-setup --force nShield_Connect_IP ESN KeyHash
```

4. Prepare for communication with the VC Connect:

```
/opt/nfast/bin/rfs-setup –gang-client –write-noauth VC_Appliance_IP
```

5. Configure the nShield Connect to use the RFS server by using the front console navigation:

   a. Navigate to System > System configuration > Remote file system > Define IPv4 RFS
   b. Enter the IP address of the RFS server
   c. Leave the port number at the default setting of 9004

3.6 Create Security World

For detailed information, please see Chapter 7, Subsection "Creating a Security World using the nShield Connect front panel" of the **nShield Connect User Guide**.

Note:
It is recommended to connect a USB keyboard for entering passphrases for the Administrator Card Set.

1. Using the front panel of the nShield Connect, choose Security World mgmt > Module initialization > New Security World.

2. Enter the default quorum for the Administrator Card Set (ACS). The minimum number of cards required for quorum operations is two out of a total of three cards in the set, as recommended by Fornetix.

3. You are now prompted to Specify all quorums, enter **NO**.

   Note:
   Choosing **NO** will use the default quorum for all operations. If you enter **YES**, you will be prompted to choose the quorum numbers required for each type of operation.

4. Select the Cipher suite for the Security World. The recommended choice is AES key (SP800-131 compliant).

5. Specify whether the Security World will conform to FIPS 140-2 requirements for roles and services at level 3. The recommended choice is the FIPS 140-2 level 3 Security World.

6. Specify whether the HSM is a valid target for remote shares. Enter **NO** as recommended by Fornetix.

7. You will now be prompted to insert the ACS cards. These will be processed individually, requiring entry and confirmation of a passphrase for each card in the set.

3.7 Configure the RFS as a Client

The Remote File System server must now be configured as a client of the nShield Connect.

1. Using the front panel of the nShield Connect, choose System > System configuration > Client config > New IPv4 client.

2. Enter the IP address of the RFS server.

3. Login to the RFS server.

4. Determine settings of the nShield Connect by using the *anonkneti* command:

   ```
   /opt/nfast/bin/anonkneti nShield_Connect_IP
   ```

   Note:
   If communication is successful, the command returns the ESN and KeyHash to use in the command discussed below in **Step 5**.

5. Configure the RFS server to use the nShield Connect by running the following command:

   ```
   /opt/nfast/bin/nethsmenroll nShield_Connect_IP ESN KeyHash
   ```

3.8 Generate Key for Use With VC Appliance

The VC Appliance requires that a key has already been created in the nShield Connect before integration. For supported key types, lengths, and module protection types, please refer to Section 2.4. Fornetix recommends using an AES-256 module-protected key.

1. Log in to the RFS server.

2. Generate a new key using the following command. This example will create the recommended AES-256 module-protected key named "koappliance":

   ```
   /opt/nfast/bin/generatekey --generate --batch pkcs11 protect=module
   type=aes size=256 plainname=koappliance
   ```

4 VC Deployment Instructions

The following must be completed as part of the deployment of VC.

4.1 Rack the VC Appliance and Connect Cables

1. Rack the VC Appliance and connect the cables by following the instructions outlined in the **VaultCore Initial Setup Guide**. If using Virtual Appliances, make sure they are fully deployed into VMware by following the instructions outlined in the **VaultCore Virtual Appliance Initial Setup Guide.**

4.2 Perform Initial Configuration of the VC Appliance

1. Perform the initial configuration of the VC Appliance by following the instructions outlined in the **VaultCore Initial Setup Guide**.

4.3 Add the VC Appliance as an Authorized Client of the nShield Connect

1. Add the IP address of the VC Appliance as an authorized client of nShield Connect. "Unprivileged" permissions are sufficient. This can be done remotely by following the "***Remote configuration of additional clients***" section of the **nShield® Connect - User Guide for Unix**.

4.4 Prepare Configuration Data from the nShield Connect

1. Gather the following information and data which will be used in the next steps:

    a. The upgrade file provided by Fornetix to load the Security World software and drivers.

    b. IP address of the nShield Connect.

    c. IP address of the Remote File System associated with the nShield Connect.

    d. *Optional*: Slot number where the key was created on the nShield Connect.

    e. Name of the key which was created on the nShield Connect for the VC Appliance.

    f. Length of the key which was created on the nShield Connect for the VC Appliance.

    g. *Optional:* If using SSH file copy to transfer files from the Remote File System associated with the nShield Connect to the VC Appliance, a username and password with permissions to read the */opt/nfast/kmdata/local* directory is needed. This option is only available for Linux-based Remote File Systems.

h. *Optional:* If using the nCipher sync tool or SSH file copy is not possible, an uncompressed tar file of the */opt/nfast/kmdata/local* directory from the Remote File System associated with the nShield Connect will be required. This is considered advanced configuration, and also allows administrators to strictly limit which keys from the Security World are transferred to the VC Appliance.

i. To create the tar file with the proper structure for uploading to the VC Appliance, follow these steps:

   i. Login to the RFS server using an account with read/write permissions to the */opt/nfast/kmdata* directory
   ii. Change to the directory using the command *cd /opt/nfast/kmdata*
   iii. Create the tar file using the command *tar -cvf local.tar local*

4.5 Begin Configuration of the nShield Connect and Upload Software

To configure the nShield Connect using the KO CLI (command line interface):

Note:
You must have a KO License file with HSM enabled, in order to use and configure the nShield Connect. If you have not installed a HSM license file yet please follow the steps in Install the HSM License File, otherwise skip to Initialize the HSM Connection.

4.5.1 Install the HSM License File

The system license applies the HSM settings and controls the ability to utilize HSM functionality on the appliance.

Before you install a license:

- The license file to be uploaded should be placed in a location that has the ability to transfer the file to the VC Appliance.

To install a license:

1. Once you receive the license file from Fornetix Support, save it locally and note the name of the file and the location in which you saved it.

2. Enter "7" at the prompt to access the Support submenu.

3. Enter "2" at the prompt to access the License submenu.

4. Enter "3" at the prompt to install a license, and press **ENTER**.

5. You are prompted to confirm you have received a new license file from Fornetix Support by selecting **Y/N**. If **N** is entered, you must register with Fornetix before proceeding. If **Y** is entered, you are prompted to enter the name of the license file to be uploaded.

6. Connect to VC Appliance IP using an scp or sftp connection, then upload the license file to the VC Appliance using the following details:

   - **Host -** hostname or IP address of the VC Appliance
   - **Username -** user name to use for authentication with the VC Appliance
   - **Password -** password (case sensitive) for the kosftpuser that is displayed on the screen
   - **Remote path -** destination path
   - **File -** name of the file displayed on the screen

7. Once the license file has been uploaded to the VC Appliance, the appropriate account settings and abilities are enabled accordingly.

The user must log out and then log back in to see the license changes take effect in the menu.

4.5.2 Install Necessary Software to Connect to nCipher nShield Connect

1. Enter "4" for Manage VaultCore Appliance Chassis and press **ENTER**.

2. Enter "6" (or "3" on a VCVA platform) for HSM Management and press **ENTER**.

3. Enter "2" for Initialize the HSM Connection and press **ENTER**.

4. The system displays a message stating you are about to begin the process to install the software necessary to connect to your nCipher nShield Connect, requiring you to upload the upgrade package provided by Fornetix Support. Confirm whether you are ready to proceed by selecting **Y/N.** Select **Y** and press **ENTER** to continue the install.

5. Select **C** to confirm you have obtained a system update file from Fornetix Support.

6. Enter the file name of the upgrade package and press **ENTER**.

7. The instructions to upgrade the package and password are displayed. Use this information to upload the upgrade package to the VC Appliance.

8. The upgrade package will be processed and the Security World software installed. Press **ENTER** when the processes complete.

4.6 Enter the nShield Connect Settings

After you finish uploading the upgrade package, the system begins to prompt you to enter information regarding your nCipher nShield Connect HSM, as well as the Remote File System (RFS).

To specify the nShield Connect settings:

1. Enter the IP Address of the nShield Connect and press **ENTER**.

2. Enter the port number of the nShield Connect (default 9004) and press **ENTER**.

3. Confirm that the ESN and KeyHash displayed are correct for the selected nShield Connect by selecting **Y/N**. If the values are correct, enter **Y** and press **ENTER.**

4.7 Enter Key Information

After you confirm the ESN and KeyHash are correct, you must specify which key stored on the nShield Connect to use for encryption of VC Appliance key material.

To specify which key to use for encryption of the VC Appliance:

1. Enter the Key Name and press **ENTER**.

2. Enter the Key Length of the nCipher nShield Connect (valid lengths are 128, 256) and press **ENTER**.

4.8 Enter Remote File System Information

Once you enter the key Information, the system will prompt you to select the method by which you wish to copy Security World files from the nCipher nShield Connect. The following options are displayed:

- Utilize the nCipher Sync Tool
- Retrieve the Files via SSH
- Upload the Required Information

Note:
It is important to use the nCipher Sync Tool. The other options are only included if the Sync Tool method does not work, or for advanced options.

4.8.1 Retrieve the Files via nCipher Sync Tool

This method will use the nCipher `rfs-sync` command to move the Security World and key files automatically from the Remote File System (RFS) to the VC Appliance.

1. Enter "1" for Utilize the nCipher Sync Tool and press **ENTER**.

2. Enter the IP Address of the Remote File System associated with the nShield Connect and press **ENTER**.

3. Review all the settings which have been entered. If the values are correct, enter **Y** and press **ENTER** to complete the configuration of the nShield Connect, the system will now reboot.

   Note:
   If you enter **N**, you will be prompted to enter information regarding your nCipher nShield Connect HSM as well as the Remote File System, confirm the ESN and KeyHash are correct, and enter the Key Name and Key Length. Then you will be prompted to select the method by which you wish to copy Security World files from the nCipher nShield Connect again.

4.8.2 Retrieve the Files via SSH

This method will use an SSH connection to move the Security World and key files from the Remote File System to the VC Appliance. This method only works with Linux-based Remote File Systems.

1. Enter "2" for Have the Appliance Retrieve the Files via SSH and press **ENTER**.

2. Enter the IP Address of the Remote File System associated with the nShield Connect and press **ENTER**.

3. Enter the Administrator username for the RFS, and press **ENTER**. This user must have permissions to read files in the */opt/nfast/kmdata/local* directory on the Remote File System.

4. Enter the password for the Administrator of the RFS, and press **ENTER**.

5. Confirm the password for the Administrator of the RFS, and press **ENTER**.

6. Review all the settings which have been entered. If the values are correct, enter **Y** and press **ENTER** to complete the configuration of the nShield Connect, the system will now reboot.

   Note:
   If you enter **N**, you will be prompted to enter information regarding your nCipher nShield Connect HSM as well as the Remote File System, confirm the ESN and KeyHash are correct, and enter the Key Name and Key Length. Then you will be prompted to select the method by which you wish to copy Security World files from the nCipher nShield Connect again.

4.8.3 Retrieve the Files via Uploading the Required Information

This method will allow the upload of a tar or zip file containing the Security World and key files. This option allows administrators to limit the files copied onto the VC Appliance to the minimum that is required for the nShield Connect. This option also allows for full configuration if the other options cannot copy the files automatically.

1. Enter "3" for Upload the Required Information and press **ENTER**.

2. Enter the name of the tar or zip file created and press **ENTER**. Follow the instructions to copy the file onto the VC Appliance. When the upload has completed, press **ENTER**.

3. Review all the settings which have been entered. If the values are correct, enter **Y** and press **ENTER** to complete the configuration of the nShield Connect, the system will now reboot.

   Note:
   If you enter **N**, you will be prompted to enter information regarding your nCipher nShield Connect HSM as well as the Remote File System, confirm the ESN and KeyHash are correct, and enter the Key Name and Key Length. Then you will be prompted to select the method by which you wish to copy Security World files from the nCipher nShield Connect again.

4.9 Verify VC Appliance

Verify the deployment of the VC Appliance by following the instructions outlined in the **VaultCore Initial Setup Guide**.

5 Backup and Restore

When a backup of VC is performed, the encrypted backup file contains the configuration of the nShield Connect.

A backup can only be restored to a VC Appliance licensed to use an nShield Connect. A restore cannot be done to a VC Appliance configured with a nCipher internal device, any other HSM provider, or a VC Appliance without an HSM integration.

A backup can only be restored in the same Security World. This means the Security World in place at the time the backup of the VC Appliance was created must still exist at the time of restore.

Because the data within VC is encrypted, great care must be taken to ensure backups of the nShield Connect as well, to ensure the master encryption key is not lost.

Warning:
If a VC Appliance is configured to use an HSM for encryption, and the HSM or the key used for encryption is permanently lost or destroyed, there is no possibility of decrypting the key material stored within the VC Appliance.

More information on backing up and restoring VC can be found in the **VaultCore Appliance Configuration Guide**.

6 Managing the nShield Connect Configuration

The KO CLI (command line interface) can be used to review, initialize, and diagnose the nShield Connect configuration. The tools are available in the KO CLI under Section 4 - Manage VaultCore Appliance Chassis, Subsection 6 - HSM Management (or subsection 3 on a VCVA platform). The menu options are detailed here in the following subsections.

More information about the KO CLI can be found in the **VaultCore Appliance Configuration Guide**.

6.1 Show Current Configuration

To display the current configuration of the nShield Connect:

1. Enter "1" and press **ENTER**.

2. Basic information about the nShield Connect is displayed, including Hardserver Status, Connection Status, and Hardware Status.

Additional menu options are available to display more detailed information. The additional menu options are detailed in the following subsections:

- HSM Hardware Configuration Details
- HSM KO Configuration Details

6.1.1 HSM Hardware Configuration Details

To display hardware configuration details:

1. Enter "1" and press **ENTER**.

2. Information regarding the FIPS Level, Server Mode, Module Mode, and Connection Status are displayed.

Additional menu options are available to display more detailed information. The additional menu options are detailed in the following subsections:

- Server Configuration Details
- Module Configuration Details

6.1.1.1 Server Configuration Details

To display hardware configuration details:

1. Enter "1" and press **ENTER**.

2. Information regarding the Mode, Serial Number, Product Name, Version, and Remote Server Port are displayed.

6.1.1.2 Module Configuration Details

To display module configuration details:

1. Enter "2" and press **ENTER**.

2. Information regarding the Mode, Serial Number, Product Name, Version, Connection ESN, Connection IP, Connection Hash, Connection Port, and Connection Status are displayed.

6.1.2 HSM KO Configuration Details

To display KO configuration details:

1. Enter "2" and press **ENTER**.

2. Information regarding the Key Name and Key Length are displayed.

6.2 Initialize the HSM Connection

This command initializes the HSM configuration settings.

Warning:
Changes to the configuration are permitted primarily for cases of IP address or key name changes. The value of the Master Key must be exactly the same in order for any existing keys in the VC Appliance which were previously encrypted with the Master Key, to be decrypted properly. Changing the VC Appliance to a differently valued Master Key will render all previously encrypted data inaccessible. Changing to a new Security World will also remove access to the previously used Master Key, and will render all previously encrypted data inaccessible

1. Enter "2" and press **ENTER**. If the system has already been configured for integration with an nShield Connect, you will be required to enter confirmation codes in order to continue with the HSM configuration.

6.3 Run Diagnostics

The Run Diagnostics menu contains diagnostic routines which can confirm correct functionality of the VC Appliance integration with the nShield Connect.

1. Enter "3" and press **ENTER** if the system has already been configured for integration with an nShield Connect.

Additional menu options are available to display more detailed information. The additional menu options are detailed in the following subsections:

- Run Diagnostic Utilities
- Download the Diagnostics Log
- Set the HSM Log Level

6.3.1 Run Diagnostic Utilities

To verify the functionality of the nShield Connect:

1. Enter "1" and press **ENTER**.

2. The following Utilities are displayed with a PASSED or FAILED Status:

   - Connect Software Check
   - Security World Valid
   - KO Appliance Key Found
   - KO Configured for HSM

   Definitions of error codes are listed in Appendix A.

6.3.2 Download the Diagnostics Log

To download the diagnostic package generated by the *nfdiag* utility:

1. Enter "2" and press **ENTER**.

2. The system creates the package for download, then provides the kosftpuser password to use to download the file.

3. To download the file, connect to the VC Appliance IP using an scp or sftp connection with the following details:

   - **Host -** hostname or IP address of the VC Appliance
   - **Username -** user name to use for authentication with the VC Appliance
   - **Password -** password (case sensitive) for the kosftpuser that is displayed on the screen
   - **Remote path –** the destination path
   - **File -** name of the file displayed on the screen

4. Press **ENTER** when you have completed the download.

6.3.3 Set the HSM Log Level

This option is reserved for future enhancement.

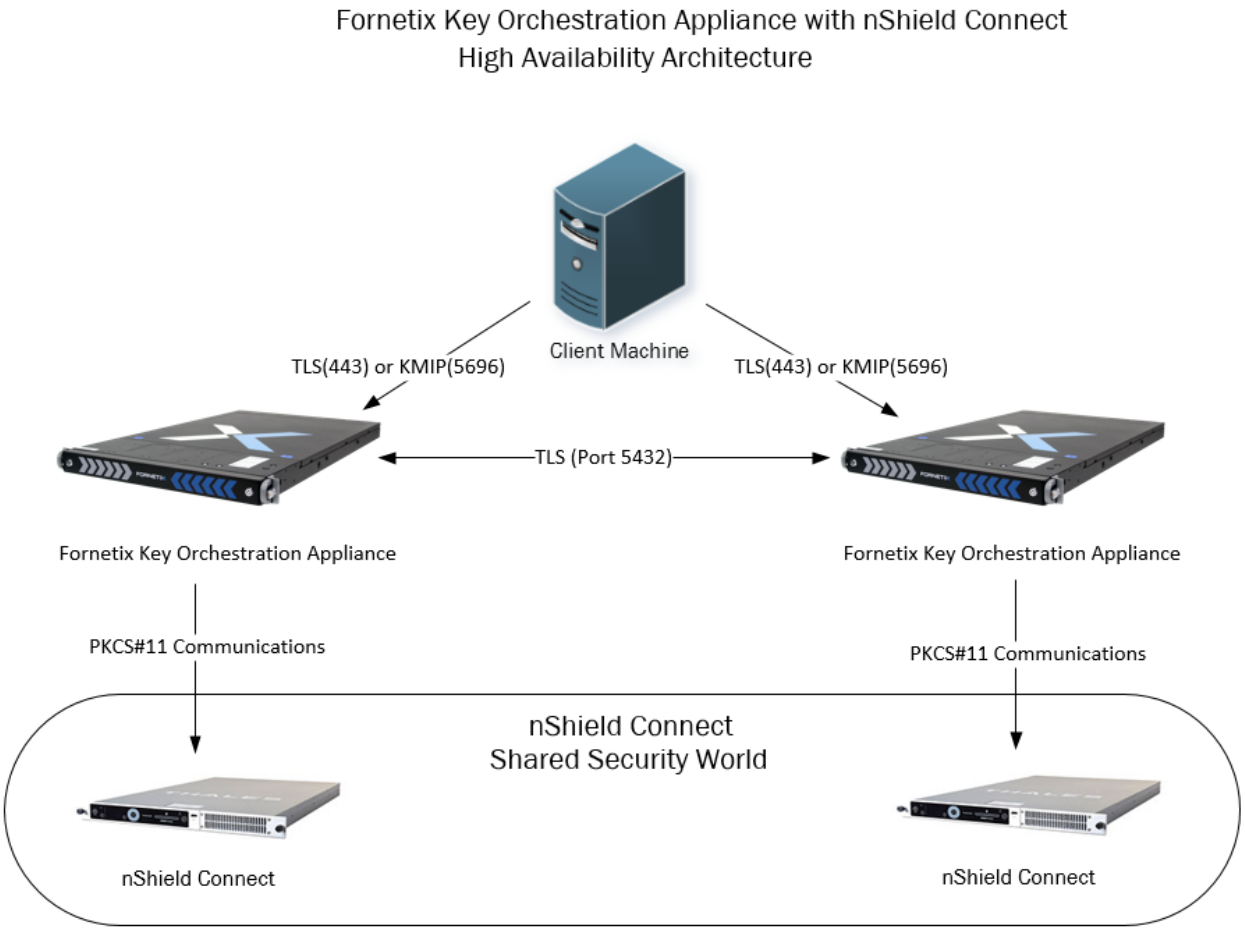
7 Clustering and Disaster Recovery

Two VC Appliances can be joined in a disaster recovery cluster. Administrators will need to ensure that the IP address of the additional VC Appliance is configured as a client of the nShield Connect as noted in Section 4.3.

All VC Appliances used in the cluster must use the same HSM type. A VC Appliance configured to use an nShield Connect can only participate in a cluster with other VC Appliances which are configured to use an nShield Connect as well. They must share the same Security World, and use the same key name and length. A VC Appliance that uses an nShield Connect for HSM integration cannot be clustered with a VC Appliance that uses an nShield Solo or any other HSM provider. A VC Appliance with an nShield Connect also cannot be clustered with a VC Appliance that does not have an HSM integration.

More information on clustering can be found in the **VaultCore Appliance Configuration Guide**.

When configuring VC Appliances to use nShield Connect network HSMs, the recommended configuration is pictured below. Two nShield Connect appliances must be configured to use a single Security World. Each of the VC Appliances should then be configured to point to one of the nShield Connect appliances directly by IP address.



8 Troubleshooting

The tools outlined in Section 6 can be used to troubleshoot issues related to the nShield Connect.

KO logs also contain information that can be used when troubleshooting issues. More information on logs can found in the **VaultCore Appliance Configuration Guide**.

Appendix A – Error Codes

MHSMT002 - Enquiry command cannot identify the module.

MHSMT003 - Security World does not exist.

MHSMT004 - Key specified in configuration does not exist.

MHSMT005 - KO services are not configured to use the HSM key.

MHSMT006 - Key generation using HSM encryption failed.