HID® ActivID® Credential Management System

Technical Note: Configuring Entrust Datacard® nShield™ HSMs

Document Reference: CMS_5.3_EntrustDatacard_TN_12.2020

Product Version: 5.3

December 2020

hidglobal.com

Copyright

Trademarks

Revision History

Date	Description	Document Version
December 2020	Update for 5.3	1.11
February 2020	Update for 5.2 (name changed from Thales nShield)	1.10
October 2019	Update for 5.1	1.9
July 2019	Update for 5.1 beta release	1.8

Contacts

Technical Support
If you purchased your product from a third party, then please contact that third party for Technical Support.

If you purchased your product directly from HID Global:

Americas	Europe, Middle East and Africa	Asia Pacific
+1 800 670 6892	+33 (0) 1 74 18 17 70	+852 3160 9873 +61 3 9111 2319

For further contact details, go to https://www.hidglobal.com/support

Customer Service
To contact HID Global Customer Service, go to https://www.hidglobal.com/customer-service

Typographic and Document Conventions

Typography	Description
blue	Cross-references within the document.
blue, underline	References to external web addresses.
bold	Action steps (paths, buttons, options); field and drop-down list labels; emphasis.
italic	File names, document titles, and file extensions.
`Code snippets`	Highlights `code snippets` within regular content.
Code samples	Highlights code samples
⚠	WARNING: This symbol indicates a critical warning. It applies to actions that if taken or not taken will break the system. Read the warning carefully and follow it.
(!)	Important: This symbol indicates something very important to the reader. Ignore this symbol at your own risk.
🗎	Note: This symbol indicates a note that should be of interest to the reader. It is not critical. Nevertheless, the reader should pay attention.

Table of Contents

Copyright 2

Trademarks 2

Revision History 2

Contacts 2

Typographic and Document Conventions 3

List of Figures 6

1.0 Introduction 7

1.1 Product Overview 7
1.2 Document Scope and Audience 7
1.3 Overview 8
1.4 HSM Product Version 8

2.0 Setting Up an nShield Solo 9

2.1 Procedure 1: Installing the nCipher Software 9
2.2 Procedure 2: Configuring the nCipher Security World 13
2.2.1 Procedure 1: Creating a New Security World/Administrator Card Set 14
2.2.2 Procedure 2: Creating a New Operator Card Set 17

3.0 Accessing the nShield Solo from ActivID KMS/CMS 20

3.1 Preparing the nShield Solo for Use with ActivID KMS 20
3.2 Preparing the nShield Solo for Use with ActivID CMS 21

4.0 Setting Up an nShield Connect 22

4.1 Task 1: Installing the nCipher Software 22
4.2 Task 2: Configuring the HSM Ethernet Port 27
4.3 Task 3: Configuring a Remote File System 28
4.3.1 Option 1: For an Authenticated Client with KNETI Authorization 29
4.3.2 Option 2: For an Unauthenticated Client without KNETI Authorization. 30
4.4 Task 4: Configuring HSM to Work with a Client System 31
4.5 Task 5: Configuring the Client System to Access the HSM 32
4.6 Task 6: Configuring an nCipher Security World 34
4.6.1 Creating a New Security World and Administrator Card Set 35
4.6.2 Creating a New Operator Card Set 38

5.0 Accessing the nShield Connect from ActivID KMS/CMS 41

5.1 Preparing the nShield Connect for Use with ActivID KMS 41
5.2 Preparing the nShield Connect for Use with ActivID CMS 42
5.3 Accessing HSM Tokens from ActivID KMS/CMS 43
5.3.1 Accessing HSM Tokens—ActivID KMS 43
5.3.2 Accessing HSM Tokens —ActivID CMS 43

6.0 Troubleshooting....44

6.1 Checking the Module State.... 44
6.2 About Log File.... 44
6.3 Insecure Key Used Too Long After Creation.... 44

List of Figures

Figure 1: ActivID KMS, ActivID CMS, and HSM Interaction 8
Figure 2: nShield Connect Front Panel 27

1.0 Introduction

1.1 Product Overview

HID® ActivID® Credential Management System (CMS) enables organizations to issue an authentication credential that goes beyond perimeter security. A smart card, smart token, virtual smart card or mobile smart card can be used to secure access to individual workstations and servers within the firewall, as well as securing access to the VPN and applications. The high assurance credential can also be used to encrypt data, hard drives, documents and emails, and for digital signatures.

ActivID CMS is a solution for issuing and managing high-assurance credentials. The solution manages authentication devices (e.g., smart cards, smart USB keys, virtual smart cards, mobile devices) and credentials they contain throughout their entire lifecycle.

Providing a full-featured Public Key Infrastructure (PKI) registration authority and credential manager for most leading PKI products, ActivID CMS enables the secure deployment and management of authentication devices that contain the following credentials:

- PKI certificates,
- One-time passwords (OTPs),
- Static passwords,
- Biometric data, and
- Demographic data.

ActivID CMS is a Web-based management system that can be integrated with existing provisioning systems and their components, including:

- Network access control systems,
- Physical access control systems,
- Enterprise database and directory infrastructures, and
- Public Key Infrastructure (PKI).

1.2 Document Scope and Audience

This technical note explains how to configure Entrust Datacard® (formerly Thales®) nShield™ Connect and Solo HSMs for use with ActivID CMS and sequence of operations required to set up the nShield HSMs for use with ActivID KMS (and later with ActivID CMS).

This technical note is not intended to replace the Entrust Datacard documentation. The intent of this technical note is to provide guidance on how to use the nShield HSM and its accessories with the HID Global solution. For example, the default location of Entrust Datacard files depends on both the support software and the Microsoft® Windows® version in use. For this reason, it is recommended that you reference and use the Entrust Datacard release notes for this type of information.

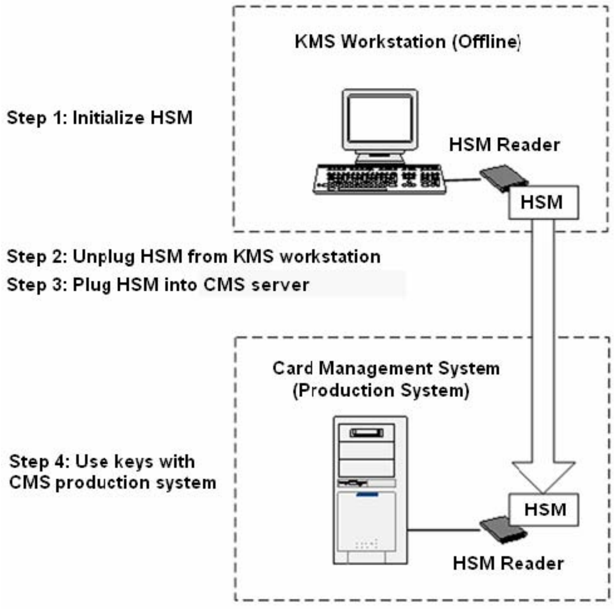
1.3 Overview

HID Global provides identity assurance solutions to manage security credentials that are populated in smart cards during the device issuance process. These security credentials (cryptographic keys) control access to smart cards during management operations (such as card application loading and personalization). ActivID Key Management System (KMS) and ActivID Credential Management System (CMS) are complementary products that ensure secure management and issuance of smart cards.

ActivID KMS enables the setup, management, maintenance, backup, and update of Hardware Security Modules (HSMs). HSMs such as the Entrust Datacard (formerly Thales) nShield Connect and nShield Solo HSMs securely store cryptographic key materials and are similar to large-storage, multi-session smart cards. However, unlike smart cards, they are used mainly on the server side of a system.

ActivID KMS ensures that HSMs are loaded with the appropriate cryptographic key materials. These keys are necessary for the ActivID CMS to take possession of the cards and, in turn, personalize the card applications that are securely loaded by ActivID CMS. Cryptographic key materials are sensitive information in the security chain. These keys must be exchanged, stored, and populated in a secure manner. A FIPS 140-certified HSM is required to meet a high-security level solution. The following figure shows the interaction between ActivID CMS, and the HSM unit.

Figure 1: ActivID KMS, ActivID CMS, and HSM Interaction



1.4 HSM Product Version

Refer to the ActivID CMS Overview for the list of supported Entrust Datacard (formerly Thales) HSMs: nShield Connect (network HSM) and nShield Solo (PCI-E card).

2.0 Setting Up an nShield Solo

This section describes how to set up an nShield Solo HSM for use with ActivID Key Management System (KMS) and ActivID Credential Management System (CMS).

Note: This section provides guidelines based on a specific version of the nCIpher products, using the nCipher terminology. Please refer to the latest nCipher documentation that refers to the specific product and version you are deploying.

2.1 Procedure 1: Installing the nCipher Software

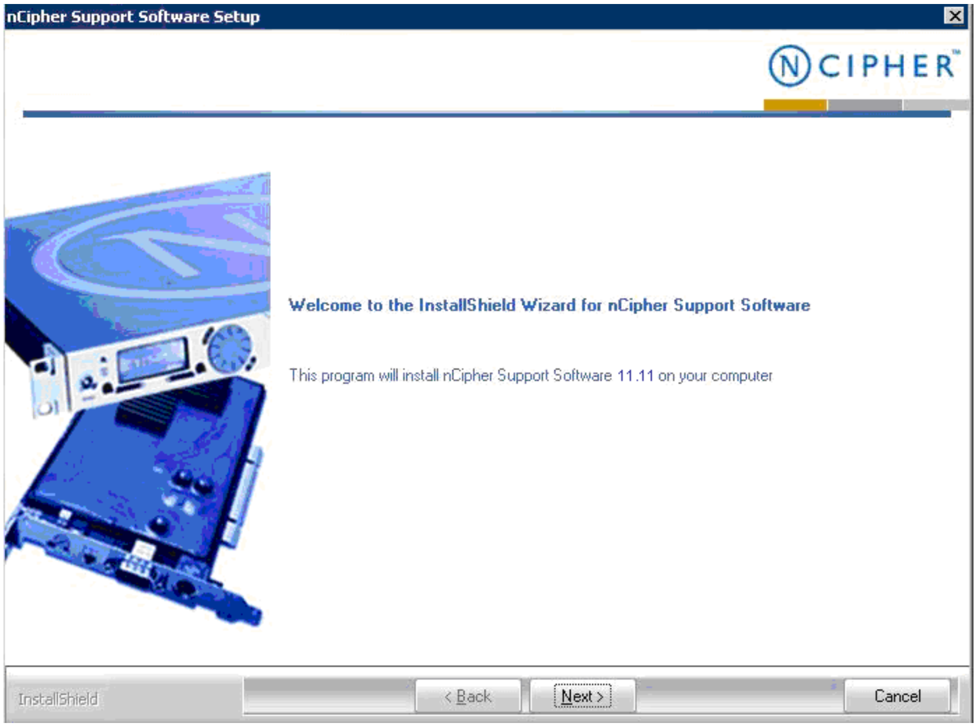
Prerequisites:

- You must install one of the following Java™ products prior to installing the nCipher components:
  - Java Runtime Environment™ (JRE)
  - Java Developer Kit™ (JDK)
- You must install the 64-bit version of the nCipher Security World software.

Note: ActivID CMS 5.0 and higher uses the 64-bit PKCS#11 library.

1. Insert the nCipher software Installation CD.

   If the installation software does not start automatically, run the *Setup.exe* file.



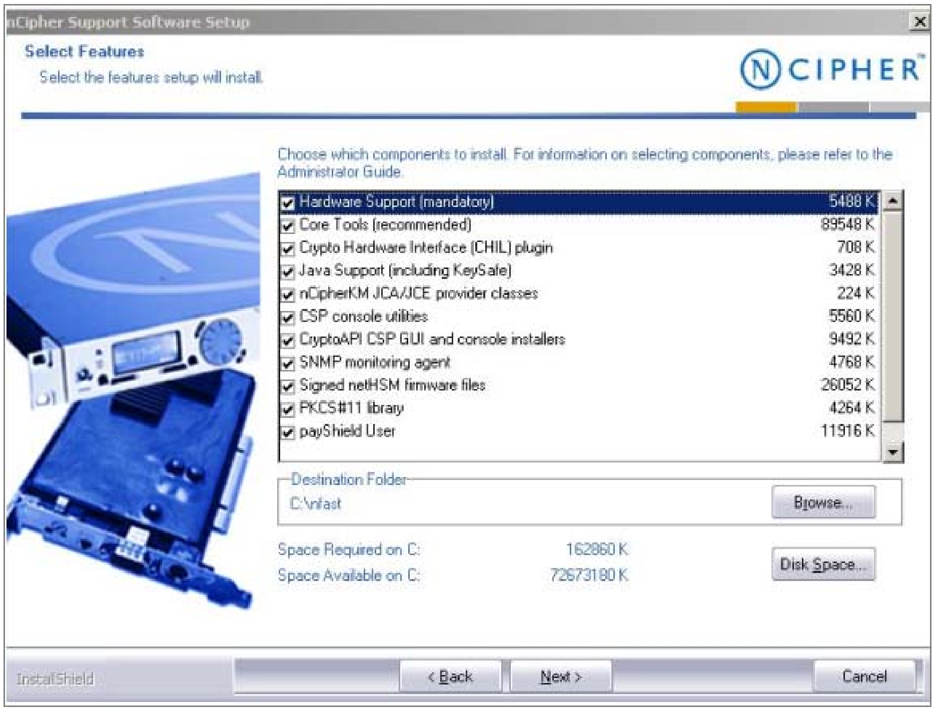
nCipher Support Software Setup

Welcome to the InstallShield Wizard for nCipher Support Software

This program will install nCipher Support Software 11.11 on your computer

2. When the Welcome page appears, click **Next**.
3. Accept the license agreement, and then click **Next**.

Note: The following steps are not intended to replace nCipher technical documentation. For specific details, see the nCipher technical documentation, follow the prompts, and take note of any tips presented here.



nCipher Support Software Setup

Select Features

Select the features setup will install.

Choose which components to install. For information on selecting components, please refer to the Administrator Guide.

☑ Hardware Support (mandatory)	5488 K
☑ Core Tools (recommended)	89548 K
☑ Crypto Hardware Interface (CHIL) plugin	708 K
☑ Java Support (including KeySafe)	3428 K
☑ nCipherKM JCA/JCE provider classes	224 K
☑ CSP console utilities	5560 K
☑ CryptoAPI CSP GUI and console installers	9492 K
☑ SNMP monitoring agent	4768 K
☑ Signed netHSM firmware files	26052 K
☑ PKCS#11 library	4264 K
☑ payShield User	11916 K

Destination Folder

C:\nfast

Space Required on C: 162860 K

Space Available on C: 72673180 K

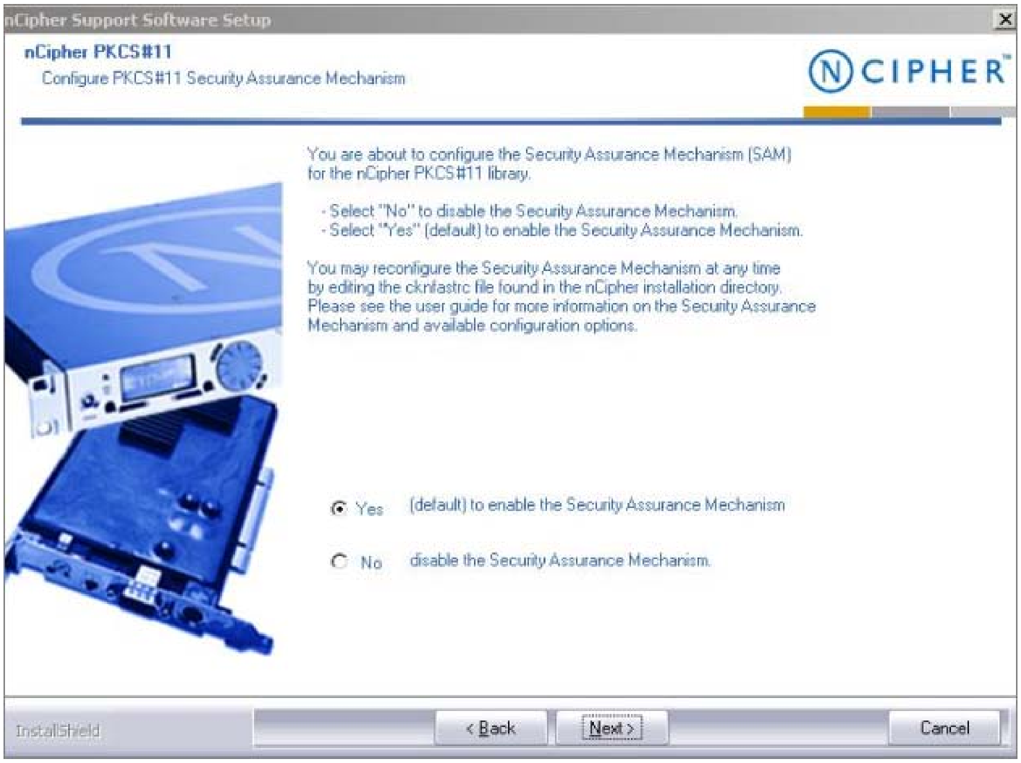
4. When the Select Features page appears:

   a. Accept the default options that are already selected.

   b. Accept the default installation directory.

   Important: It is strongly recommended that you accept the default installation directory. In this document, the installation directory is referred to as <installdir>.

   c. Click **Next**.



nCipher PKCS#11

Configure PKCS#11 Security Assurance Mechanism

You are about to configure the Security Assurance Mechanism (SAM) for the nCipher PKCS#11 library.

- Select "No" to disable the Security Assurance Mechanism.
- Select "Yes" (default) to enable the Security Assurance Mechanism.

You may reconfigure the Security Assurance Mechanism at any time by editing the cknfastrc file found in the nCipher installation directory. Please see the user guide for more information on the Security Assurance Mechanism and available configuration options.

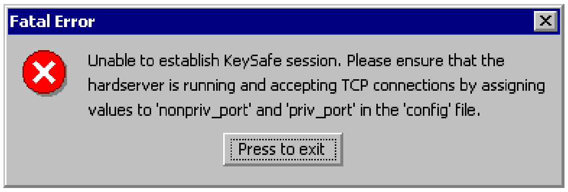
● Yes (default) to enable the Security Assurance Mechanism

○ No disable the Security Assurance Mechanism.

5. When the Configure PKCS#11 Security Assurance Mechanism page appears, perform the following tasks:
   a. Select the **Yes** option (the default), which enables the Security Assurance Mechanism.
   b. Click **Next**.
   c. Click **Finish** when the displayed message indicates that installation has been completed.
6. Turn off your PC.
7. Install the nShield Solo PCI-E card in your PC.

   Note: Consult the hardware installation manual prior to installing the HSM in the system on which ActivID KMS is installed.

8. To prepare for configuring nCipher Security World, perform the following tasks:
   a. Set the HSM to its pre-initialization state by setting the Mode switch to I (see the rear panel for switch settings).
   b. Start the KMS workstation.
9. Launch the KeySafe utility, which displays the following message after receiving the first request to run the software.

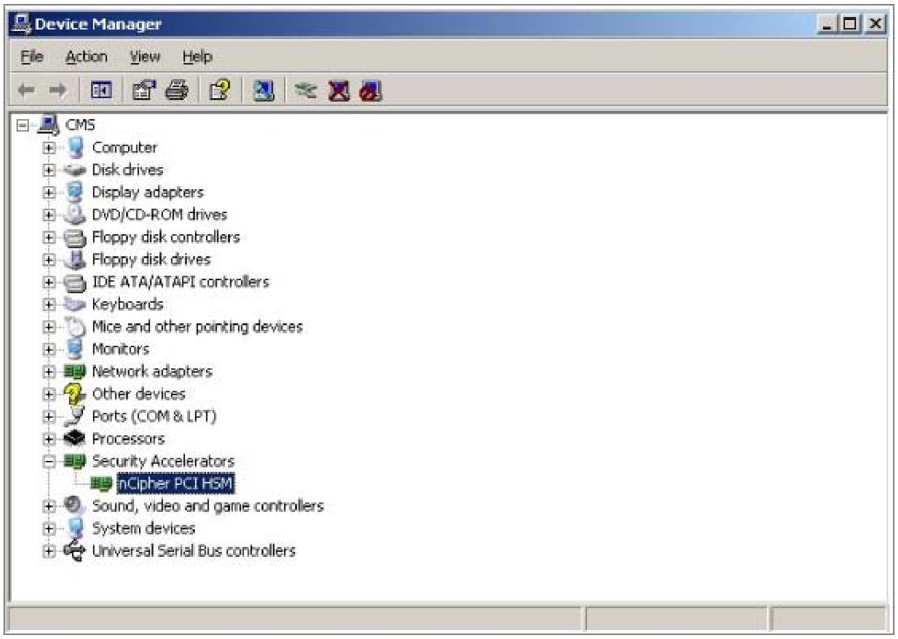


Fatal Error

Unable to establish KeySafe session. Please ensure that the hardserver is running and accepting TCP connections by assigning values to 'nonpriv_port' and 'priv_port' in the 'config' file.

10. Click **Press** to exit.
11. Navigate to the **C:\ProgramData\nCipher\Key Management Data** directory, and then open the configuration file.
12. Uncomment the nonpriv_port and priv_port lines in the **server_startup** section.
13. Edit the lines to reflect the values of nonpriv_port=9000 and privport=9001 so that the KeySafe utility can start.
14. Reboot the system after updating the configuration file.

Note: The device should now appear in Device Manager, and the nFast server service should be running (see the following illustration that shows the Device Manager window).



2.2 Procedure 2: Configuring the nCipher Security World

Security World is an nCipher proprietary concept. Each Security World is comprised of an HSM unit and smart cards:

- ACS (the Administrator Card Set), which contain credentials for managing a specific Security World and to use for recovery operations.

- OCS (the Operator Card Set), which control access to the Application Keys (for example, ActivID KMS and ActivID CMS).

Each Security World also includes keys and certificates that are encrypted by the Security World Key and stored on the computer where the Security World has been created (in the **C:\ProgramData\nCipher\Key Management Data** directory).

Notes:

- Each Security World is stored in a different subdirectory (kmdata_nn). Before you can use a Security World HSM with ActivID KMS, you must configure the Security World on the HSM. Key materials are stored in the nCipher Security World.
- During the HSM cloning process using ActivID KMS, the Security World is also cloned onto other HSMs.

There are two procedures for creating a new Security World:

- Procedure 1: Creating a New Security World/Administrator Card Set
- Procedure 2: Creating a New Operator Card Set

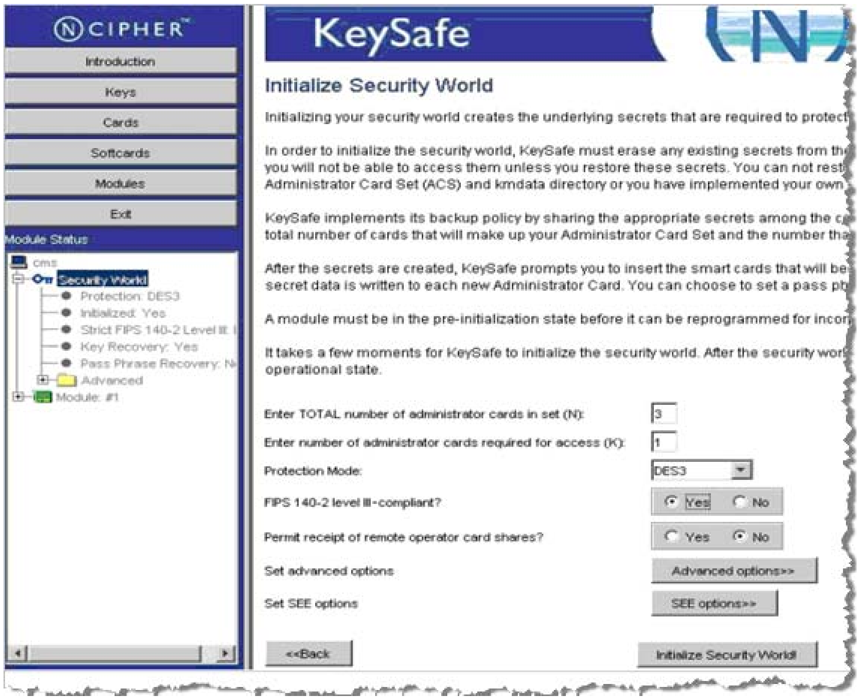
2.2.1 Procedure 1: Creating a New Security World/Administrator Card Set

To create a new Security World, you must use the nCipher KeySafe utility and complete the following steps.

WARNING: ActivID CMS only supports a value of K=1; other values do not work.

1. Set the HSM to its pre-initialization state. For a PCI-E HSM, you must manually set the Mode switch on the PCI card to (I).
2. Turn your PC On.
3. Launch the nCipher KeySafe utility.
4. Click **Modules** to display the Initialize Security World page.

   The following illustration is an example of Security World configuration for multiple administrators.



Initialize Security World

Initializing your security world creates the underlying secrets that are required to protect

In order to initialize the security world, KeySafe must erase any existing secrets from th
you will not be able to access them unless you restore these secrets. You can not rest
Administrator Card Set (ACS) and kmdata directory or you have implemented your own

KeySafe implements its backup policy by sharing the appropriate secrets among the c
total number of cards that will make up your Administrator Card Set and the number tha

After the secrets are created, KeySafe prompts you to insert the smart cards that will be
secret data is written to each new Administrator Card. You can choose to set a pass ph

A module must be in the pre-initialization state before it can be reprogrammed for incor

It takes a few moments for KeySafe to initialize the security world. After the security wor
operational state.

Enter TOTAL number of administrator cards in set (N): 3

Enter number of administrator cards required for access (K): 1

Protection Mode: DES3

FIPS 140-2 level III-compliant? ● Yes ○ No

Permit receipt of remote operator card shares? ○ Yes ● No

Set advanced options Advanced options>>

Set SEE options SEE options>>

<<Back Initialize Security World!

5. Respond to the parameter prompts to configure your Security World. Perform the following steps.

   a. Enter a value in the **Enter TOTAL number of administrator cards in set (N)**: text box (in this example, N=3).

   b. Enter a value in the **Enter number of administrator cards required for access (K)**: text box (in this example, K=1).

   c. Select either **AES** or **DES3** from the **Protection Mode** drop-down menu. The mode you choose selects the algorithm that will be used to protect the Security World keys.

   Note: The example illustrates the number of administrator cards (ACS: Administrator Card Set) as 3/1 (N/K), which allows multiple administrators to perform administrative tasks.

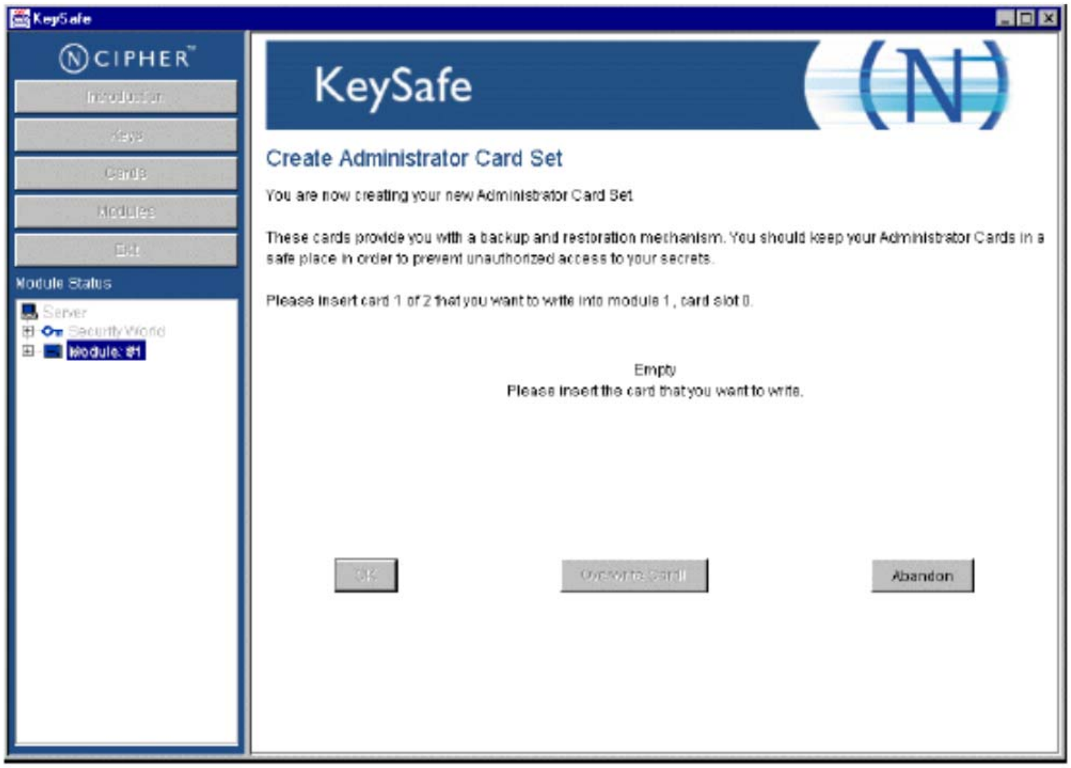
6. Select the **FIPS 140-2 level III-compliant** option (**Yes** or **No**), which sets the security level (FIPS 140-2 or FIPS 140-3) that is applicable for your HSM. This security level only applies to the Security World to be created and does not define the security level that the HSM physically supports.

7. Accept the default **No** option for the Permit receipt of remote operator card shares prompt.

   Important:

   - Do not select the **Advanced** options (the Set advanced options setting is not required at this time).
   - Do not select the **SEE** options (the Set SEE options setting is not required for the HSM to work in the ActivID CMS environment; SEE refers to Secure Engine Execution).

8. Click **Initialize Security World**. You will be prompted to insert your administrator card.



Create Administrator Card Set

You are now creating your new Administrator Card Set.

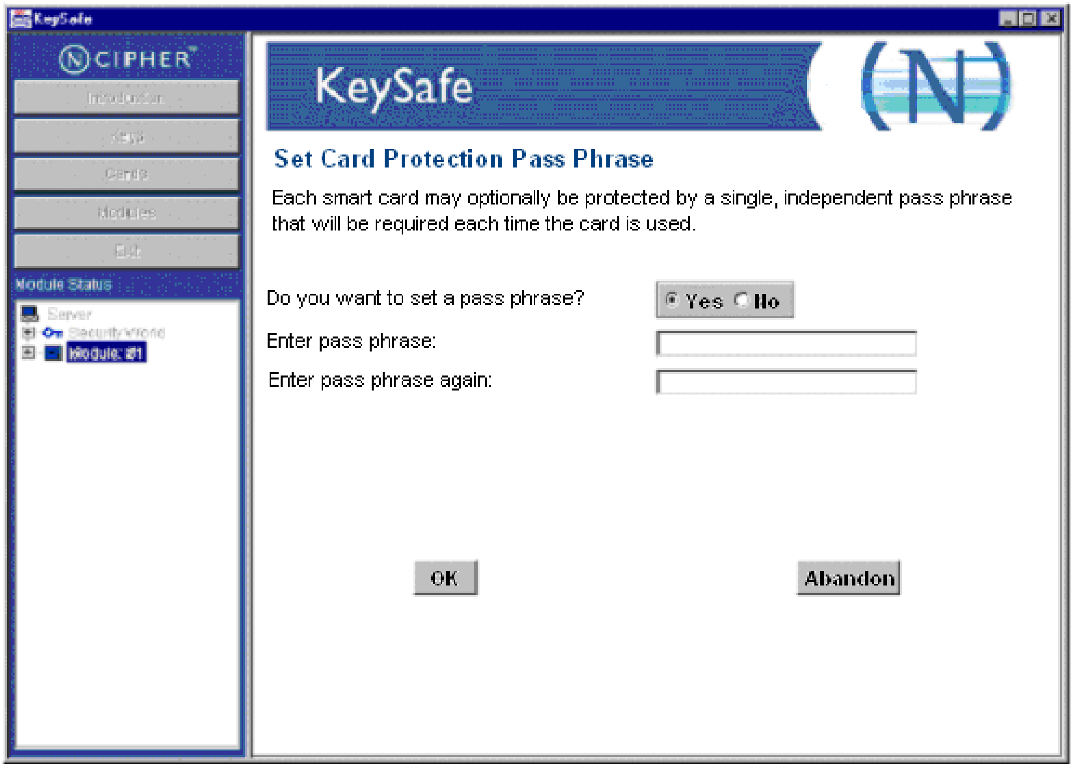
These cards provide you with a backup and restoration mechanism. You should keep your Administrator Cards in a safe place in order to prevent unauthorized access to your secrets.

Please insert card 1 of 2 that you want to write into module 1, card slot 0.

Empty
Please insert the card that you want to write.

9. Insert the first of the N administrator cards (in the example N=3).

   KeySafe displays a page where you can set a pass phrase (PIN) that protects the card using a single, independent pass phrase that is required each time the card is used.



Set Card Protection Pass Phrase

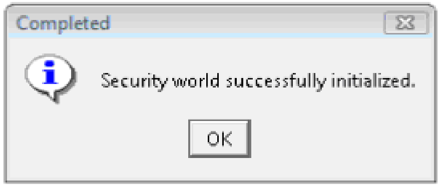
Each smart card may optionally be protected by a single, independent pass phrase that will be required each time the card is used.

Do you want to set a pass phrase? ● Yes ○ No

Enter pass phrase:

Enter pass phrase again:

10. Select Yes to set a pass phrase.
11. Enter and confirm a pass phrase, and then click OK.
12. Repeat this procedure to configure the second and third smart cards. When the Security World has been initialized, the following confirmation message is displayed.



Security world successfully initialized.

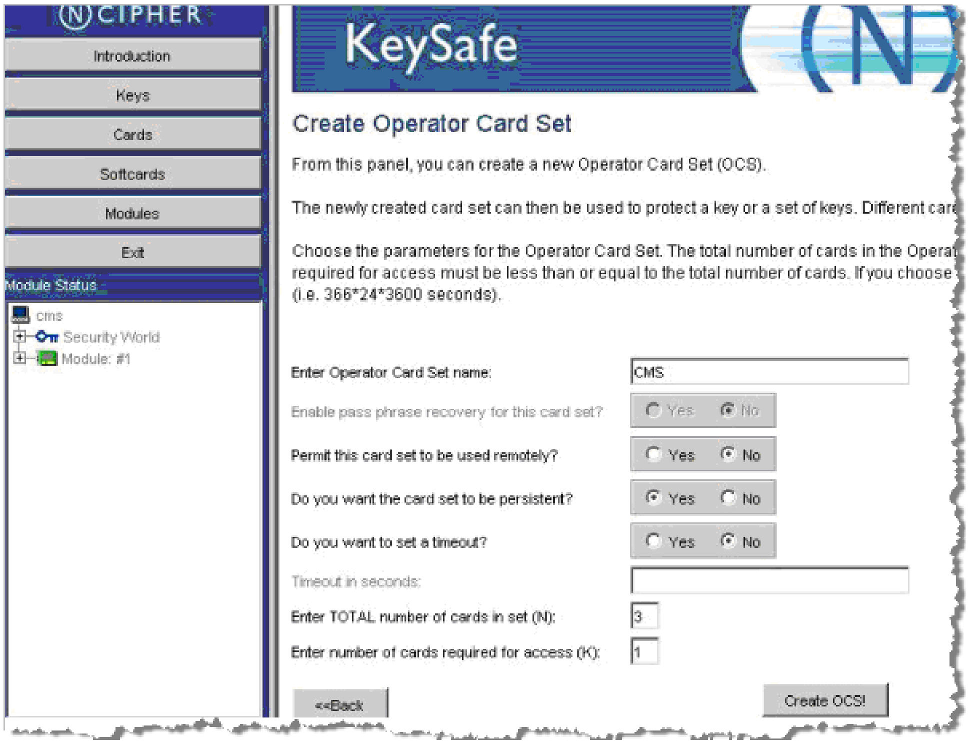
13. Click OK.
14. Set the HSM back to Operational (O) mode using the Mode switch on the back panel, and then reboot your system.
15. Launch KeySafe and verify that the HSM can be contacted, and that the Security World has been created (you should see an entry corresponding to the new Security World).

2.2.2 Procedure 2: Creating a New Operator Card Set

To create an Operator Card Set to protect access to the ActivID CMS keys, complete the following steps.

1. Launch KeySafe.

2. Click **Cards**.
3. Click **Create New OCS**, which displays the Create Operator Card Set window.



Create Operator Card Set

From this panel, you can create a new Operator Card Set (OCS).

The newly created card set can then be used to protect a key or a set of keys. Different car

Choose the parameters for the Operator Card Set. The total number of cards in the Operat required for access must be less than or equal to the total number of cards. If you choose (i.e. 366*24*3600 seconds).

Enter Operator Card Set name: CMS

Enable pass phrase recovery for this card set? ○ Yes ● No

Permit this card set to be used remotely? ○ Yes ● No

Do you want the card set to be persistent? ● Yes ○ No

Do you want to set a timeout? ○ Yes ● No

Timeout in seconds:

Enter TOTAL number of cards in set (N): 3

Enter number of cards required for access (K): 1

4. Respond to the parameter prompts to configure your Security World. Perform the following tasks.

   a. Enter a new card set name (for example, CMS) in the **Operator Card Set name** field.

   b. Select **No** for the **Permit this card to be used remotely** option.

   c. Select **Yes** for the **Do you want the card set to be persistent** option. When you click **Yes** to have the card set to be persistent, the keys protected by an OCS card remain available in the module even if the card is removed from the nCipher card reader.

      Important: It is recommended that you set this option, which enables several applications to access the HSM at the same time without forcing multiple operators to insert their cards during a session.

   d. Click **No** for the **Do you want to set a timeout** option (if you choose to set a timeout, this value cannot exceed one year in length).

   e. Enter a value for the total number of cards in the set (**N**). The total number of cards in the OCS cannot exceed 64.

   f. Enter the number of cards required for access (**K**). The number of cards required for access must be less than or equal to the total number of cards in use.

      WARNING: As per nCipher Security World requirements, if you cannot present the proper number of cards (K/N) if and when required, then the keys that are protected using that card may be unusable. As previously described in the Administrator Card

Sets, the total number of cards in an ACS set is (N) and the number of administrator cards required for access is (K). This formula is the same for an Operator Card Set.

5. Click **Create OCS**. You will be prompted to set card protection, just as when you created pass phrases for N cards for the ACS (as done previously when you set the pass phrase).
6. When prompted, enter and confirm a pass phrase (equivalent to HSM Operator PIN) for all the cards.

When you have finished creating the Operator Card Set, the HSM is ready for use in ActivID KMS and ActivID CMS.

3.0 Accessing the nShield Solo from ActivID KMS/CMS

This section provides a brief description of the process by which you prepare the nShield Solo HSM for use with ActivID KMS and with ActivID CMS.

3.1 Preparing the nShield Solo for Use with ActivID KMS

As described in previous sections, an nShield Solo HSM is installed on the system where ActivID KMS is installed. Following best practices, the ActivID KMS and ActivID CMS are installed and running on different systems.

For specific details on preparing the HSM for use with ActivID KMS, refer to the ActivID KMS technical documentation set for more information (this technical note is not intended to replace the ActivID KMS documentation). The following steps summarize the preparation process.

1. Copy the PKCS #11 *cknfast-64.dll* file to the ActivID KMS directory.

   The *cknfast-64.dll* file is located in the <installdir>\nCipher\nfast\toolkits\pkcs11\ directory.

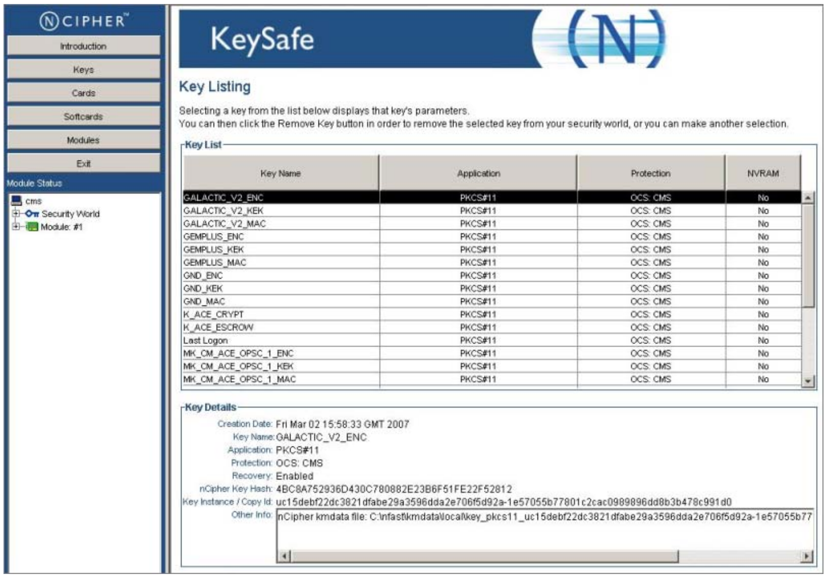
2. Make sure that the *cknfastrc* configuration file (located in <installdir>\nCipher\nfast\cknfastrc) contains only the following two lines:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=tokenkeys;unwrap_mech;unwrap_kek;explicitness
CKNFAST_NO_ACCELERATOR_SLOTS=1
```

   Note: All keys injected using ActivID KMS are located in the Security World you created previously using the directions in this technical note. You can view the key labels and attributes using ActivID KMS or by using the KeySafe utility (illustrated in the following figure).

   Important: If you are migrating from a HSM containing extractable keys, you need to add the *longterm* flag to *CKNFAST_OVERRIDE_SECURITY_ASSURANCES* in the *cknfastrc* file. See also the *HID ActivID Credential Management System HSM Migration User Guide*.

3. Launch KeySafe.



Key Listing

Selecting a key from the list below displays that key's parameters.
You can then click the Remove Key button in order to remove the selected key from your security world, or you can make another selection.

Key List

Key Name	Application	Protection	NVRAM
GALACTIC_V2_ENC	PKCS#11	OCS: CMS	No
GALACTIC_V2_KEK	PKCS#11	OCS: CMS	No
GALACTIC_V2_MAC	PKCS#11	OCS: CMS	No
GEMPLUS_ENC	PKCS#11	OCS: CMS	No
GEMPLUS_KEK	PKCS#11	OCS: CMS	No
GEMPLUS_MAC	PKCS#11	OCS: CMS	No
GND_ENC	PKCS#11	OCS: CMS	No
GND_KEK	PKCS#11	OCS: CMS	No
GND_MAC	PKCS#11	OCS: CMS	No
K_ACE_CRYPT	PKCS#11	OCS: CMS	No
K_ACE_ESCROW	PKCS#11	OCS: CMS	No
Last Logon	PKCS#11	OCS: CMS	No
MK_CM_ACE_OPSC_1_ENC	PKCS#11	OCS: CMS	No
MK_CM_ACE_OPSC_1_KEK	PKCS#11	OCS: CMS	No
MK_CM_ACE_OPSC_1_MAC	PKCS#11	OCS: CMS	No

Key Details

Creation Date: Fri Mar 02 15:58:33 GMT 2007
Key Name: GALACTIC_V2_ENC
Application: PKCS#11
Protection: OCS: CMS
Recovery: Enabled
nCipher Key Hash: 4BC8A752936D430C780882E23B6F51FE22F52812
Key Instance / Copy Id: uc15debf22dc3821dfabe29a3596dda2e706f5d92a-1e57055b77801c2cac0989896dd8b3b478c991d0
Other Info: nCipher kmdata file: C:\nfast\kmdata\local\key_pkcs11_uc15debf22dc3821dfabe29a3596dda2e706f5d92a-1e57055b77

4. Click **Keys**, and then click **List Keys**.

3.2 Preparing the nShield Solo for Use with ActivID CMS

To install the HSM on the ActivID CMS server, perform the following steps:

1. Install the HSM and the nCipher software on the ActivID CMS server, but do not create the Security World. Instead, you must use the Security World created for the ActivID KMS system. To copy the Security World configuration to the ActivID CMS server, copy the **kmdata\local** directory from the ActivID KMS system to the same location on the ActivID CMS server.
2. Copy **<installdir>\nCipher\nFast\cknfastrc** to the same location on the ActivID CMS server.

   Note: You do not need to copy the file if ActivID CMS will be installed from scratch with HSM support. Instead, you just need to provide the right path during the ActivID CMS setup.

3. To enable any administrator to run KeySafe, in the **<installdir>\nCipher\nFast\kmdata\preload** directory, change the NTFS permissions to include modified rights for the local administrator group. The default user with permission to start KeySafe is limited to the user who installed it.

Important: Once ActivID CMS is installed, if the PKCS#11 library path is changed after upgrading the nCipher Security World software (for example, version 12.50 or higher), you must update the *crystoki.ini* file, found in **%PROGRAMDATA%\HID Global\Credential Management System\Shared Files**, as follows:

```
LibNT=C:/Program Files/nCipher/nfast/toolkits/pkcs11/cknfast.dll
```

4.0 Setting Up an nShield Connect

This section describes how to set up an nShield Connect (formerly netHSM) HSM for use with ActivID Key Management System (KMS) and ActivID Credential Management System (CMS).

Note: The guidelines in this section are based on a specific version of the nCipher products, using the nCipher terminology. Refer to the latest nCipher documentation concerning the specific product and version you are deploying.

4.1 Task 1: Installing the nCipher Software

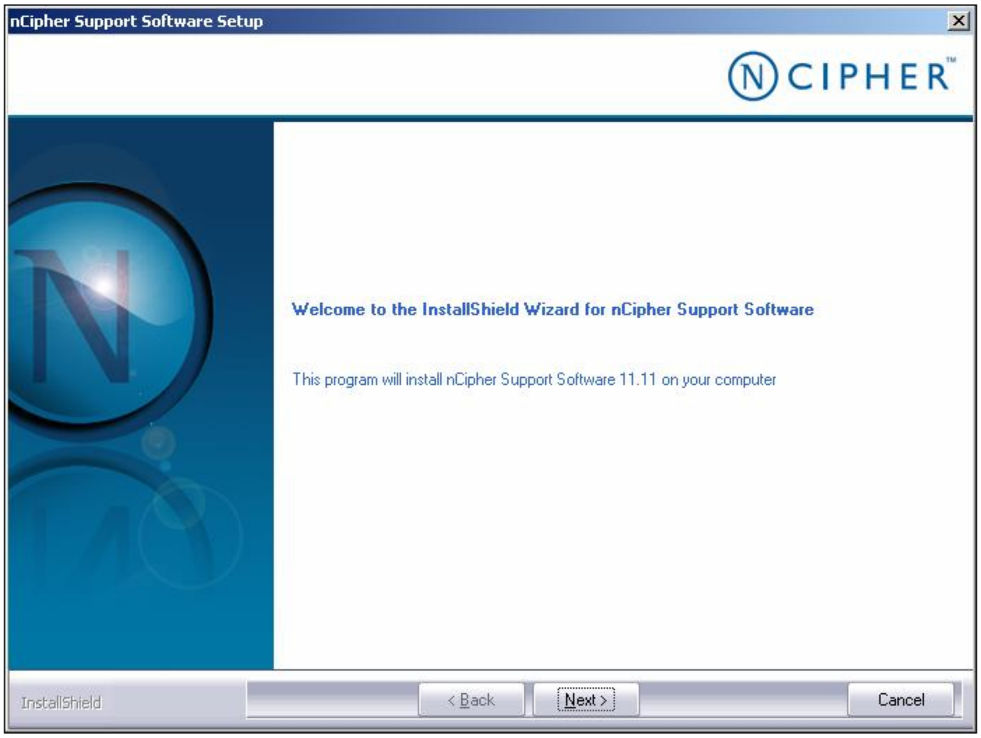
Prerequisites:

- You must install one of the following Java products prior to installing the nCipher components:
  - Java Runtime Environment (JRE)
  - Java Developer Kit (JDK)
- You must install the 64-bit version of the nCipher Security World software.

Note: ActivID CMS 5.0 and higher uses the 64-bit PKCS#11 library.

1. Connect the Ethernet cable to the nShield Connect unit (use the Ethernet port 1 or 2).
2. Insert the nCipher software installation CD into your system.

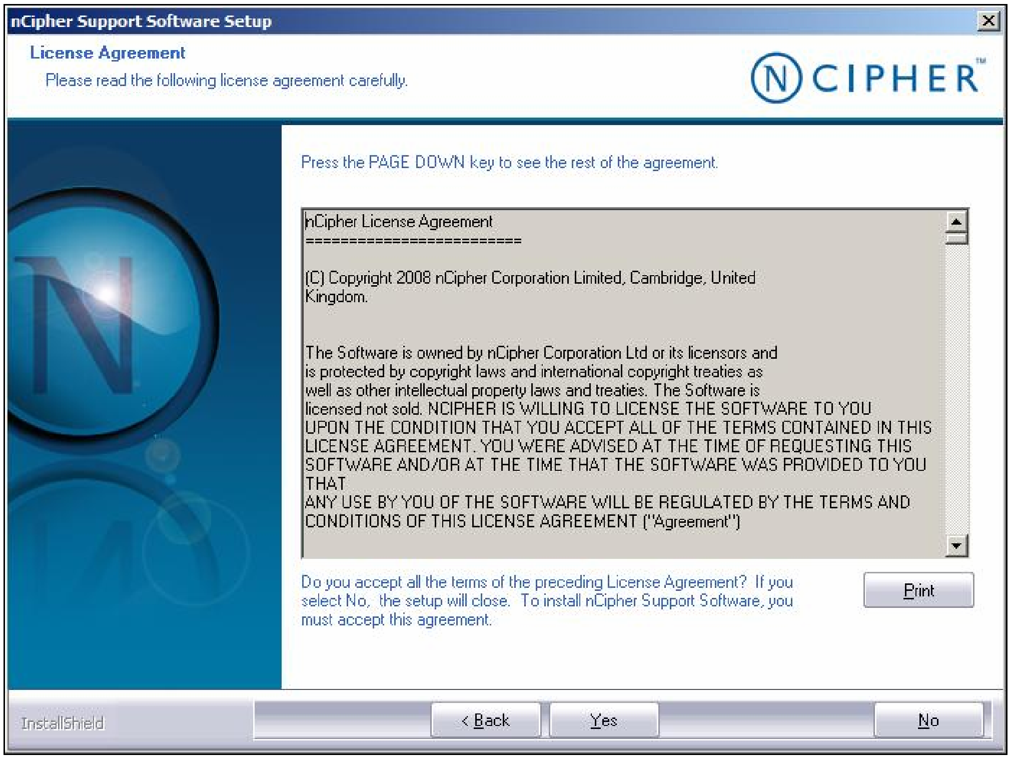
   If the installation utility does not start automatically, you can double-click the *Setup.exe* file to start it.



Welcome to the InstallShield Wizard for nCipher Support Software

This program will install nCipher Support Software 11.11 on your computer

3. When the Welcome window is displayed, click **Next**.



License Agreement

Please read the following license agreement carefully.

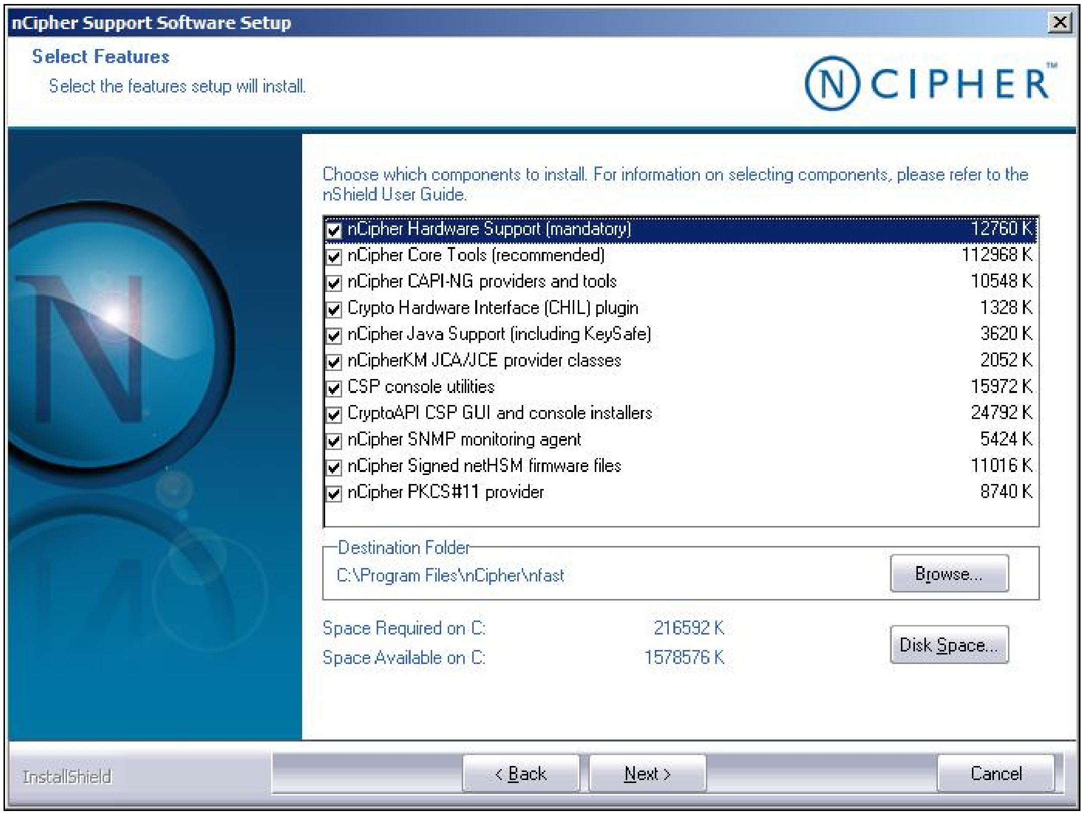
Press the PAGE DOWN key to see the rest of the agreement.

```
nCipher License Agreement
=========================

(C) Copyright 2008 nCipher Corporation Limited, Cambridge, United
Kingdom.

The Software is owned by nCipher Corporation Ltd or its licensors and
is protected by copyright laws and international copyright treaties as
well as other intellectual property laws and treaties. The Software is
licensed not sold. NCIPHER IS WILLING TO LICENSE THE SOFTWARE TO YOU
UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS
LICENSE AGREEMENT. YOU WERE ADVISED AT THE TIME OF REQUESTING THIS
SOFTWARE AND/OR AT THE TIME THAT THE SOFTWARE WAS PROVIDED TO YOU
THAT
ANY USE BY YOU OF THE SOFTWARE WILL BE REGULATED BY THE TERMS AND
CONDITIONS OF THIS LICENSE AGREEMENT ("Agreement")
```

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install nCipher Support Software, you must accept this agreement.

4. Click **Yes** to accept the license agreement, and click **Next**.

Note: The remaining steps in this procedure are not intended to replace nCipher technical documentation. Read and review the nCipher material, follow the presented prompts, and note any additional tips documented here.



Select Features

Select the features setup will install.

Choose which components to install. For information on selecting components, please refer to the nShield User Guide.

☑ nCipher Hardware Support (mandatory)	12760 K
☑ nCipher Core Tools (recommended)	112968 K
☑ nCipher CAPI-NG providers and tools	10548 K
☑ Crypto Hardware Interface (CHIL) plugin	1328 K
☑ nCipher Java Support (including KeySafe)	3620 K
☑ nCipherKM JCA/JCE provider classes	2052 K
☑ CSP console utilities	15972 K
☑ CryptoAPI CSP GUI and console installers	24792 K
☑ nCipher SNMP monitoring agent	5424 K
☑ nCipher Signed netHSM firmware files	11016 K
☑ nCipher PKCS#11 provider	8740 K

Destination Folder

C:\Program Files\nCipher\nfast

Space Required on C: 216592 K

Space Available on C: 1578576 K

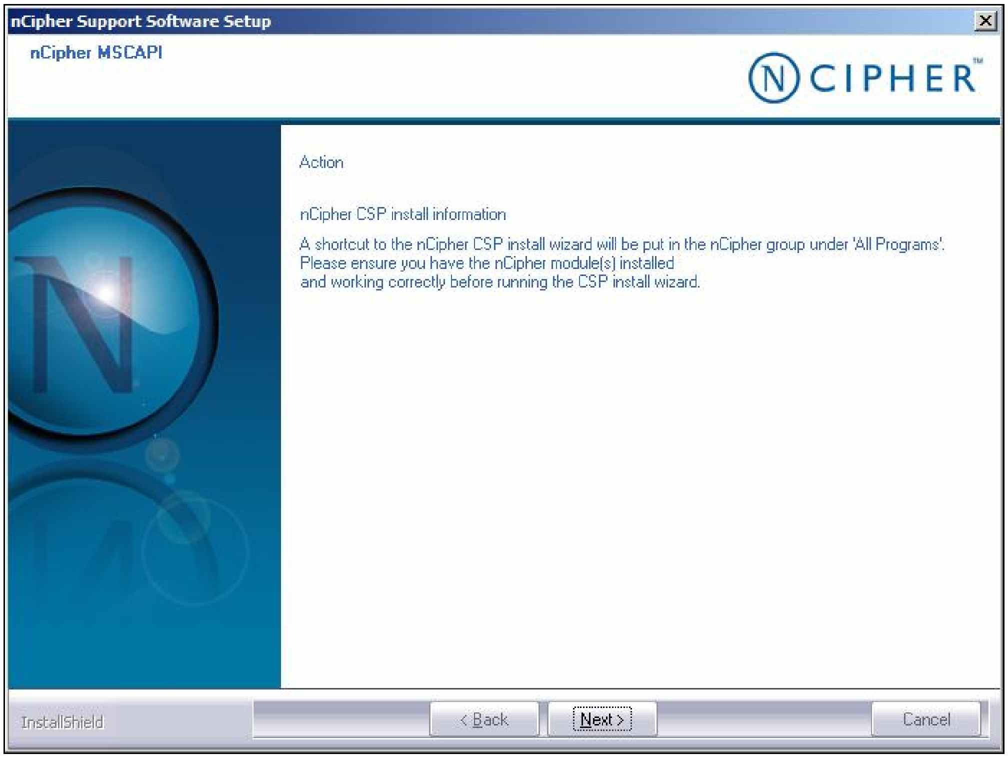
5. When the Select Features window displays, complete the following tasks:

   a. Accept the default options that are already selected.

   b. Accept the default installation directory.

   Important: It is strongly recommended that you accept the default installation directory. In this document, the installation directory is referred to as <installdir>.

   c. Click **Next**.

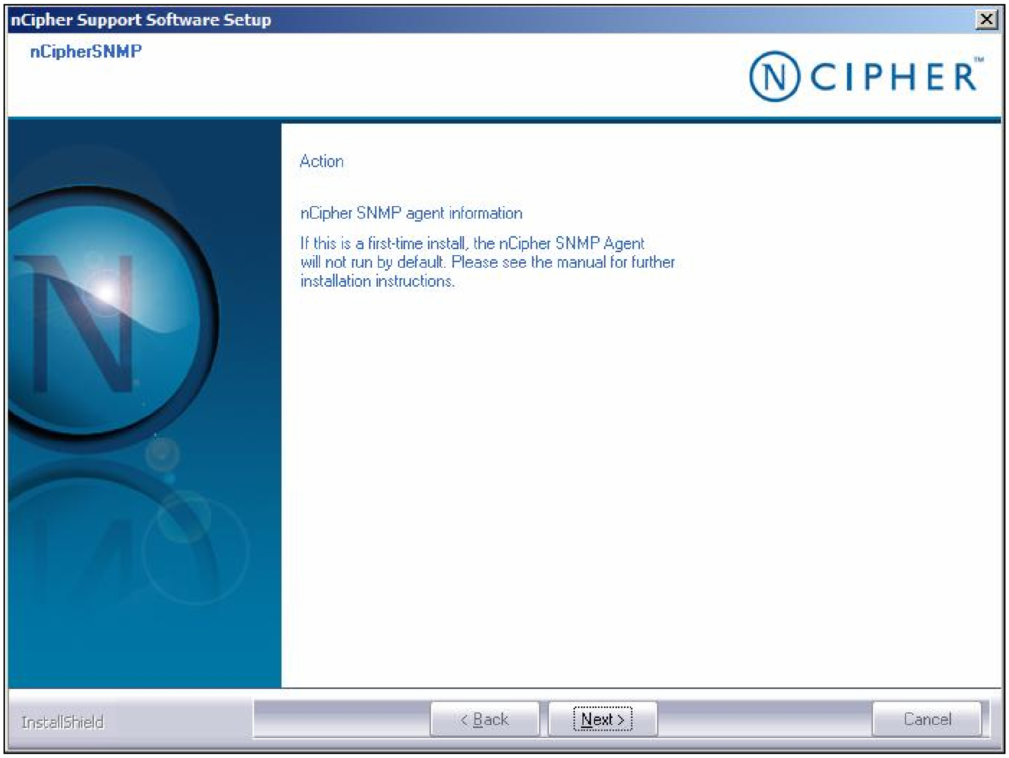


Action

nCipher CSP install information

A shortcut to the nCipher CSP install wizard will be put in the nCipher group under 'All Programs'.
Please ensure you have the nCipher module(s) installed
and working correctly before running the CSP install wizard.

6. Click **Next**.

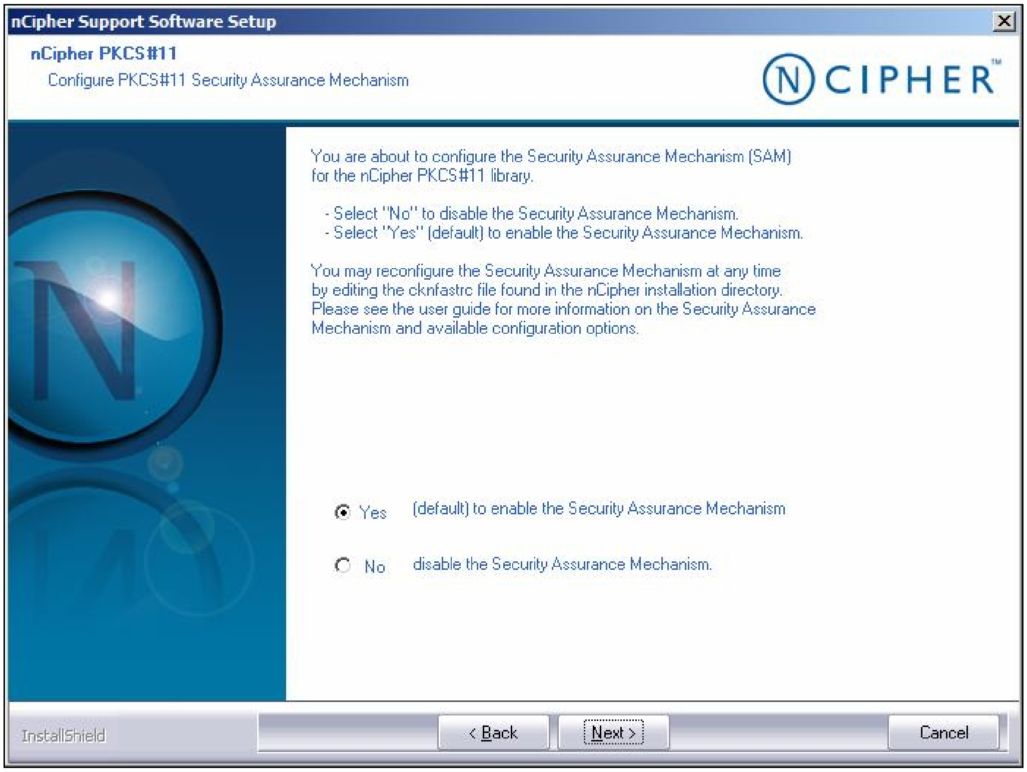


Action

nCipher SNMP agent information

If this is a first-time install, the nCipher SNMP Agent
will not run by default. Please see the manual for further
installation instructions.

7. Click **Next**.


nCipher Support Software Setup
nCipher PKCS#11
Configure PKCS#11 Security Assurance Mechanism
NCIPHER™
InstallShield
< Back
Next >
Cancel

You are about to configure the Security Assurance Mechanism (SAM) for the nCipher PKCS#11 library.

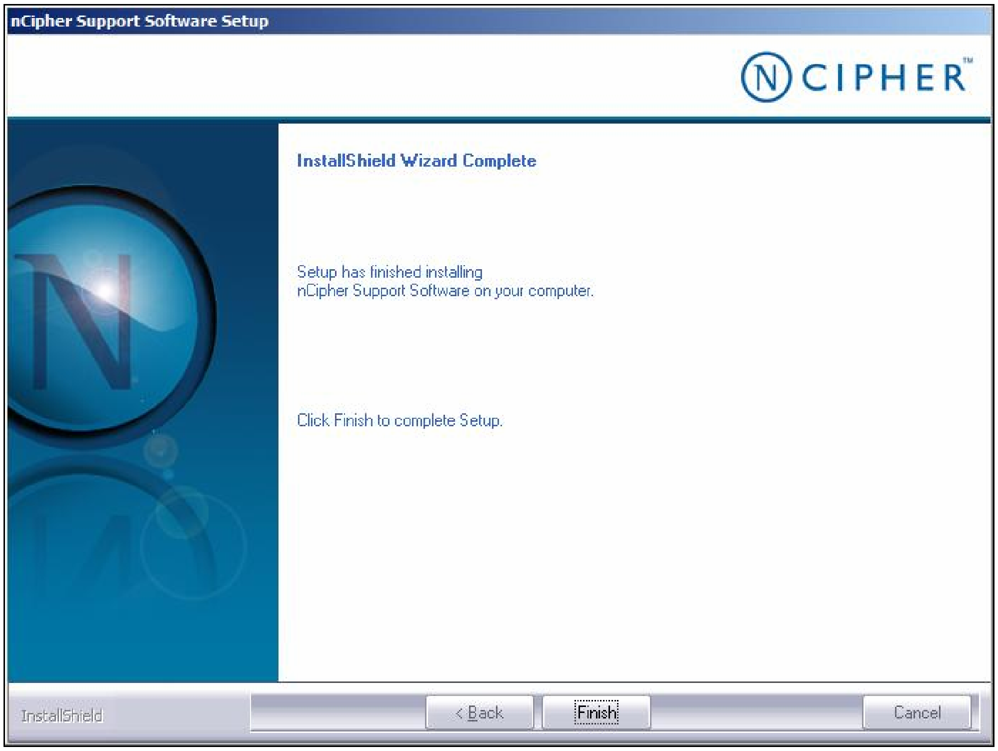
- Select "No" to disable the Security Assurance Mechanism.
- Select "Yes" (default) to enable the Security Assurance Mechanism.

You may reconfigure the Security Assurance Mechanism at any time by editing the cknfastrc file found in the nCipher installation directory. Please see the user guide for more information on the Security Assurance Mechanism and available configuration options.

● Yes (default) to enable the Security Assurance Mechanism

○ No disable the Security Assurance Mechanism.

8. Select **Yes** to enable the Security Assurance Mechanism, and then click **Next**.
9. In the nCipher PKCS#11 window, complete the following tasks:
   a. Click **Yes** to enable the Security Assurance Mechanism (which is the default).
   b. Click **Next** to display the Installation Completed message.


nCipher Support Software Setup

InstallShield Wizard Complete

Setup has finished installing
nCipher Support Software on your computer.

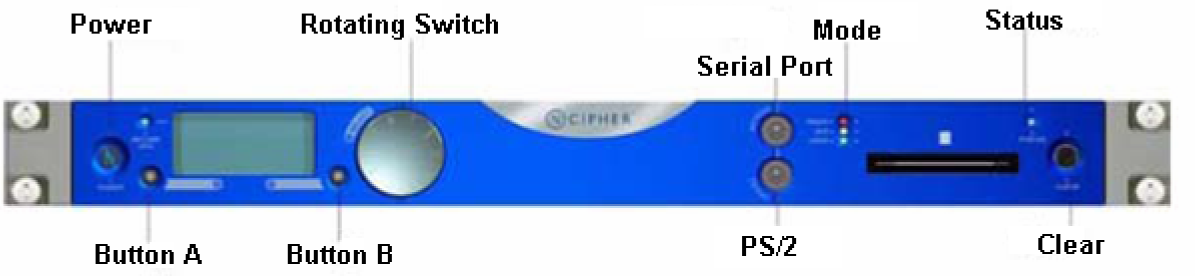
Click Finish to complete Setup.

10. Click **Finish** when the Installation Completed message displays.

4.2 Task 2: Configuring the HSM Ethernet Port

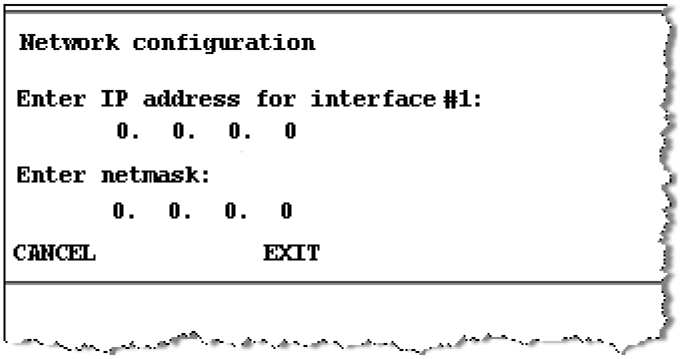
The first step in configuring an HSM Ethernet port is to assign it an IP address. Configure the HSM Ethernet port by completing the following steps.

Figure 2: nShield Connect Front Panel



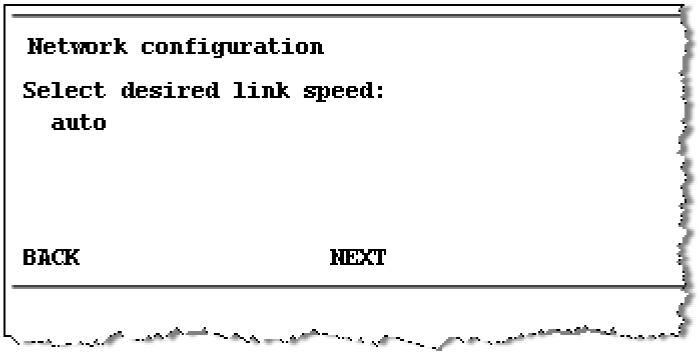
1. Using buttons A and B and the Rotating Switch on the nShield Connect front panel, complete the following tasks to display the following screen:
   a. Press Button B to select **System**
   b. Press Button B to select **System configuration**
   c. Press Button B to select **Network configuration**

d. Press Button B to select Set up interface #1



```
Network configuration

Enter IP address for interface #1:
       0.  0.  0.  0

Enter netmask:
       0.  0.  0.  0

CANCEL           EXIT
```

2. Set each field of the IP address and netmask for the interface.
3. Press button B when the settings are correct, which displays the following screen:



```
Network configuration
Select desired link speed:
  auto



BACK                 NEXT
```

Note: nCipher recommends that you use the auto option which configures your network speed for automatic negotiation.

4. When prompted, press button B to accept the new interface.
5. When prompted to reboot now or later, press button A to select a later reboot or press button B to reboot now.

Note: Repeat this series of steps to configure the second Ethernet interface (Interface #2).

4.3 Task 3: Configuring a Remote File System

The Remote File System (RFS) contains a copy of the Security World data which serves as a backup. For details about creating an nCipher Security World, see Task 6: Configuring an nCipher Security World. The RFS needs to be located on a separate server or on a client system (running either ActivID KMS or ActivID CMS). You must execute KeySafe from the system where the RFS is created.

You must repeat the same procedure performed in Task 1 on the server where the RFS resides (see Task 1: Installing the nCipher Software for details). The Task 1 procedure installs the nCipher software environment and the utility necessary to create the RFS.

Notes:

- There is one RFS for each HSM unit. In the following example, the command set enables several clients to connect to the HSM (where the client can be the system running ActivID KMS or ActivID CMS). The RFS configuration accepts access by cooperating client machines, where the client can either be authenticated or non-authenticated.
- In the following example, there are references to KNETI, which is the nCipher integrity key of the HSM (installed when the HSM is shipped). This is the key used for authentication between the HSM and clients.

The first step in the following procedure involves making a choice between the following two options:

- Option 1: For an Authenticated Client with KNETI Authorization (authenticated client)
- Option 2: For an Unauthenticated Client without KNETI Authorization.(unauthenticated client)

Determine which option you plan to use and select either Option 1 or Option 2.

4.3.1 Option 1: For an Authenticated Client with KNETI Authorization

Option 1 enables the client to connect to the RFS with KNETI authorization.

Note: If necessary, in the following commands and examples, replace C:\Program Files with your nCipher installation directory.

On the server system, enter the following command:

```
C:\Program Files\nCipher\nfast\bin>rfs-setup --force --gang-client <IP CLIENT> <netHSM ESN> <netHSM KNETI HASH>
```

The IP address identified as IP CLIENT is the IP address for the client system connected to the HSM, for example:

```
C:\Program Files\nCipher\nfast\bin>rfs-setup --force --gang-client 192.168.5.170 683E-33D9-2AF5 95a316146da7d9feb1fb0258746baed9990776c7
```

The result:

```
Removing old remote_file_system entries with remote_esn 683E-33D9-2AF5
Adding read-only remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local exists
Adding new writable remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local\sync-store exists
```

```
Saving the new config file and configuring the hardserver
Done
```

4.3.2 Option 2: For an Unauthenticated Client without KNETI Authorization.

Option 2 enables the client to connect to the RFS without KNETI authorization (use this option if you trust the current network environment).

Note: If necessary, in the following commands and examples, replace `C:\Program Files` with your nCipher installation directory.

On the server system, enter the following command:

```
C:\Program Files\nCipher\nfast\bin>rfs-setup --gang-client --write-noauth <IP CLIENT>
```

For example:

```
C:\Program Files\nCipher\nfast\bin>rfs-setup --gang-client -write-noauth 192.168.5.170
```

The result:

```
Adding read-only remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local exists
Adding new writable remote_file_system entries
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local\sync-store exists
Saving the new config file and configuring the hardserver
Done
```

Important: You must repeat one of the two options listed for step 1 in the procedure for each client involved.

1. Synchronize the client(s).

   You must synchronize the kmdata between the cooperating client and the RFS. The rfs-sync command is sent each time that a client is initialized so that it retrieves data from the RFS. The synchronization is executed from each client involved.

   Note: The following example, for an unauthenticated client, is provided for illustration purposes only.

   On each client system, enter the following command:

   ```
   C:\Program Files\nCipher\nfast\bin>rfs-sync --setup --no-authenticate < File Server IP>
   ```

The File Server IP represents the IP address for the server system where the RFS resides, for example:

```
C:\Program Files\nCipher\nfast\bin>rfs-sync --setup --no-authenticate 192.168.5.93
```

The result:

```
No current RFS synchronization configuration.
Configuration successfully written; new config details:
Using RFS at 192.168.5.93:9004: not authenticating.
```

2. To display the configuration summary, enter the following command:

```
C:\Program Files\nCipher\nfast\bin>rfs-sync -show
```

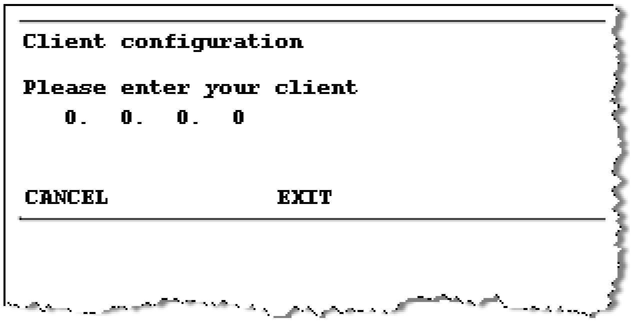
The result:

```
Using RFS at 192.168.5.93:9004: not authenticating.
```

4.4 Task 4: Configuring HSM to Work with a Client System

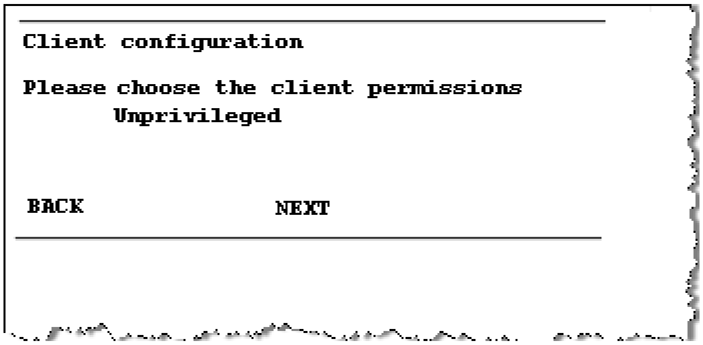
Connecting with the client is done using Ethernet (port 1 or 2) and depends upon the port to which you connected with the HSM (in the following example, port 1 is used). Configure HSM to work with a client system by completing the following steps:

1. Using buttons A and B and the Rotating Switch on the nCipher front panel menu (see Figure 2: nShield Connect Front Panel), complete the following tasks:
   a. Press Button B to select **System**
   b. Press Button B to select **System Configuration**
   c. Scroll down using the Rotating Switch and press Button B to select **Client Configuration**
   d. Press Button B to select **New Client**



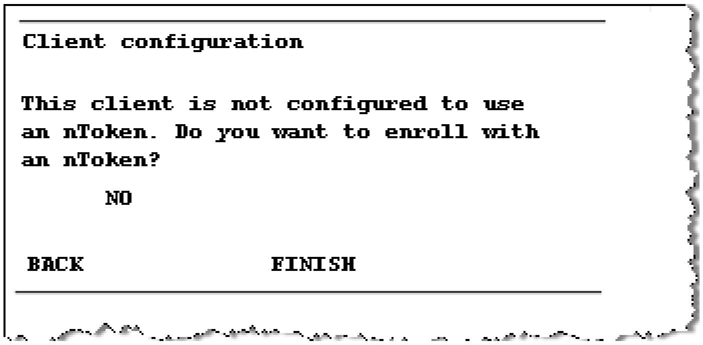
```
Client configuration

Please enter your client
   0.  0.  0.  0


CANCEL              EXIT
```

2. Enter the IP address for the client using the dotted decimal notation format.
3. Press Button B to display Client permissions.



```
Client configuration

Please choose the client permissions
      Unprivileged


BACK                 NEXT
```

4. Using the Rotating Switch, select **privileged** on any port for the client.
5. Press Button B to display the following message.



```
Client configuration


This client is not configured to use
an nToken. Do you want to enroll with
an nToken?

      NO

BACK                 FINISH
```

6. Using the Rotating Switch, select NO to indicate that you do not want to enroll using the nToken.

   Selecting this option means that the client is enrolled without nToken authentication.
7. When **Finish** is displayed, press Button B to end this operation.
8. Repeat this series of steps for each client that is involved.

4.5 Task 5: Configuring the Client System to Access the HSM

To establish a connection with the HSM from the client system, perform the following steps in this procedure.

Note:

- You must configure each client individually to use the nShield Connect.
- Before attempting client configuration, you must first obtain the following information from the nShield Connect front panel:
  - ESN (Electronic Serial Number)
  - HSM IP address
  - Hash of the KNETI key (nCipher integrity key)

The ESN and hash of the KNETI key are also readable from the nCipher *anonkneti* utility in <installdir>\nCipher\nfast\bin\. From this directory, you must enter the following command:

```
anonkneti – <netHSM IP>
```

Note: If necessary, in the following commands and examples, replace `C:\Program Files` with your nCipher installation directory.

1. On the client system, open a DOS command prompt window, and enter the following commands:

```
C:\Program Files\nCipher\nfast\bin>nethsmenroll --force -p <netHSM IP> <netHSM ESN> <netHSM KNETI
HASH>
```

   Important: You must enter two (2) dashes (**--**) with the force option as shown in the following example (in **bold**):

```
C:\Program Files\nCipher\nfast\bin> nethsmenroll --force -p 192.168.5.100 683E-33D9-
2AF5 95a316146da7d9feb1fb0258746baed9990776c7
```

2. Enable the TCP socket for Java and KeySafe by entering the following command:

```
C:\Program Files\nCipher\nfast\bin\config-serverstartup -sp
```

3. Stop the hardServer on the client by entering the following command:

```
C:\Program Files\nCipher\nfast\bin\net stop "nfast server"
```

   Note: The hardServer is the nCipher software that controls communication between the hardware and the applications running on the client system. "nfast server" represents the name of the server.

4. Restart the hardServer by entering the following command:

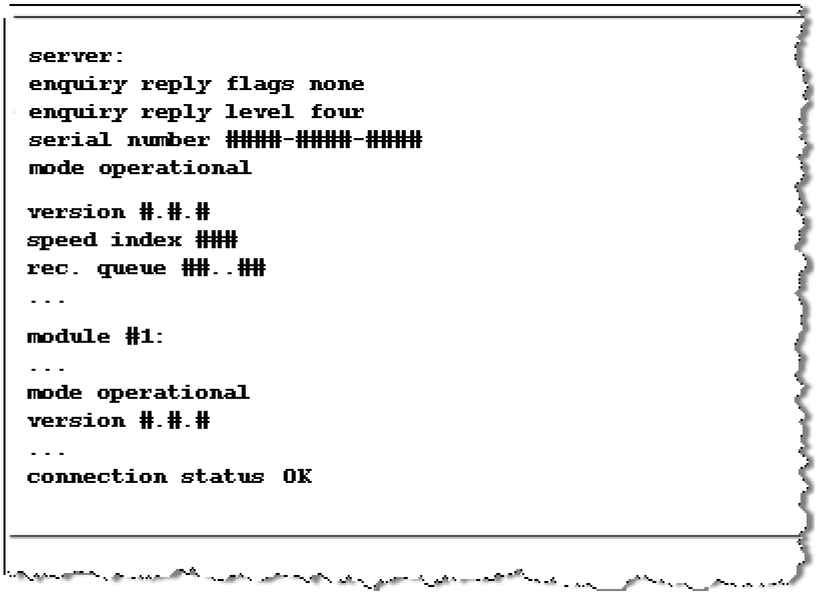
```
C:\Program Files\nCipher\nfast\bin\net start "nfast server"
```

5. Verify that you can launch the KeySafe utility.

   Note: Repeat the previous steps for each client system with which you intend to connect to the HSM.

6. Confirm that the HSM and Client connection is working by opening a DOS command prompt window and entering the following command:

```
C:\Program Files\nCipher\nfast\bin>enquiry
```



```
server:
enquiry reply flags none
enquiry reply level four
serial number #####-#####-#####
mode operational

version #.#.#
speed index ####
rec. queue ##..##
...
module #1:
...
mode operational
version #.#.#
...
connection status OK
```

In response to the enquiry request, the Connection Status for the module must return an OK response to indicate there has been a successful installation. If any errors occur, please see the nCipher technical documentation for details and more information.

4.6 Task 6: Configuring an nCipher Security World

Security World is an nCipher proprietary concept. Each Security World is comprised of an HSM unit and the following two sets of smart cards:

- ACS (the Administrator Card Set): this contains credentials for managing a specific Security World and for use with recovery operations.
- OCS (the Operator Card Set): this controls access to the Application Keys (for example, for applications such as ActivID KMS and ActivID CMS).

Each Security World also includes the keys and certificates that are encrypted by the Security World Key and stored on the computer where the Security World has been created (in the C:\ProgramData\nCipher\Key Management Data\ directory).

Notes:

- Each Security World is stored in a different subdirectory (kmdata_nn). Before you can use a Security World HSM with ActivID KMS, you must first configure the Security World on the HSM. Key materials are stored in the nCipher Security World.
- During the HSM cloning process using ActivID KMS, the Security World is also cloned onto other HSMs.

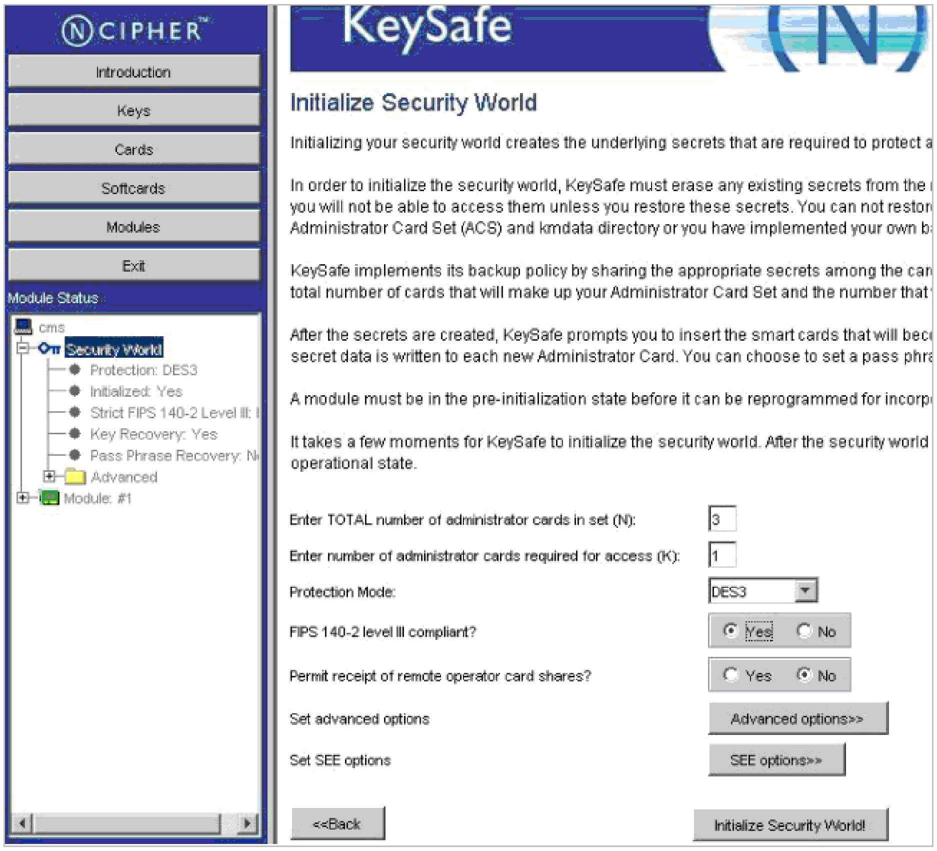
The following are the two procedures for creating a new Security World:

- Creating a new Security World and Administrator Card Set
- Creating a new Operator Card Set

4.6.1 Creating a New Security World and Administrator Card Set

To create a new Security World, you must use the nCipher KeySafe. Perform the following steps to create a new Security World.

1. Turn on your PC system and launch the nCipher KeySafe utility.
2. Click **Modules** to display the Initialize Security World page.



cms
Security World
Protection: DES3
Initialized: Yes
Strict FIPS 140-2 Level III:
Key Recovery: Yes
Pass Phrase Recovery: N
Advanced
Module: #1

Initialize Security World

Initializing your security world creates the underlying secrets that are required to protect a

In order to initialize the security world, KeySafe must erase any existing secrets from the
you will not be able to access them unless you restore these secrets. You can not restor
Administrator Card Set (ACS) and kmdata directory or you have implemented your own b

KeySafe implements its backup policy by sharing the appropriate secrets among the car
total number of cards that will make up your Administrator Card Set and the number that

After the secrets are created, KeySafe prompts you to insert the smart cards that will bec
secret data is written to each new Administrator Card. You can choose to set a pass phra

A module must be in the pre-initialization state before it can be reprogrammed for incorp

It takes a few moments for KeySafe to initialize the security world. After the security world
operational state.

Enter TOTAL number of administrator cards in set (N): 3

Enter number of administrator cards required for access (K): 1

Protection Mode: DES3

FIPS 140-2 level III compliant? ● Yes ○ No

Permit receipt of remote operator card shares? ○ Yes ● No

Set advanced options

Set SEE options

Note: In this Initialize Security World page example, the number of defined administrator cards in set (N) is 3 and the number of defined administrator cards for access (K) is 1. For example, this combination of N and K card settings allows multiple administrators to perform administrative tasks.

3. Enter the appropriate values for your Security World by completing the following tasks in the Initialize Security World page:
   a. Enter the number of cards in the **Enter Total Number of administrator cards in set (N)** text box; in this example, it is 3 (N=3).
   b. Enter the number of cards in the **Enter number of administrator cards required for access (K)** text box; in this example, it is 1 (K=1).

c. Click to select **AES** (Advanced Encryption Standard) or DES3 (Triple Data Encryption Standard) in the **Protection Mode** pull-down menu. The mode you select determines the algorithm used to protect the keys in the Security World Key.

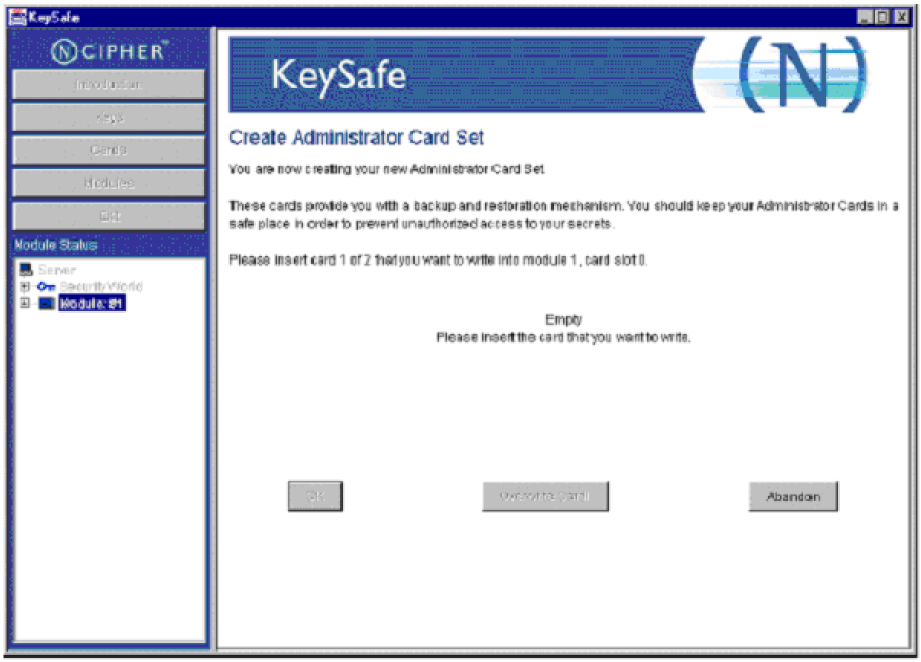
d. Click to select **Yes** or **No** from the **FIPS 140-2 level III compliant** options. The security level you select is applicable to your HSM and only applies to the Security World being created. This security level has nothing to do with the security level that the HSM physically supports.

e. Click to select **Yes** or **No** from the **Permit receipt of remote operator card shares** options. It is recommended that you accept the **No** option (which is the default).

f. No selection is required at this time for the **Set advanced options**.

g. No selection is required at this time for the **Set SEE options**. SEE refers to Secure Engine Execution. This setting is not required for the HSM to work in the ActivID KMS / CMS environment.

h. Click **Initialize Security World** to display the Create Administrator Card Set page.



Create Administrator Card Set

You are now creating your new Administrator Card Set

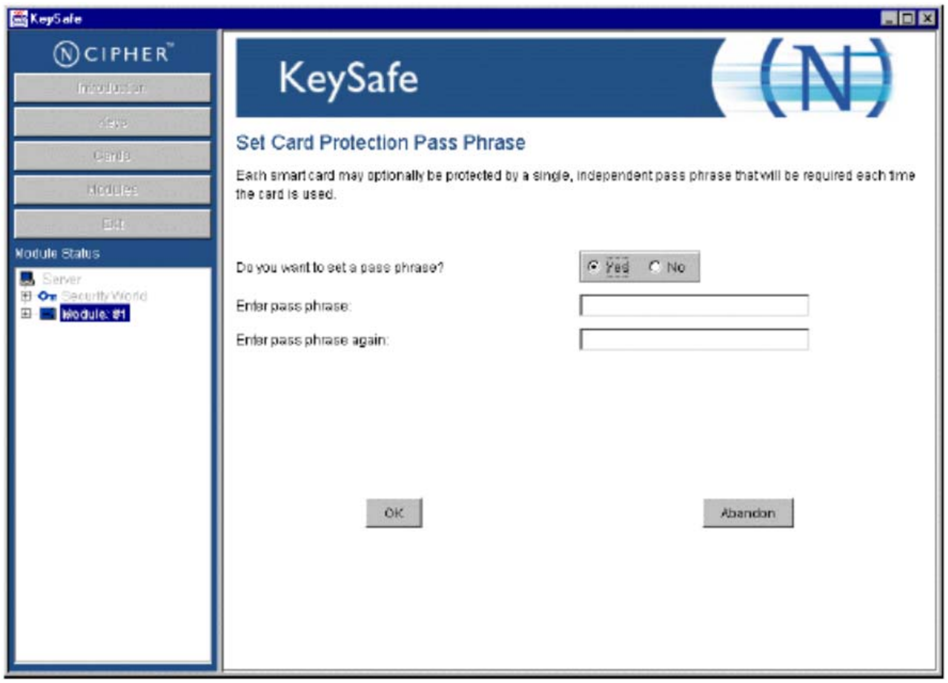
These cards provide you with a backup and restoration mechanism. You should keep your Administrator Cards in a safe place in order to prevent unauthorized access to your secrets.

Please insert card 1 of 2 that you want to write into module 1, card slot 0.

Empty
Please insert the card that you want to write.

4. Insert the first of the N set of administrator cards (in the example N=3), which displays the Set Card Protection Pass Phrase page.

   KeySafe displays a page where you set a pass phrase (PIN) to protect the card with a single, independent pass phrase that is required each time that the card is used.



Set Card Protection Pass Phrase

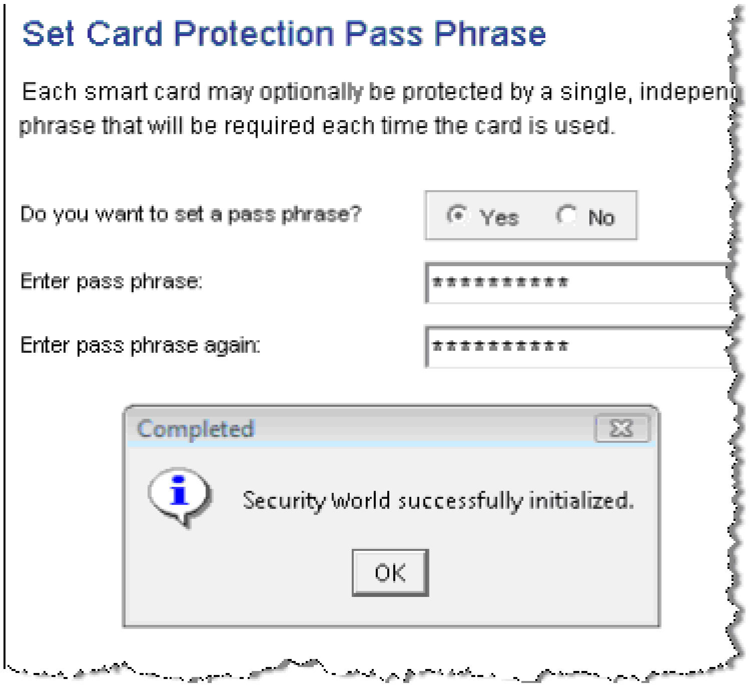
Each smart card may optionally be protected by a single, independent pass phrase that will be required each time the card is used.

Do you want to set a pass phrase? ● Yes ○ No

Enter pass phrase:

Enter pass phrase again:

5. In the Set Card Protection Pass Phrase page, perform the following tasks:
   a. Click to select the **Yes** option.
   b. Enter the pass phrase (PIN) in the **Enter pass phrase** text box.
   c. Enter the pass phrase again to confirm it in the **Enter pass phrase again** text box.
   d. Click **OK**.
6. Repeat this same procedure for the second and third set of smart cards. When the Security World has been created, the following message window displays.



Set Card Protection Pass Phrase

Each smart card may optionally be protected by a single, indepen
phrase that will be required each time the card is used.

Do you want to set a pass phrase? ● Yes ○ No

Enter pass phrase: **********

Enter pass phrase again: **********

Completed

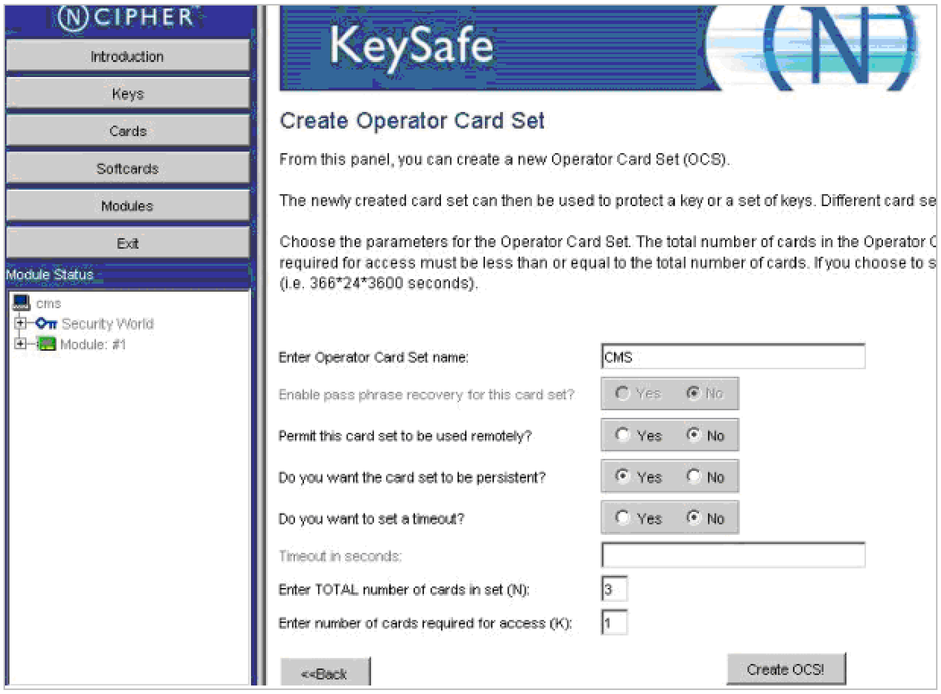
Security World successfully initialized.

7. In the Security World successfully initialized window, click **OK**.
8. Reboot your client system.
9. Launch *KeySafe* and verify that the HSM can be contacted and the Security World has been created (you should see an entry corresponding to the new Security World).

4.6.2 Creating a New Operator Card Set

Complete the following procedure to create an Operator Card Set that protects access to the ActivID CMS keys. To create a new operator card set, complete the following tasks.

1. Launch *KeySafe*.
2. Click **Cards**.
3. Click **Create New OCS** which displays the Create Operator Card Set page.



Create Operator Card Set

From this panel, you can create a new Operator Card Set (OCS).

The newly created card set can then be used to protect a key or a set of keys. Different card se

Choose the parameters for the Operator Card Set. The total number of cards in the Operator C required for access must be less than or equal to the total number of cards. If you choose to s (i.e. 366*24*3600 seconds).

Enter Operator Card Set name:	CMS
Enable pass phrase recovery for this card set?	○ Yes ● No
Permit this card set to be used remotely?	○ Yes ● No
Do you want the card set to be persistent?	● Yes ○ No
Do you want to set a timeout?	○ Yes ● No
Timeout in seconds:	
Enter TOTAL number of cards in set (N):	3
Enter number of cards required for access (K):	1

<<Back Create OCS!

4. Enter the appropriate values for your Operator Card Set by responding to the parameter and prompts and completing the following tasks in this page:

   a. Enter a new card set name (for example, CMS) in the **Enter Operator Card Set name** text box.

   b. Click the **No** option from the **Permit this card to be used remotely** option choices.

   c. Click the **Yes** option from the **Do you want the card set to be persistent** option choices.

      When you click **Yes** for persistent, the keys protected by an OCS card remain available in the module even if the card is removed from the nCipher card reader (It is recommended that you use this option). This mode enables multiple applications to access the HSM simultaneously without requiring multiple operators to insert their cards during a session.

   d. Click to the **No** option from the **Do you want to set a timeout** option choices. If you choose to set a timeout period, this maximum duration cannot be longer than one year in length.

   e. Enter the number of cards in the **Enter Total Number of administrator cards in set (N)** text box (the total number cannot exceed 64).

   f. Enter the number of cards in the **Enter number of administrator cards required for access (K)** text box (the number of cards required for access must be less than or equal to the total number of cards).

WARNING: For an Administrator Card Set, the total number of cards is (N) and the number of administrator cards required for access is (K). This same formula applies for an Operator Card Set. As per nCipher Security World requirements, if you cannot present the proper number of cards (K/N) if and when required, the keys that are protected using this card may be unusable.

5. Click **Create OCS**.

   This window prompts you to set card protection similar to when you created pass phrases for N cards for the ACS (see step 5 in 4.6.1 for details).

   You need to enter a pass phrase (equivalent to an HSM Operator PIN), and enter a confirmation pass phrase for all the cards when prompted. When you are finished creating the Operator Card Set, the HSM is ready for use in ActivID KMS and ActivID CMS.

5.0 Accessing the nShield Connect from ActivID KMS/CMS

This section provides a brief description of the process by which you prepare the nShield Connect HSM for use with ActivID KMS and with ActivID CMS.

5.1 Preparing the nShield Connect for Use with ActivID KMS

The following procedure briefly summarizes the process of preparing the nShield Connect for use with ActivID KMS.

1. Copy the PKCS #11 *cknfast-64.dll* file to the ActivID KMS directory.

   The *cknfast-64.dll* file is located in the <installdir>\nCipher\nfast\toolkits\pkcs11\ directory.

2. Make sure that the *cknfastrc* configuration file (located in <installdir>\nCipher\nfast\cknfastrc) contains only the following two lines:

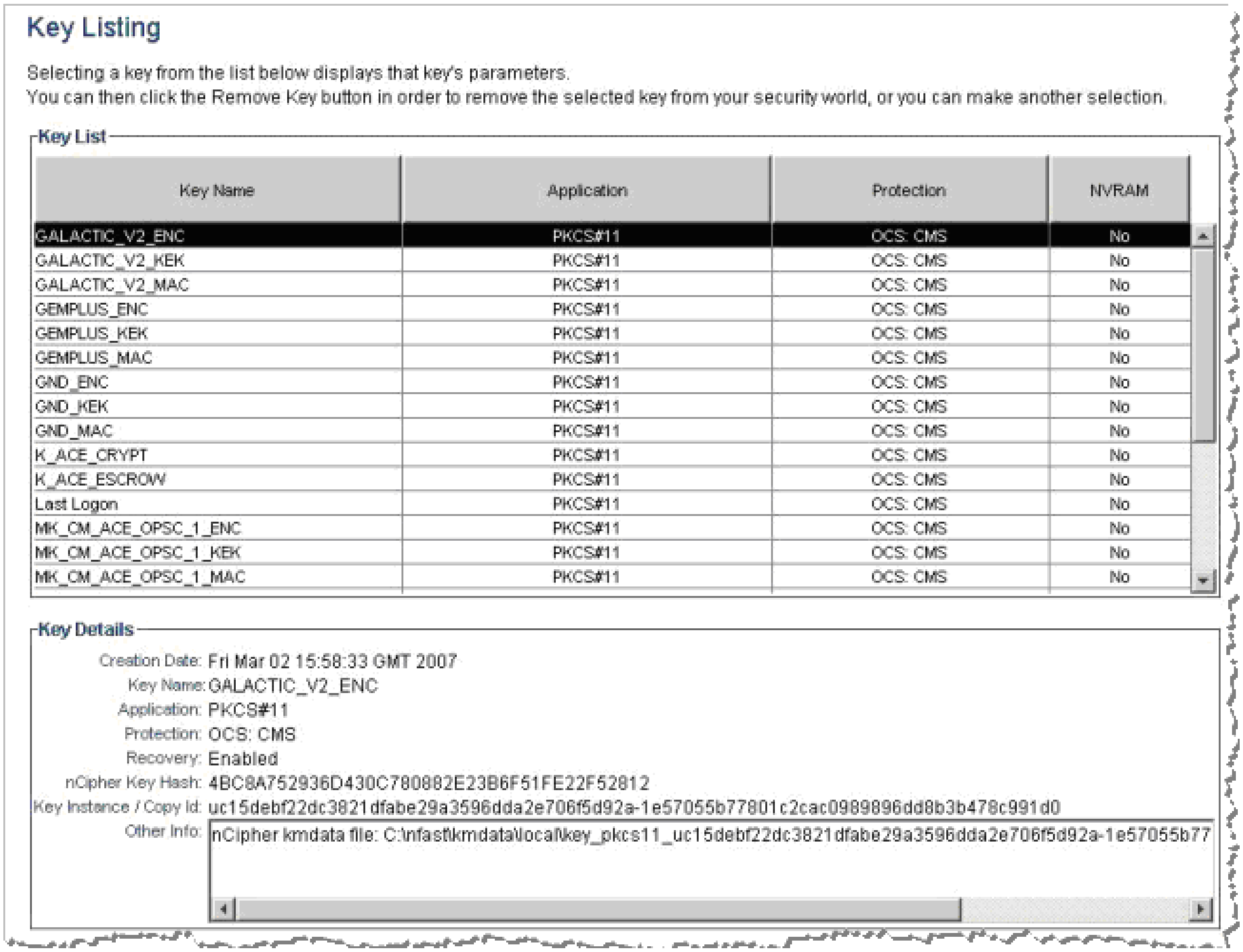
```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=tokenkeys;unwrap_mech;unwrap_kek;explicitness
CKNFAST_NO_ACCELERATOR_SLOTS=1
```

Note: All keys that are injected using ActivID KMS are located in the Security World created using the directions described in this technical note (see Task 6: Configuring an nCipher Security World). You can view the key labels and attributes using ActivID KMS or using the KeySafe utility (see next illustration).

Important: If you are migrating from a HSM containing extractable keys, you need to add the *longterm* flag to *CKNFAST_OVERRIDE_SECURITY_ASSURANCES* in the *cknfastrc* file. See also the *HID ActivID Credential Management System HSM Migration User Guide*.

3. Launch KeySafe.

4. Click **Keys** and click **List Keys** to display the Key Listing window.



Key Listing

Selecting a key from the list below displays that key's parameters.
You can then click the Remove Key button in order to remove the selected key from your security world, or you can make another selection.

Key List

Key Name	Application	Protection	NVRAM
GALACTIC_V2_ENC	PKCS#11	OCS: CMS	No
GALACTIC_V2_KEK	PKCS#11	OCS: CMS	No
GALACTIC_V2_MAC	PKCS#11	OCS: CMS	No
GEMPLUS_ENC	PKCS#11	OCS: CMS	No
GEMPLUS_KEK	PKCS#11	OCS: CMS	No
GEMPLUS_MAC	PKCS#11	OCS: CMS	No
GND_ENC	PKCS#11	OCS: CMS	No
GND_KEK	PKCS#11	OCS: CMS	No
GND_MAC	PKCS#11	OCS: CMS	No
K_ACE_CRYPT	PKCS#11	OCS: CMS	No
K_ACE_ESCROW	PKCS#11	OCS: CMS	No
Last Logon	PKCS#11	OCS: CMS	No
MK_CM_ACE_OPSC_1_ENC	PKCS#11	OCS: CMS	No
MK_CM_ACE_OPSC_1_KEK	PKCS#11	OCS: CMS	No
MK_CM_ACE_OPSC_1_MAC	PKCS#11	OCS: CMS	No

Key Details

Creation Date: Fri Mar 02 15:58:33 GMT 2007
Key Name: GALACTIC_V2_ENC
Application: PKCS#11
Protection: OCS: CMS
Recovery: Enabled
nCipher Key Hash: 4BC8A752936D430C780882E23B6F51FE22F52812
Key Instance / Copy Id: uc15debf22dc3821dfabe29a3596dda2e706f5d92a-1e57055b77801c2cac0989896dd8b3b478c991d0
Other Info: nCipher kmdata file: C:\nfast\kmdata\local\key_pkcs11_uc15debf22dc3821dfabe29a3596dda2e706f5d92a-1e57055b77

5.2 Preparing the nShield Connect for Use with ActivID CMS

The following procedure briefly summarizes the process of preparing the nShield Connect for use with ActivID CMS.

1. Copy **<installdir>\nCipher\nfast\cknfastrc** to the same location on the ActivID CMS server.

   Note: You do not need to copy the file if ActivID CMS will be installed from scratch with HSM support. Instead, you just need to provide the right path during the ActivID CMS setup.

2. Restart the ActivID CMS server.

Important: Once ActivID CMS is installed, if the PKCS#11 library path is changed after upgrading the nCipher Security World software (for example, version 12.50 or higher), you must update the *crystoki.ini* file, found in **%PROGRAMDATA%\HID Global\Credential Management System\Shared Files**, as follows:

```
LibNT=C:/Program Files/nCipher/nfast/toolkits/pkcs11/cknfast.dll
```

5.3 Accessing HSM Tokens from ActivID KMS/CMS

Depending upon how the nShield Connect HSM was configured, it may expose one or more HSM tokens to ActivID KMS and ActivID CMS.

5.3.1 Accessing HSM Tokens—ActivID KMS

ActivID KMS forces the operator to select the HSM token to use during an ActivID KMS session when there is more than one token available. If there is only a single HSM token, that token is automatically selected. Each HSM token is identified by a slot ID number as well as a token name. To identity an HSM token, ActivID KMS displays both the slot ID and token name for each HSM token.

Important: The slot ID cannot be used as the unique identifier for an HSM that manages several tokens because the HSM re-orders the slot ID depending on the availability of tokens.

5.3.2 Accessing HSM Tokens —ActivID CMS

To choose the correct token, configure an ActivID CMS file, which includes either the recorder slot ID or token name. For example, for ActivID CMS for Windows, perform the following steps:

1. Locate the *cmsslot.ini* file on the ActivID CMS distribution.
2. In the <CMS_distribution>\HSM folder:
   a. Copy the *cmsslot.ini* file to the Windows folder of your ActivID CMS server.
   b. In the cmsslot.ini file specify either a TokenName or a SlotID (if the cmsslot.ini file is not found, ActivID CMS chooses to connect to the slot that has the fewer number of sessions).

Note: If High Availability has been configured, the *cmsslot.ini* file must contain a reference to either a physical token or to a virtual token.

3. Locate the %PROGRAMDATA%\HID Global\Credential Management System\Local Files\pkcs11.cfg file and add the following line:

```
slot=xxxxxx
```

where *xxxxx* is the SlotID.

6.0 Troubleshooting

This section provides brief tips on how to start analyzing the nShield HSM configuration if you encounter issues or error conditions. If you do, then contact the HID Global or nCipher Technical Support Services and provide them with the appropriate information needed to start diagnosis or resolve the issue.

6.1 Checking the Module State

The enquiry utility returns information about the status of the HSM. This utility tool is located in the bin subdirectory of the nCipher directory (for example, <installdir>\nCipher\nFast\bin\enquiry.exe).

Check for any entry that starts with Mode, which indicates whether the module is currently in an operational state or is non-operational. If the module appears to be non-operational, you need to check the status LED on the PCI or PCIe card. If the Status LED is continuously on, then this indicates that the module is working properly. If the LED is either off, or if it flashes irregularly, then you must check the nCipher Hardware Installation.pdf on the nCipher Installation CD (refer to the section on Troubleshooting nCipher Modules for details).

6.2 About Log File

To activate the logs, refer to the *Appendix D* in the *nShield_Admin.pdf* on the nCipher Installation CD for details.

6.3 Insecure Key Used Too Long After Creation

If ActivID CMS fails to run at least two days or more after the HSM having been migrated to FIPS (for more details, see the *HID ActivID Credential Management System HSM Migration User Guide*), be sure to add the *longterm* flag to *CKNFAST_OVERRIDE_SECURITY_ASSURANCES* in the *cknfastrc* file. See also section 3.1 Preparing the nShield Solo for Use with ActivID KMS on page 20.

hidglobal.com