MyID

Version 11.4

Thales nShield HSM

Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: INT1970-05 November 2019

Copyright

Conventions Used in this Document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important
  - Bulleted lists are used when the order is unimportant or to show alternatives

- **Bold** is used for menu items and for labels.

  For example:
  - "Record a valid email address in **'From' email address**"
  - Select **Save** from the **File** menu

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and italic*** are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the installation media.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

Warning:	You must take a backup of your database before making any changes to it.

Contents

1 Introduction

This document provides a step-by-step guide to the configuration of MyID® to integrate with a Thales nShield Hardware Security Module (HSM).

Note: If you have an existing installation of MyID and intend to change the HSM used with it, or want to migrate MyID database keys from the server registry or smart card to an HSM, contact Intercede customer support for further information quoting reference SUP-41.

1.1 Supported nShield HSM models

nShield HSMs have two main types:

- **Acceleration-only modules** – (nFast series) these modules provide cryptographic acceleration only, and do not allow sensitive key data to be managed within the HSM. This type of module is typically used as an SSL accelerator, and may therefore improve IIS performance, but will not provide benefits to MyID itself.
- **Key-management modules** – (nShield series) these modules *in addition* to providing cryptographic acceleration, are able to store sensitive key data internally, providing assurance that these keys are more secure than if they were stored within the computer. It is this type of HSM that this document is relating to.

nShield HSMs are available as internal PCI card, an external SCSI device, or a network connected device that can support multiple clients (netHSM). All of these form factors are supported by MyID, but the details of installing and configuring the HSM may differ depending on the type of HSM used.

MyID supports the following nShield HSM models:

- nShield Connect
- nShield Solo

Each model is available in different performance variants. All variants are supported; however, for production use, you are recommended to use the variants with the highest performance rating.

MyID has been tested with the Thales nShield Connect 500+.

Note: The nShield Edge USB version of the HSM is compatible with MyID, but is not supported due to the low performance rating; it is not suitable for production environments.

1.2 Hardware and software requirements

The ***Installation and Configuration*** document contains details of the hardware and software required to support MyID. Any late changes to these requirements are provided in the ***Release Notes***.

Refer to your nShield HSM documentation for recommendations of the hardware and software needed for the nShield HSM.

Intercede recommends the use of nShield support software version 12.40.2 – this version of nShield software has been used to perform internal testing.

1.3 SHA256 support

MyID has been tested using SHA256 for the PIV server hash algorithm.

1.4 Limitations

Currently, you can not import or export AES192 keys encrypted by an AES transport key, or 3DES keys encrypted by an AES transport key. This is an issue with nShield firmware and will be addressed in a future firmware release.

As a workaround, for 3DES keys use another 3DES key as the transport key. For AES192 keys, either import into software rather than the HSM, or if possible use AES256 keys.

1.5 Multiple HSMs

MyID manages a connection to a single HSM. If you have more than one HSM set up for failover purposes, your HSM administrator must ensure that the data is synchronized between each HSM.

1.6 HSM Test Utility

A utility is provided with MyID to help confirm configuration with Hardware Security Modules (HSMs). This tool mimics the PKCS#11 transactions used by MyID and will exercise all functions of the HSM that MyID requires. You can use this utility to test cryptographic performance on the system; for example, to determine the optimum number of threads (concurrent operations) to achieve the best scalability for a given HSM.

You can find this utility in the `\Support Tools\HSM Integration\` folder on the MyID product media.

To set the number of HSM concurrent sessions, see the *HSM concurrency* section in the ***Installation and Configuration Guide***. This section also contains information on how to configure the number of retries for failed operations.

1.7 Change history

Version	Description
INT1970-01	Released with MyID 11.0.
INT1970-02	Released with MyID 11.1.
INT1970-03	Released with MyID 11.2.
INT1970-04	Released with MyID 11.3.
INT1970-05	Released with MyID 11.4.

2 Pre-Installation Requirements

2.1 Install HSM hardware and software

Follow the instructions that come with the nShield hardware to install the hardware and the software. The exact details of hardware installation will differ depending on the exact model of HSM.

The nShield support software must be installed on the MyID® application server.

2.1.1 Security Assurance Mechanism

If you enable the Security Assurance Mechanism, the HSM will disable any keys that were not generated on the HSM after 48 hours – this means that any factory keys that you import onto the HSM will be disabled.

When you install the nShield client software on the MyID application server, you are asked whether you want to enable the Security Assurance Mechanism. For MyID to operate correctly with the HSM, choose **No**.

Warning:	If you do not select **No** when prompted for the Security Assurance Mechanism, any imported factory keys expire after 48 hours.

If you have enabled the Security Assurance Mechanism, you must disable it.

To disable the Security Assurance Mechanism:

1. Open the `cknfastrc` file in the `nfast` directory.

   The `CKNFAST_OVERRIDE_SECURITY_ASSURANCES` setting determines whether the Security Assurance Mechanism is enabled or not.

   If the Security Assurance Mechanism is enabled, `cknfastrc` will contain the line:

   ```
   CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
   ```

2. To disable the Security Assurance Mechanism, change this line to:

   ```
   CKNFAST_OVERRIDE_SECURITY_ASSURANCES=all
   ```

3. Save the `cknfastrc` file.
4. Restart the MyID KeyServer.

2.2 Initialize the security world

The nShield HSMs implement a 'security world' – a set of rules that determine what operations can be performed on sensitive key data, and by whom. To initialize the security world the HSM must be re-initialized – when this is done, any old data that was previously encrypted under the old security world will be lost.

If the HSM is a netHSM, the security world should be set up using the menu system of the HSM itself. A PCI or SCSI HSM uses nShield's KeySafe program to initialize the security world.

During the initialization of the security world you will be prompted to decide whether to initialize the HSM in FIPS140-2 level 2 or level 3. Once the HSM has been initialized, you cannot change the FIPS140-2 mode between level 2 and level 3 – therefore, you must set this to the FIPS140-2 mode required when initializing the security world.

Some installations (for example, US government) may have a regulatory requirement to run the HSM in FIPS140-2 level 3 mode. The choice to run the HSM in FIPS140-2 level 3 is generally driven by regulatory compliance requirements.

A netHSM is capable of supporting many clients; if you are using a netHSM it is possible that the security world has already been initialized and that the HSM is already servicing existing applications or servers. In this case you would not want to re-initialize the security world since this would impact the existing applications.

2.2.1 What is FIPS140-2?

FIPS140-2 is an accreditation that provides assurance that a security device fulfils a set of requirements. A FIPS140-2 validated HSM both provides assurance of high security, and also regulatory requirement. It is possible that for certain applications adherence to a particular level of FIPS140-2 is a requirement.

FIPS140-2 level 2

Provided a FIPS-140-2 validated version of the firmware is running on the HSM, nShield HSM devices supported by MyID operate as a minimum in FIPS140-2 level 2 mode. This security accreditation ensures that the device follows a very stringent set of rules – that the device is physically secure and tamper-proof, that the rules which govern how keys can be created and used are secure, and that the hardware and software itself is well designed and robust.

FIPS140-2 level 3

This mode implements additional rules on top of FIPS140-2 level 2, such as stipulating that *no* private key can be exported (while in level 2 it is possible to specify on creation whether they can or cannot be exported), and requiring that additional administrator cardset authorization is required to generate or import new keys.

As stated in the nShield user guide, the FIPS140-2 level 3 does not provide additional security to the protection of the keys, but is instead intended to provide regulatory compliance. In this mode, some operations such as key generation or key import may require an additional 'FIPS authorization' to work. This means that an administrator or operator cardset must have been used to authorize the operation. In the case of MyID using module protected keys, this additional FIPS authorization can be performed through the nCipher KeySafe utility by selecting an operation such as key generation that prompts for a card to be inserted for FIPS authorization.

2.3 Configure remote file system / client connectivity

Note: This step applies only to netHSM. If you are not using a netHSM please skip this section.

The netHSM is capable of supporting multiple client computers at once. At least one of these client computers will be the MyID application server.

One computer on the network is designated the 'remote file system', and is used to store information used by the HSM. See the netHSM administrator guide that ships with the nShield HSM for instructions on configuring this. The 'Basic Software Setup' document that ships with the netHSM summarizes the steps required to configure this.

Once the MyID application server has been configured to connect to the HSM, verify the connectivity by running nShield's KeySafe program. Ensure that the module is listed, and its State is described as **Operational:Usable**. If the KeySafe program cannot communicate with the module, MyID will not be able to communicate with the module.

Note: You must have a 32-bit version of the Java Runtime Environment installed before you can install KeySafe; the KeySafe installation does not recognize a 64-bit JRE.

2.4 Levels of security offered by nShield HSM

The nShield HSM allows for a range of levels of security to protect its keys. For each key or application it is important to understand how best to protect the key.

2.4.1 Keys protected by module

In this configuration, the key is stored encrypted on the hard disk, encrypted by the module key. The key may be used at any time by any application on the computer hosting the HSM.

This configuration allows for maximum convenience, since applications using the key are not reliant on the status of the HSM smartcard reader. This is the recommended configuration for the MyID Application server.

If you have nCipher Load Sharing Mode enabled, the module slot will detect with a serial number of 'Load Balanced'.

Note: Load Sharing Mode is not enabled by default when the nShield software is installed. Load Sharing Mode is a software configuration that is *not* related to the initialization of the security world.

2.4.2 Keys protected by module and smartcard

In this configuration, the key is stored encrypted on the hard disk, encrypted by the module key, and an (operator card-set) smartcard that is configured to not require logon. The key may be used by any application on the computer hosting the HSM, but the card must be in the card reader. In the event of a reboot of the MyID application server, the operator card must be inserted into the HSM card reader.

2.4.3 Keys protected by module and smartcard with PIN

In this configuration, the key is stored encrypted on the hard disk, encrypted by the module key, and an (operator card-set) smartcard that is configured to require logon. The key may be used by any application on the computer hosting the HSM, but the card must be in the card reader, and the application must provide the correct PIN to the smartcard.

This configuration allows for maximum security, since user interaction is required to make the key available to the application. However, since user interaction (for instance after a reboot) is required, this may not be suitable if 24-7 availability is the prime goal.

Auto-startup will not be possible, since the PIN must be provided to the Keyserver when the server boots.

2.4.4 Keys protected by module and 'softcard'

'Softcard' is a feature introduced in nShield software version 10 and later. A PIN is required to authenticate to the HSM, but no smartcard is required.

Auto-startup will not be possible because the PIN must be provided to the Keyserver when the server boots.

For 'softcard' protection to be used, the nShield software installed on the MyID application server must have Load Sharing Mode enabled.

2.5 The role of the HSM card-reader

The nShield HSM has its own dedicated smartcard reader that plugs directly into the HSM. This reader may hold a single operator card at any one time.

Since MyID is designed to be a server application servicing multiple client workstations simultaneously it is important that it is not required that the card in the HSM card-reader is required to be swapped at any point, since it is likely the MyID server will be locked away in a server room, with the connecting clients having no access to the HSM card reader.

It is important to decide what applications the HSM is to be used for before setting up the system in order to plan for providing the appropriate level of protection to all keys.

Although the nShield hardware supports '*k* or *n*' cardset protection – i.e. k out of a possible n cards must be authenticated to in order to allow access to the key, MyID only supports '1 on *n*' cardsets – i.e. any one, out of a possible *n* cards must be authenticated to in order to allow access to the key.

Ultimately it is vital that *if* operator card sets are used, only a single operator card set is required for the operation of the entire MyID server, since it will not be possible to swap operator card sets on the server.

Note: It is suggested that for MyID, 'Module protection' (i.e. cards not required) may be the most suitable option, since this option is best for high availability, with automatic recovery and startup after a reboot.

2.5.1 Module or Card-set to protect Keyserver database key

MyID uses a secret key to protect sensitive data in the database, this key is called the Keyserver database key, and is managed by the nShield PKCS#11 library. This library allows for a mixture of keys to be cardset protected, and other keys to be module protected.

2.5.2 Module or Cardset to protect CSP keys

The nShield CSP is set as either cardset, or module protected at the point of installation.

If the CSP is card-set protected, then it is important that a '1 of *n*' card-set is used to protect the CSP, where the cards do not have PIN protection. For the CSP to operate one of the cards in the card-set must remain in the HSM card reader permanently. If the CSP is card-set protected, and it is also intended that the Keyserver database key is to be card-set protected, it is important that the same card-set is used to protect both sets of keys, in order that no card swaps are required.

If the CSP is module protected, then the HSM card-reader will not be required for CSP operation.

2.6 Install nShield CSP

The nShield CSP is installed once the security world has been initialized via an icon on the desktop.

Note: As MyID is a 32-bit application, you must run the 32-bit CSP Install Wizard.

Since the MyID server is designed to run as a background task with a minimum of administrator intervention, it is important that card swaps are not required on the HSM card-reader, and that no PIN prompts appear on the MyID Server. For this reason it is recommended that:

- If maximum availability is the prime goal, then module protection can be used instead of card protection. In this scenario cards are not required to be present in the HSM card-reader in order to access the keys.
- If Card-Protection is used for the HSM CSP, then a '*1 of n*' cardset is used with cards that are not PIN protected. One of these cards would then sit permanently in the HSM card-reader.
- If Card-Protection is used for the HSM CSP *and* for the Keyserver database key protection, then the same cardset is used to protect both the CSP and the keyserver database key. This will guarantee that no card-swaps are required on the HSM card-reader (which will be locked away in a server room).

The nShield CSP can be used for the following purposes:

- Protection of the Microsoft CA private key

  The Microsoft CA private key is used to sign every certificate, and CRL that is issued by the CA. In order to increase confidence that bogus certificates are not created, the CA private key can be stored within the hardware nShield CSP (as opposed to the default Microsoft software CSP.)

  This private key resides on the CA computer. In a distributed environment where the CA is not hosted on the MyID COM server, a separate HSM would be required (installed on the CA computer) to protect this key.

  Note that the Certificate Services Components must be installed *after* installation of the nShield CSP, so that the nShield CSP is available when configuring the certificate services.

- Protection of the Microsoft W2k3 CA Key Recovery Agent (KRA) private key

  This key is used to decrypt users' archived private keys. In order to enable private key recovery for users' certificates, a KRA certificate must be requested on the MyID COM server to enable decryption of the recovered keys. By default the Microsoft default (software) CSP is used to protect this private key. Additional security can be added by generating this private key within the hardware nShield CSP. In order to facilitate this, the certificate template that defines the KRA certificate must be edited to allow the nShield CSP to be used for this type of certificate (by default only the Microsoft Software CSPs are allowed for this certificate type.) For further instruction on requesting the KRA certificate see the ***Microsoft Windows CA Integration Guide***, supplied with MyID.

  This private key would reside in an HSM on the MyID Application Server (not the CA computer).

- Protection of any CSP protected X509 certificate's private key

  Any certificate that is requested for the nShield CSP will store the private key securely within the HSM.

When you are creating the required certificates, if you are duplicating existing certificates make sure of the following:

- Check all the settings. In particular, on the **Issuance Requirements** tab, make sure that you set the **Number of authorized signatures** to `1`, the **Policy type required in signature** option to **Application policy** and the **Application policy** option to **Certificate Request Agent**.

2.6.1 Using KSP instead of CSP

MyID can use the KSP instead of the CSP for server certificates. See the following documents for details of setting up server certificates:

- ***PIV Integration Guide*** (for PIV Content Signer Certificate)
- ***Microsoft Windows CA Integration Guide*** (for Enrollment Agent and KRA certificates)
- ***Mobile Identity Management Installation and Configuration Guide*** (for mobile badge layout content signer certificate)
- ***Smart Card Integration Guide*** (for OPACITY signing certificate)

  Note: You must configure the SafeNet KSP specifically for the MyID COM+ user account if the SafeNet KSP is to be used when issuing the CVC Signing Certificate for OPACITY.
- ***Administration Guide*** (for SCEP signing certificate)

2.7 Copy nShield PKCS#11 driver into System directory

On 32-bit operating systems, copy the `CknFast.DLL` file from the `Program Files\nCipher\bin` folder to the `Windows\System32` folder.

On 64-bit operating systems, copy the `CknFast.DLL` file from the `Program Files (x86)\nCipher\bin` folder to the `Windows\Syswow64`) folder.

If you do not carry out this step, you cannot use the HSM to initialize the Keyserver database key within the GenMaster application.

3 After Installing nShield

3.1 Check the NFAST_KMDATA environment variable

You must check the `NFAST_KMDATA` environment variable for the location of the expected security world files.

The default is:

```
C:\ProgramData\nCipher\Key Management Data
```

Note: `ProgramData` is a system protected hidden folder.

If you do not set this correctly, you see the following message in KeySafe:

```
Status:Operational:foreign
```

3.2 Check the PKCS11 interface to the HSM

After you have installed KeySafe, you can run the following at the command line to check the PKCS11 interface to the HSM:

```
cklist
```

If this operation works, the PKCS11 interface is operational and the HSM will be listed as a master key option when you install MyID.

3.3 Initialize the Keyserver Database key as an HSM protected key

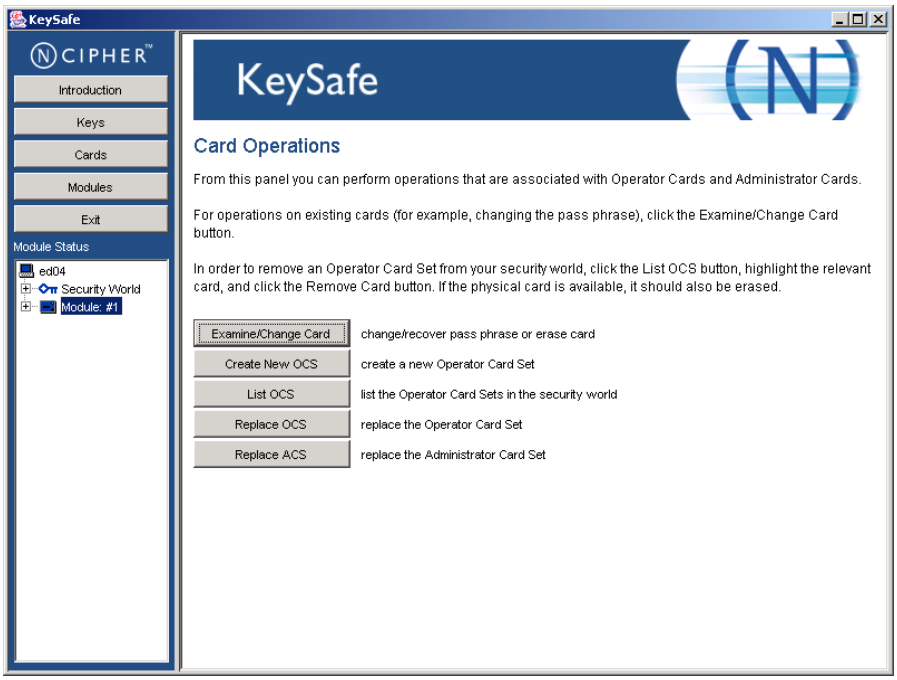
As described in the ***Installation and Configuration Guide***, run the GenMaster application to initialize the Keyserver database key.

These instructions highlight differences between standard (non HSM) GenMaster operation, and GenMaster operation where the key is protected by the HSM.

3.3.1 Card set protected

Follow this section to create an Operator card set if a Keyserver database key is to be card set protected. If a suitable card-set has already been created then this section may be skipped.

1. Run the KeySafe application, which ships with the nShield hardware.



   a) Highlight the module in the tree view, and click **Cards**.

   b) Click **Create New OCS** (Operator Card Set) on the main screen.

2. The **Create Operator Card Set** page is displayed.

   a) Create a unique name for the card-set.

b) Make sure:

- The card-set does *not* have a timeout
- Decide on an appropriate value for **N** (the total number of cards in the card-set).

  In the event of loss or damage to all the cards in the card-set, the keys will no longer be accessible, and therefore any data encrypted with the keys may be lost. In choosing to protect the keys with cards it is important to realize that access to the keys (and therefore data encrypted by the keys) is dependant on presenting the card-set to the system.

  Do *not* enter **1** for the value **N** – this will mean that only one card is created, and if it is lost, all keys and data protected by the card-set will be lost.

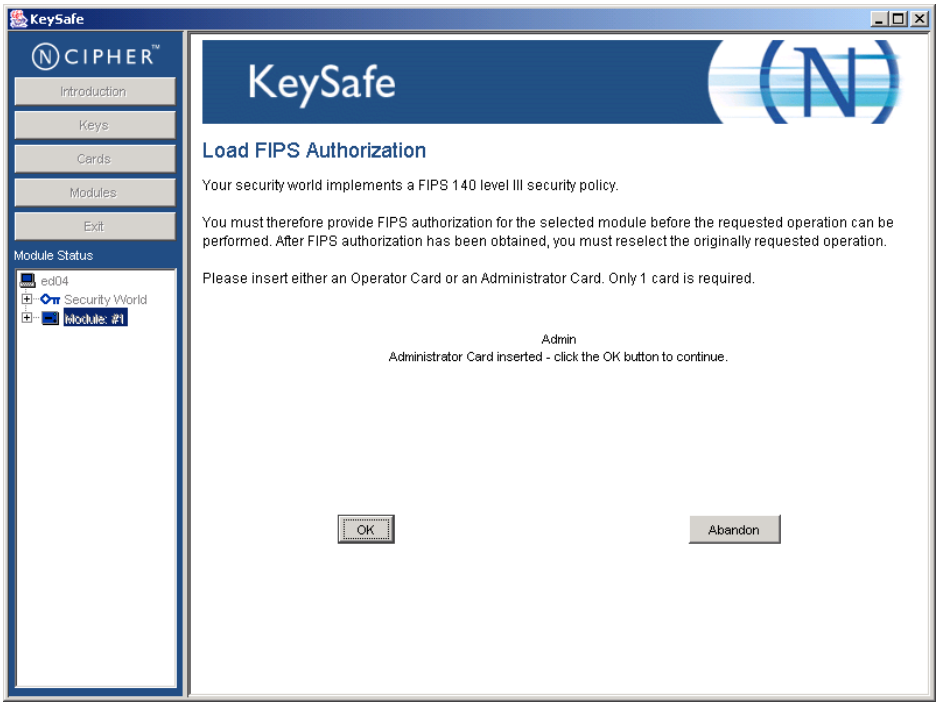
  Note: As long as one functioning card in a card-set remains it will be possible to generate additional cards in the KeySafe software in the future.

- **K**, the total number of cards required for access is **1**
- For the rest of the settings follow the screenshot above.

3. FIPS140-1 level 3 authorization

If the security world has been initialized in FIPS140-1 level 3 mode, additional authentication must be presented in order to validate the creation of a new operator card-set.

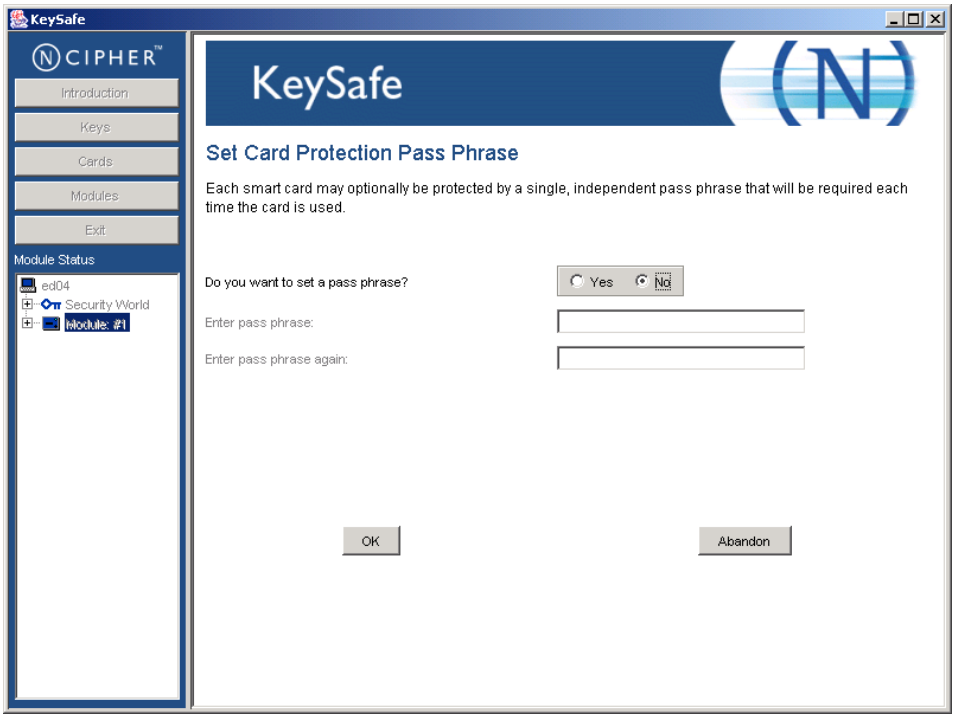
Present an administrator card to authorize the operation.



4. Create each individual card in the card-set.

   For each card in the card-set you will be asked to insert a blank card:

5. The **Set Card Protection Pass Phrase** page is displayed.



   For each card in the card-set you will be asked to enter a PIN if required. If you have decided that the card-set is to be PIN protected select **Yes** to set a pass phrase, and enter the pass phrase.

   If the security world is FIPS140-2 level 3 protected, it is advisable to set a PIN on the operator card-set, as this will enable the HSM to be FIPS authorized to enable key generation and key import.

Note: It is strongly recommended that you do not create a card-set where some cards require a pass phrase, and others do not.

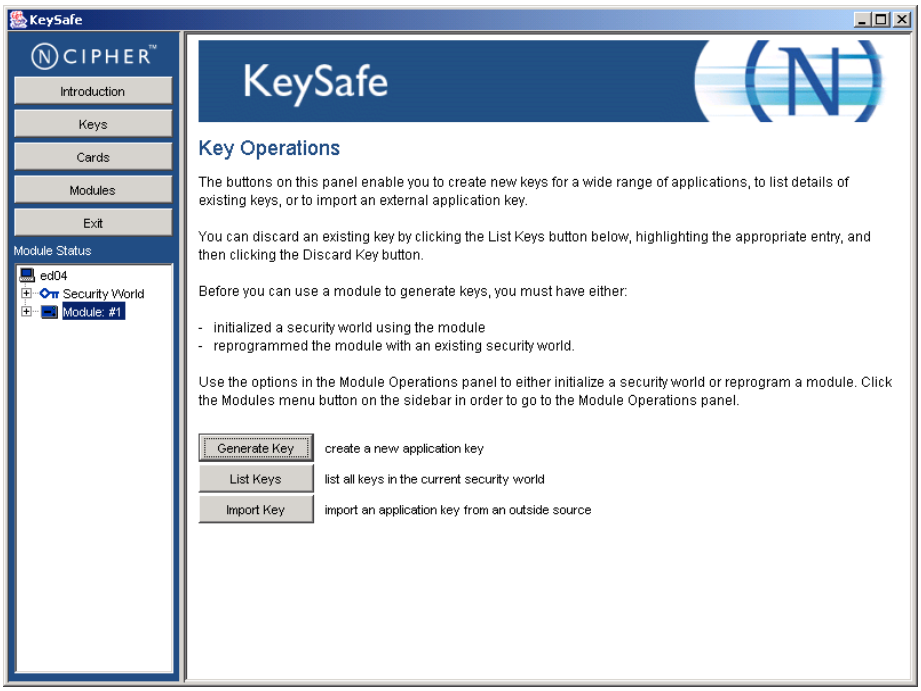
6. Repeat the previous two steps for each card in the card-set.

3.3.2 Use KeySafe to generate the Keyserver database key

If the HSM is *not* initialized in FIPS140-1 level 3 mode and the 'softcard' option or 'operator cardset with PIN' option is not being used, the GenMaster program will automatically generate the database key. In this case go to section *3.3.3*, *Run GenMaster to initialize the Keyserver database key*.

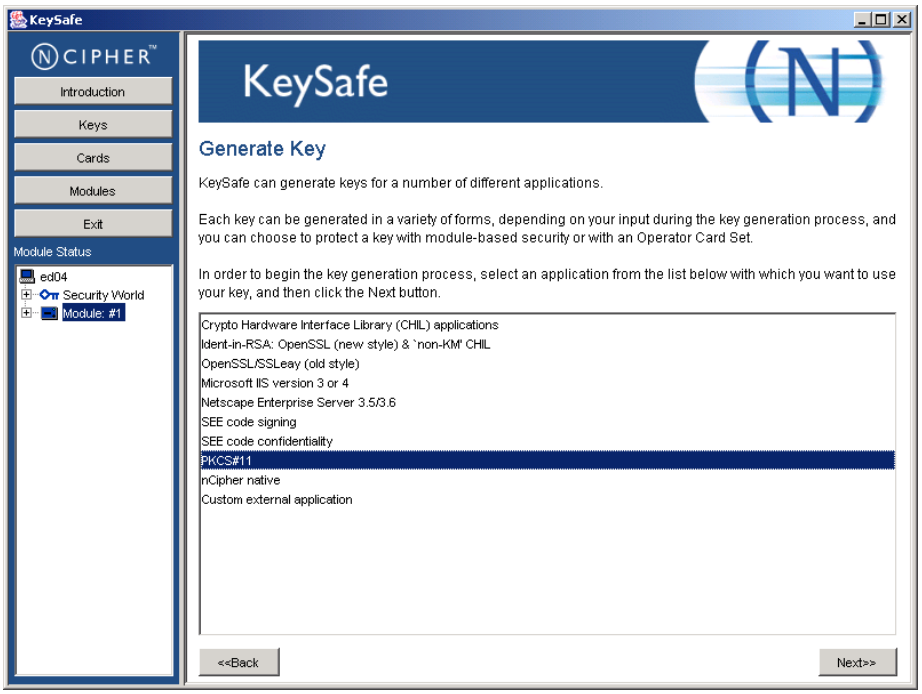
If the HSM *is* initialized in FIPS140-1 level 3, it will require user authentication to the HSM before generating the database key. If this requirement is not met (either by using 'softcard' or 'operator cardset with PIN'), you must either use the KeySafe program to generate the Keyserver database key within Keysafe, or perform a FIPS authorization on the HSM before running GenMaster as described in section *3.4*, *FIPS 140-2 level 3 authorization for generating or importing keys*.

1. Run KeySafe program.
   a) Highlight the module in the tree view, and click **Keys** on the left hand side.
   b) In the main window, click **Generate Key**.

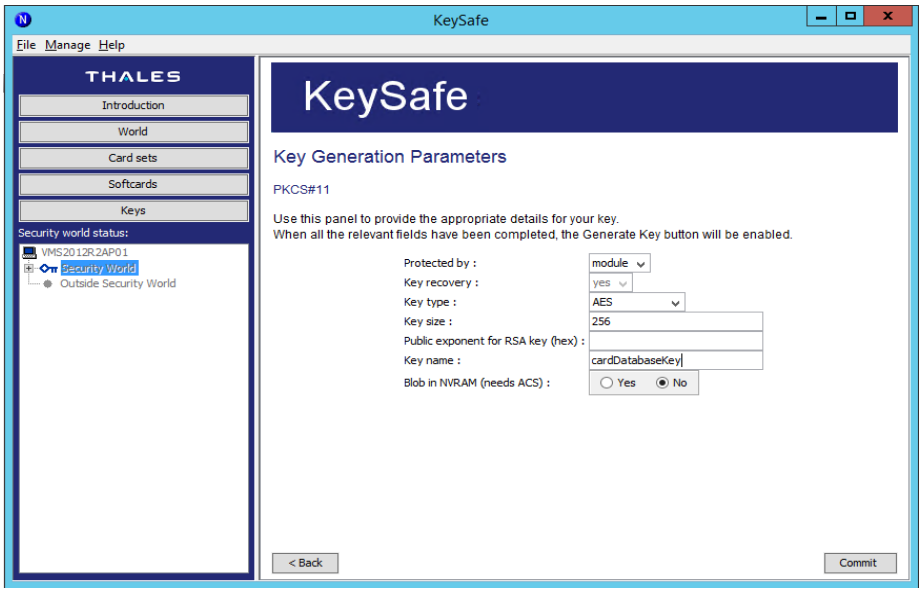


2. The **Generate Key** page is displayed.

   Select **PKCS#11** in the list, and click **Next**.



3. The **Key Generation Parameters** page is displayed.



a) Set the **Key type** as **AES**, and the **Key size** as **256**.

Note: If you are running a MyID installation older than MyID 10.4, select **Triple-DES**.

b) In **Protected by:**

- If the key is to be protected by the module, select **Module**.
- If the key is to be card-set protected, select **Smart card** and insert a card from the card-set into the HSM card-reader.

c) Enter a unique key name in the **Key name** box and make a note of it, as you will need to enter it into the GenMaster application later.

If multiple keys of the same name exist, GenMaster will report an error, since it is not possible to unambiguously identify the key.

d) Click **Generate Key** to proceed.

4. FIPS 140-2 level 3 authorization.

   If the security world has been initialized in FIPS 140-2 level 3 mode, additional authentication may be required in order to validate the creation of a new operator key. Follow the on screen instructions in this case. Note that after FIPS authorization has been granted, you must click on the **Generate Key** button again to generate the key.

3.3.3 Run GenMaster to initialize the Keyserver database key

As part of the MyID installation procedure, the GenMaster application is run to initialize the Keyserver database key. See the ***Installation and Configuration Guide*** for details.

Note: By default, you cannot use GenMaster to save the PIN for a Thales nShield HSM. If you want to store this PIN encrypted in the registry for the MyID COM+ user, you can use the SetHSMPIN utility. See the *Setting the HSM PIN* section in the ***Installation and Configuration Guide*** for details.

3.4 FIPS 140-2 level 3 authorization for generating or importing keys

If your security world is initialized in FIPS 140-2 level 3 mode, the HSM must be FIPS authorized before being able to generate or import a key. This includes key generation by GenMaster, and key generation or key ceremony import from MyID workflows such as **Manage GlobalPlatform Keys** or **Key Manager**.

The HSM is FIPS authorized when a PIN is supplied to it. If your security world is already PIN protected (for example, operator card with PIN), then it will already be FIPS authorized and this step will not be necessary. Otherwise, before performing the operation in MyID that would perform the key generation or key import, you can manually FIPS authorize the HSM as follows:

1. Run the KeySafe program.
2. Highlight the module in the tree view, then click **Keys** on the left hand side.
3. In the main window, click **Generate Key**.

   The Generate Key page is displayed.
4. Select **PKCS#11** in the list, and click **Next**.
5. Set the following options:
   - **Protected By** – set to **module**.
   - **Key type** – set to **AES**.
   - **Key size** – set to **256**.
   - You must also provide a unique key name; for example:

     ```
     testFIPSauth
     ```

   By generating a test key through KeySafe, KeySafe will prompt for a card and PIN to be entered if it has not already been FIPS authorized.

   KeySafe displays a message that says:

   ```
   FIPS authorization successfully loaded
   ```

Afterwards, you can delete the test key using KeySafe to keep the system tidy.

MyID can now perform key generation or key import.

6. In the event of the HSM being restarted, FIPS authorization will be lost, and this procedure can be repeated if necessary. Note that in MyID under normal circumstances, keys are only generated or imported as part of occasional setup steps, so there is no need to repeat this procedure in day to day running of the system.

3.5 Backup considerations

The cryptographic keys stored in the HSM are business critical data. If these keys are lost (for example, due to hardware failure) MyID will be unable to operate correctly and will lose the ability to manage issued devices.

You must create a backup strategy to protect the data in the HSM. If you generate any additional keys or import any additional keys, you must make sure your backup is up-to-date.

After setting up the nShield security world, smart cards containing the security world key are created. You must ensure that enough smart cards are created to account for possible hardware failure of nShield security world smartcards. If PINs are used to protect these smart cards, the PINs must not be lost or forgotten. In the event of the loss of the nShield smart cards or PINs, it will not be possible to recover the nShield security world to a new HSM. In the event of a hardware failure this would render the cryptographic keys unrecoverable.

nShield HSM stores keys on the MyID application server (and nShield Remote File System if configured) as encrypted files in the `kmdata` directory. You must back up this directory; to recover the keys, both the nShield security world smartcards and `kmdata` directory are required.