MyID PIV

Version 12.13

Entrust nShield HSM Integration Guide

ENTRUST READY

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

Document reference: INT1970-12.13.0-PIV

December 2024

Copyright

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

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:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks 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 product 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

Entrust nShield HSM Integration Guide **1**
Copyright **2**
Conventions used in this document **6**
Contents **7**
1 Introduction **8**
2 Overview **9**
2.1 Hardware and software requirements 9
2.1.1 SHA256 support 9
2.1.2 Supported nShield HSM models 9
2.1.3 Multiple HSMs 10
2.2 HSM Test Utility 10
3 Installing the HSM **11**
3.1 Install HSM hardware and software 11
3.1.1 Security Assurance Mechanism 12
3.2 Initialize the security world 12
3.2.1 What is FIPS140-2? 13
3.3 Configure remote file system / client connectivity 13
3.4 Levels of security offered by nShield HSM 14
3.4.1 Keys protected by module 14
3.4.2 Keys protected by module and smart card 14
3.4.3 Keys protected by module and smart card with PIN 14
3.4.4 Keys protected by module and 'softcard' 14
3.5 The role of the HSM card reader 15
3.5.1 Module or card set to protect Keyserver database key 15
3.5.2 Module or card set to protect KSP or CSP keys 15
3.6 Install nShield KSP or CSP 16
3.6.1 Using KSP instead of CSP 17
3.7 Copy nShield PKCS#11 driver 17
4 After installing nShield **18**
4.1 Check the NFAST_KMDATA environment variable 18
4.2 Check the PKCS#11 interface to the HSM 18
4.3 Initialize the Keyserver Database key as an HSM protected key 18
4.3.1 Operator card set protected 18
4.3.2 Run GenMaster to initialize the Keyserver database key 18
4.4 FIPS 140-2 level 3 authorization for generating or importing keys 19
4.4.1 nShield Security World software version 13 and later 19
4.4.2 nShield Security World software prior to version 13 19
4.5 Backup considerations 20

1 Introduction

This document provides a step-by-step guide to the configuration of MyID® to integrate with an Entrust 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.

2 Overview

This section contains an overview of the support for Entrust nShield HSMs, including prerequisites, supported models, and limitations.

2.1 Hardware and software requirements

Hardware requirements, supported platforms, and software requirements are specified in the *Hardware and software requirements* section of the ***Installation and Configuration Guide***.

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

This release of MyID has been tested with the following Entrust nShield configuration:

Model	Security World Client	Connect Image	Security World Version	FIPS Certified	FIPS Firmware
nShield Connect XC	13.4.4	13.4.3	v3 - DLf3072s256mAEScSP800131Ar1	Yes	12.72.1 Historical: 9/21/2026
nShield 5c	13.4.4	13.2.2	v3 - DLf3072s256mAEScSP800131Ar1	140-3 Provisional	13.2.2

If you are using a different configuration of the nShield HSM, you are recommended to use the HSM Test Utility to validate integration; see section *2.2*, *HSM Test Utility*.

MyID supports HSMs running in FIPS 140-2 L3 mode and 140-3 Provisional mode. When using these modes, the HSM does not allow 3DES and RSA 1024.

2.1.1 SHA256 support

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

2.1.2 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.

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.

2.1.3 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.

2.2 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.

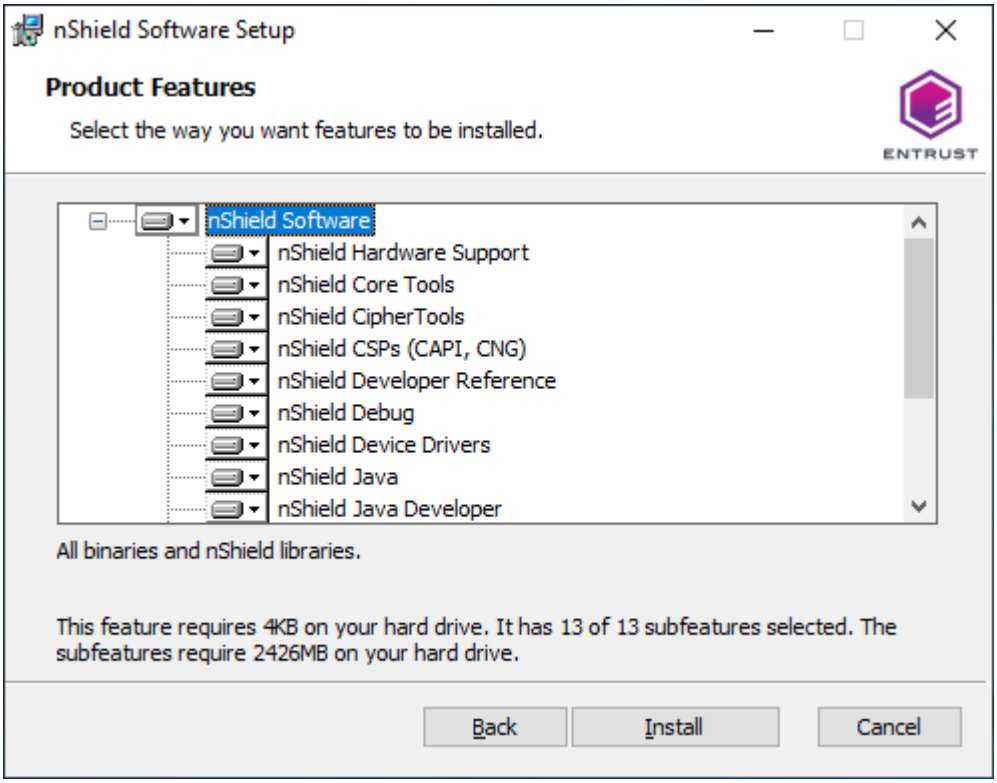
3 Installing the HSM

This section contains instructions on installing your HSM.

3.1 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. Install all of the features provided in the installation program.



3.1.1 Security Assurance Mechanism

The nShield Security Assurance Mechanism means that 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, by default the Security Assurance Mechanism is enabled.

Warning: If you do not disable the Security Assurance Mechanism, any imported factory keys expire after 48 hours.

To disable the Security Assurance Mechanism:

1. Open the `cknfastrc` file in the `nfast` directory.
2. To disable the Security Assurance Mechanism, set the following option:
   - `CKNFAST_OVERRIDE_SECURITY_ASSURANCES`

     Set this option to `all` to disable the Security Assurance Mechanism. If the option already exists in the file with a value other than `all`, set the value to `all`. If the option does not already exist, add it to the file:

     ```
     CKNFAST_OVERRIDE_SECURITY_ASSURANCES=all
     ```
3. Save the `cknfastrc` file.
4. Restart the MyID KeyServer.

3.2 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.

3.2.1 What is FIPS140-2?

FIPS140-2 is an accreditation that provides assurance that a security device fulfills 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.

3.2.1.1 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.

3.2.1.2 FIPS140-2 level 3

This mode implements additional restrictions on top of FIPS140-2 level 2 on the available algorithms and modes, and additional HSM card set authorization is required to generate or import new keys.

3.3 Configure remote file system / client connectivity

Note: This step applies only to netHSM. If you are not using a netHSM, you can 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 you have configured the MyID application server to connect to the HSM, verify the connectivity by running nShield's `enquiry` command line utility. Ensure that the module is listed, and that its `State` is described as `Operational`. If `enquiry` does not report the HSM as `Operational`, MyID cannot communicate with the module.

Note: If you have multiple MyID application servers, and do not have a remote file system configured, you must manually copy any keys from the `C:\ProgramData\nCipher\Key Management Data\local` folder of the machine that created the key to the same location on the other MyID application servers.

3.4 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.

3.4.1 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 smart card reader. This is the recommended configuration for the MyID Application server.

If you have nShield 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.

3.4.2 Keys protected by module and smart card

In this configuration, the key is stored encrypted on the hard disk, encrypted by the module key, and an (operator card set) smart card 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.

3.4.3 Keys protected by module and smart card with PIN

In this configuration, the key is stored encrypted on the hard disk, encrypted by the module key, and an (operator card set) smart card 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 smart card.

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.

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

3.4.4 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 smart card is required.

Automatic 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.

3.5 The role of the HSM card reader

The nShield HSM has its own dedicated smart card 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 of n" card set protection – that is, *k* out of a possible *n* cards must be authenticated to in order to allow access to the key, MyID only supports "1 of n" card sets – that is, 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" (that is, 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.

In addition to the card slot on the HSM, there is an optional nShield "Remote Admin Client" feature that allows a card reader attached to a computer to connect to the HSM and behave as if that card reader were attached to the HSM

3.5.1 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 card set protected, and other keys to be module protected.

3.5.2 Module or card set to protect KSP or CSP keys

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

If the KSP or 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 KSP or CSP to operate one of the cards in the card set must remain in the HSM card reader permanently. If the KSP or 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 KSP or CSP is module protected, then the HSM card-reader will not be required for KSP or CSP operation.

3.6 Install nShield KSP or CSP

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

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 KSP or CSP, then a '1 of n' card set 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 KSP or CSP and for the Keyserver database key protection, then the same card set is used to protect both the KSP or 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 KSP or 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 KSP or CSP (as opposed to the default Microsoft software KSP or 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 KSP or CSP, so that the nShield KSP or 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) KSP or CSP is used to protect this private key. Additional security can be added by generating this private key within the hardware nShield KSP or CSP. In order to facilitate this, the certificate template that defines the KRA certificate must be edited to allow the nShield KSP or CSP to be used for this type of certificate (by default only the Microsoft Software KSP or CSPs are allowed for this certificate type.) For further instruction on requesting the KRA certificate see and *Key Recovery Agent certificate requirements* section of the ***Microsoft Windows CA Integration Guide***.

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

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

  Any certificate that is requested for the nShield KSP or 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**.

Note: In FIPS 140-2 L3 mode, some aspects of the KSP or CSP are not supported; for example, you cannot request a KSP or CSP-backed certificate.

3.6.1 Using KSP instead of CSP

You are recommended to use the KSP in preference to the CSP. MyID can use the KSP instead of the CSP for server certificates. See the following for details of setting up server certificates:

- The *Configure server signing certificates* section of the ***PIV Integration Guide*** (for PIV Content Signer Certificate)
- The *Enrollment Agent certificate* and *Key Recovery Agent certificate requirements* sections of the ***Microsoft Windows CA Integration Guide*** (for Enrollment Agent and KRA certificates)
- The *Setting the content signing certificate* section of the ***Mobile Identity Management*** guide (for mobile badge layout content signer certificate)
- The *Setting up the CVC signing certificate* section of the ***Smart Card Integration Guide*** (for OPACITY signing certificate)
- The *Signing and encryption certificates for SCEP* section of the ***Administration Guide*** (for SCEP signing certificate)

3.7 Copy nShield PKCS#11 driver

Copy the `cknfast.dll` file from the `nfast\bin` folder in the nShield software folder to the `Windows\System32` folder.

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

4 After installing nShield

This section contains instructions on configuring your HSM after installation.

4.1 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 the `Key Management Data` folder in the nShield software folder under `C:\ProgramData`.

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
```

4.2 Check the PKCS#11 interface to the HSM

After you have installed KeySafe, you can run the following at the command line to check the PKCS#11 interface to the HSM:

```
cklist
```

If this operation works, the PKCS#11 interface is operational and the HSM will be listed as a master key option when you install MyID.

4.3 Initialize the Keyserver Database key as an HSM protected key

As described in the *Using GenMaster* section 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.

4.3.1 Operator card set protected

Follow the nShield documentation 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 you can skip this process.

Note: While nShield allows operator card sets with a "k of n" quorum (where there are *n* cards, but to provide authorization *k* cards must be presented), when using an operator card set in MyID, *k* must be 1 (for example, a 1 of 5 card set), since in practice you can insert only one card at once.

4.3.2 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 *Using GenMaster* section in the ***Installation and Configuration Guide*** for details.

Note: By default, you cannot use GenMaster to save the PIN for an Entrust 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.

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

When an nCipher HSM is in FIPS140-2 level 3 mode, there are some additional requirements that you must meet for the HSM to perform certain operations. This includes key generation by GenMaster, and key generation or key ceremony import from MyID workflows such as **Manage GlobalPlatform Keys** or **Key Manager**.

If these requirements are not met, some operations will fail, and the following error may be reported:

```
PKCS11 error: 0x800000e0 : FIPS token not present
```

4.4.1 nShield Security World software version 13 and later

To make the HSM FIPS authorized, you must insert an admin or operator card, either into the HSM card slot or into a card reader connected to the HSM through the nShield remote admin client. If the card is not present, MyID cannot use the HSM.

4.4.2 nShield Security World software prior to version 13

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.

To generate or import keys, the following requirement must be met:

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
   ```

   Afterward, 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.

4.5 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 smart cards. 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 smart cards and `kmdata` directory are required.