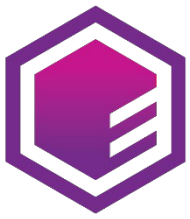
PrimeFactors™
APPLIED DATA PROTECTION



ENTRUST

EncryptRIGHT and nShield HSM

Integration Guide

Prime Factors Holding Company, dba Prime Factors
1400 Executive Parkway, Ste 100
Eugene, OR 97401

Phone: 541.345.4334

Technical Support

Prime Factors' web site provides up-to-the-minute product and company information.

Should you experience technical issues that cannot resolve using this document, you may contact us for more help.

Online Support Request: **https://www.primefactors.com/request-support/**

Technical Support Phone: 541.345.4334

Support Hours: 8:00 am to 5:00 pm (Pacific Time), Monday through Friday

Answering service available 24 hours a day, 7 days a week.

You can also use the above telephone numbers and web site to obtain other information about Prime Factors or our products.

EncryptRIGHT and nShield HSM Integration Guide

Document Number crns43100-091322

Contents

About EncryptRIGHT

EncryptRIGHT is a flexible and scalable software solution that helps implement application-layer data security governance, allowing enterprises to simplify data protection by abstracting data protection policies from application programming while providing a complete separation of duties between information security and application programming.

Leveraging a Data Security Governance approach, EncryptRIGHT defines and enforces how data is protected, who may access specific data, and what format that data will take when access is granted. EncryptRIGHT provides data encryption, tokenization, data masking, key management, audit-logging, and reporting functionality to protect Personally Identifiable Information (PII) and other sensitive data of global customers across many industries, including financial services, healthcare, global logistics, manufacturing, energy, and more. Whether complying with global data protection regulations or industry standards, reducing the scope of PCI-DSS audits, protecting privacy, pseudonymizing or anonymizing data, managing data sovereignty, or subpoena-proofing the cloud, EncryptRIGHT delivers a seamless data protection solution where data is most at risk of being breached.

At the heart of EncryptRIGHT is the security database which holds all product definitions including keys, user definitions, and data protection policy definitions. Each record is hashed and encrypted and a hardware security module (HSM), such as the Entrust nShield Connect, can add hardware protection to keys and cryptographic processes.

Prerequisites

Before EncryptRIGHT can be integrated with an nShield Connect or nShield as a Service, the Entrust Security World must be installed and fully configured. Entrust provides documentation that cover the installation process and available features:

- Entrust nShield Connect Documentation
  - Installation Guide nShield Connect
  - User Guide - nShield Connect - Unix
  - User Guide - nShield Connect - Windows
- Entrust Remote Administration
  - User Guide - nShield Remote Administration Client

If your nShield HSM is a remote, unit, you will also need to have an nShield Trusted Verification Device.

IMPORTANT: Prime Factors has tested against and verified EncryptRIGHT compatibility with nShield Security World versions **12.60** and **12.81**. Version **12.71** is *not* supported.

In addition, EncryptRIGHT integration requires the configuration of an Operator Card Set (OCS) during the Security World setup.

EncryptRIGHT Setup

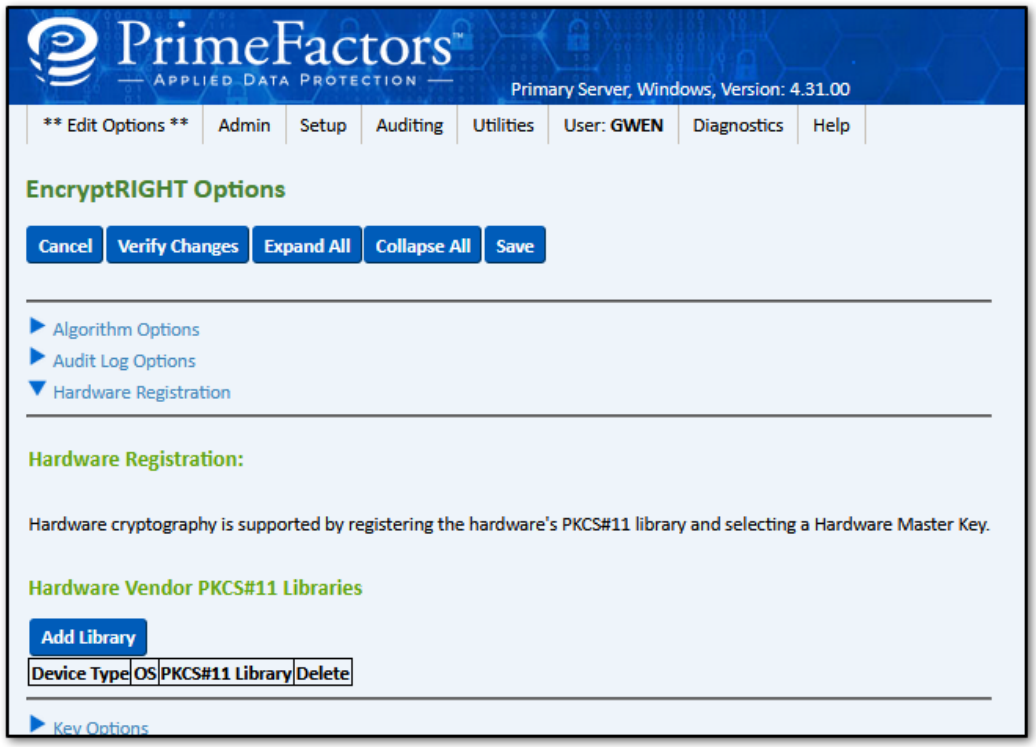
Once you have installed the nShield Security World Software, including creating the OCS with a Passcode, you will need to either install the EncryptRIGHT application or configure an existing installation to use the HSM. Installation instructions for EncryptRIGHT are provided in the EncryptRIGHT Setup and Security Configuration Guide.

IMPORTANT: EncryptRIGHT must be installed on the same machine on which the nShield Security World is installed.

Hardware Registration

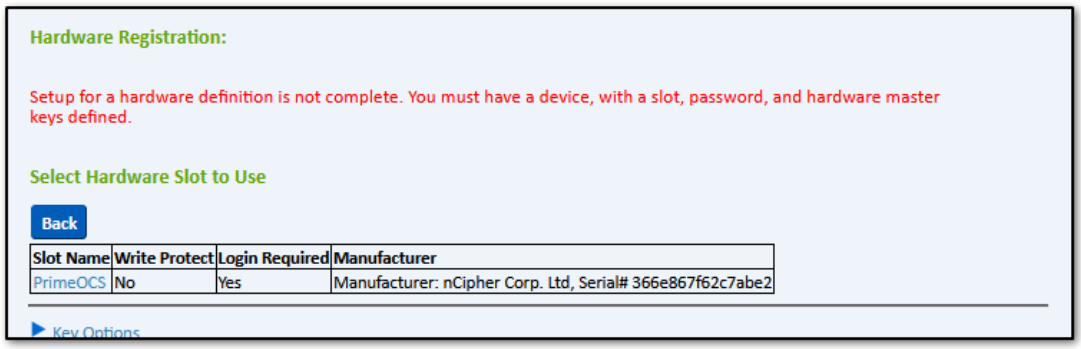
To set up the nShield as part of a new EncryptRIGHT installation or add one to an existing EncryptRIGHT installation:

1. Open Hardware Registration:
   - If you are setting up your nShield/EncryptRIGHT integration during the EncryptRIGHT setup, you will come to the Hardware Registration options as part of post-installation configuration steps.
   - If you are adding an nShield to an existing EncryptRIGHT installation, log on to your EncryptRIGHT Primary Server and go to **Admin > Options > Hardware Registration**.
2. Click **Add Library**.

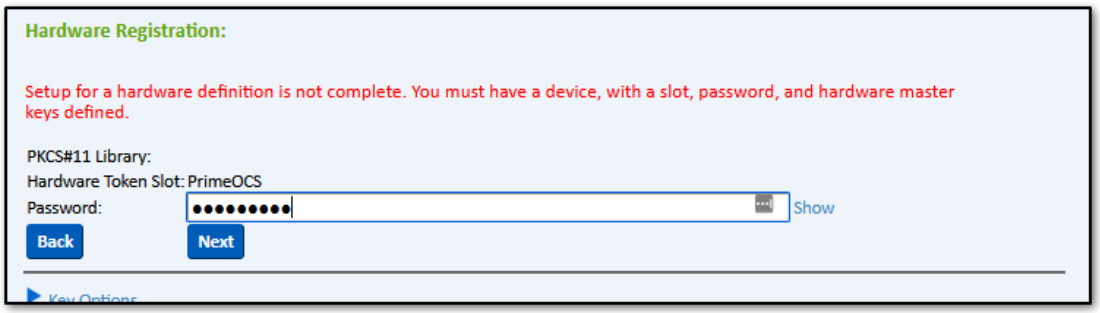


- Supply the location of the **nShield PKCS#11 library**. In most cases, clicking **Default Library** will supply the correct location. If you've installed it to a custom location, you will need to manually specify it (or navigate to it via the **Browse** button.)
- If you are going to use an nShield HSM on multiple machines of the same operating system type, their installation location will need to be the same on each system.
- If you have the nShield software installed to different locations on different machines with the same operating system, you will need to uninstall/reinstall as appropriate so that the software is installed to the same locations.
- If you will be using nShield HSMs on multiple operating systems, you will need to add the library for each operating system on your EncryptRIGHT Primary Server, regardless of its platform. For example, even if your EncryptRIGHT Primary Server is running Windows, if you are also planning to use HSM support via EncryptRIGHT on Linux machines, you will need to supply the location of the PKCS#11 library there as well. Obviously, you cannot browse to the location of a library on another operating system.

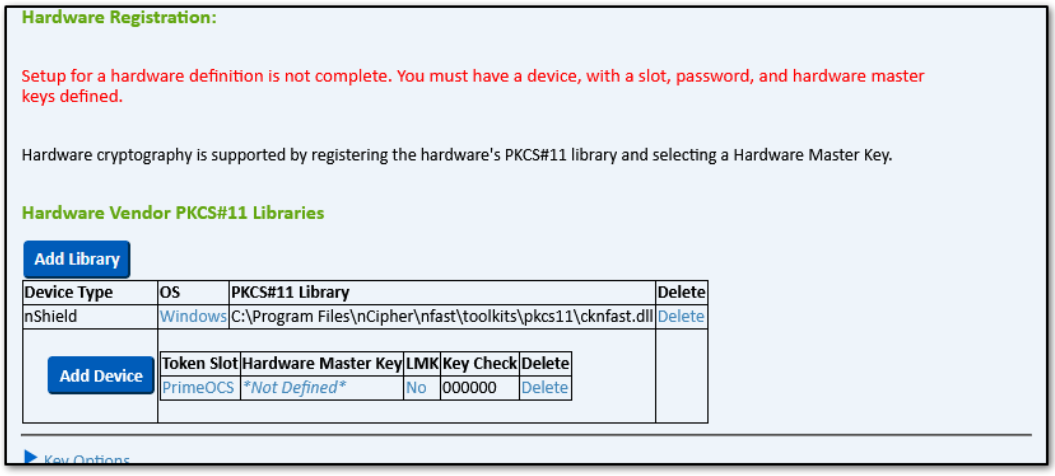
3. Click **Next** to see a list of OCS slots.



4. You should see the name of the OCS defined during the prerequisite steps. Click the **slot name** (link in blue text) and you will be prompted to provide the **OCS password** used when you set up your Operator Card Set.



5. Enter the **OCS Password** and click **Next**. The screen will display your token slot with Hardware Master Key Not Defined:



Hardware Registration:

Setup for a hardware definition is not complete. You must have a device, with a slot, password, and hardware master keys defined.

Hardware cryptography is supported by registering the hardware's PKCS#11 library and selecting a Hardware Master Key.

Hardware Vendor PKCS#11 Libraries

Add Library

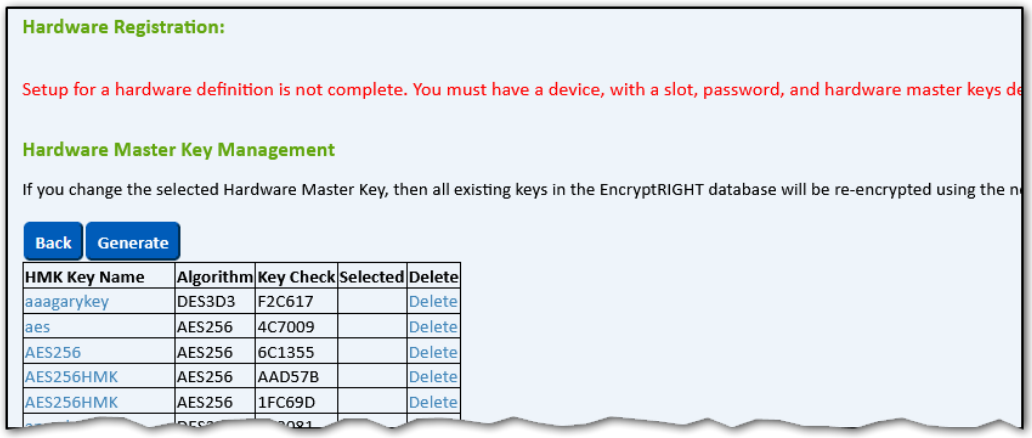
Device Type	OS	PKCS#11 Library	Delete
nShield	Windows	C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll	Delete

Add Device

Token Slot	Hardware Master Key	LMK	Key Check	Delete
PrimeOCS	*Not Defined*	No	000000	Delete

▶ Key Options

6. Click the words **Not Defined** to display a list of available Hardware Master Key names.



Hardware Registration:

Setup for a hardware definition is not complete. You must have a device, with a slot, password, and hardware master keys de

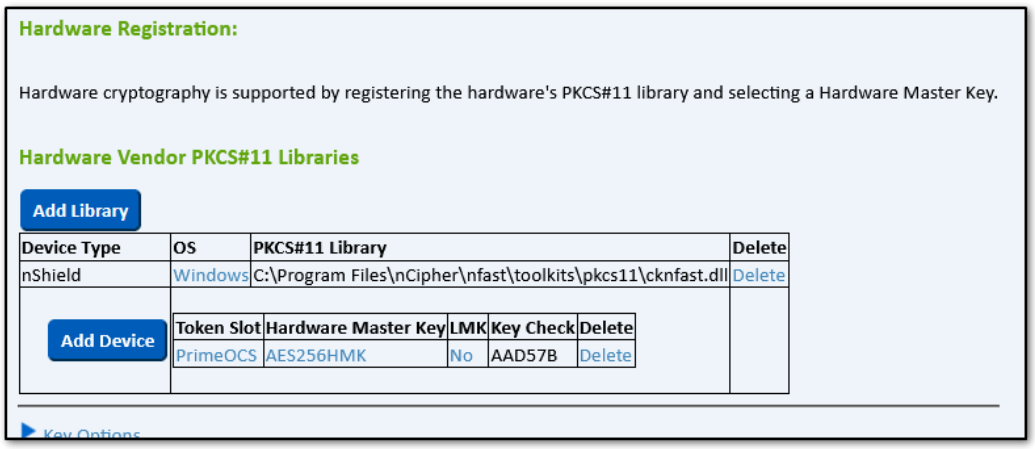
Hardware Master Key Management

If you change the selected Hardware Master Key, then all existing keys in the EncryptRIGHT database will be re-encrypted using the n

Back Generate

HMK Key Name	Algorithm	Key Check	Selected	Delete
aaagarykey	DES3D3	F2C617		Delete
aes	AES256	4C7009		Delete
AES256	AES256	6C1355		Delete
AES256HMK	AES256	AAD57B		Delete
AES256HMK	AES256	1FC69D		Delete

7. Either select an **existing Hardware Master Key** from the list, or click **Generate** to create a new one. This completes your hardware registration.



Hardware Registration:

Hardware cryptography is supported by registering the hardware's PKCS#11 library and selecting a Hardware Master Key.

Hardware Vendor PKCS#11 Libraries

Add Library

Device Type	OS	PKCS#11 Library	Delete
nShield	Windows	C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll	Delete

Add Device

Token Slot	Hardware Master Key	LMK	Key Check	Delete
PrimeOCS	AES256HMK	No	AAD57B	Delete

▶ Key Options

8. Click **Save** at the top of the screen to finish and return to the main menu.

9. If your EncryptRIGHT footprint has multiple EncryptRIGHT instances connecting to the nShield Security World, perform an EncryptRIGHT synchronization from the Primary Server to those installations so they will get the settings for accessing the nShield Security World.

Securing EncryptRIGHT Keys with an HSM

The Hardware Master Key (HMK) key is a randomly generated Key Encrypting Key that is created by EncryptRIGHT during the hardware registration process. It enables EncryptRIGHT to use the HSM to generate Hardware Protected Keys (only available for use by EncryptRIGHT), or Hardware Native Keys (available for use by EncryptRIGHT as well as other applications that utilize the nShield HSM), and export or import them from the HSM under the HMK. The HMK can also be used to harden the protection for the EncryptRIGHT database by encrypting the Local Master Key (LMK), which is used to secure the internal EncryptRIGHT database, with the HMK.

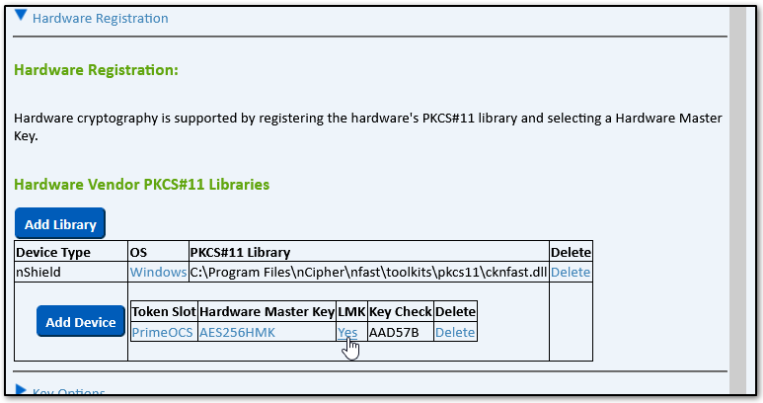
Enable HSM Protection for LMK

Selecting this option adds additional security by binding any EncryptRIGHT installation to an nShield environment. It will not be possible to use EncryptRIGHT without nShield Security World connectivity. This can help protect against someone making a copy of an EncryptRIGHT Primary Server's filesystem and trying to use EncryptRIGHT in another environment. If the installation cannot communicate with nShield Security World, it will not be able to decrypt the internal database EncryptRIGHT uses and won't be able to load any of the configuration required to encrypt and decrypt data.

IMPORTANT: If you decide to use nShield to protect EncryptRIGHT's LMK you should establish a disaster recovery procedure for nShield Security World. Entrust Support can provide guidelines on the best way to accomplish this task.

To enable HSM protection for the LMK:

1. In EncryptRIGHT, select **Admin > Options > Hardware Registration**.
2. Beside your active Token Slot, click the blue **No** in the LMK column, turning it into a



Yes.

3. Click **Save** to close the options screen. You'll see a message confirming the LMK re-encryption.

Disable HSM Protection for LMK

The nShield is used to decrypt the hardware encrypted values, so once you have enabled HSM support for the LMK, you must have HSM connectivity to disable it.

To disable HSM LMK Support:

1. In EncryptRIGHT, select **Admin > Options > Hardware Registration**.
2. Beside your active Token Slot, click the blue **Yes** in the LMK column, turning it into a **No.**
3. Click **Save** to close the options screen. You'll see a message confirming that LMK encryption was removed.

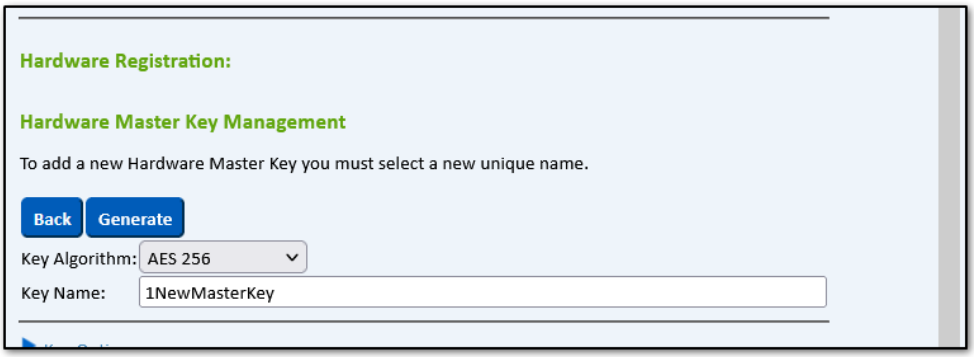
Manage Hardware Master Keys

The Hardware Master Key (HMK) enables EncryptRIGHT to protect keys generated by the HSM and, optionally, the LMK that encrypts the internal EncryptRIGHT database.

If the HMK is changed, all existing keys will need to be decrypted under the old HMK and re-encrypted under the new one. EncryptRIGHT will handle the conversion process, providing useful information along the way.

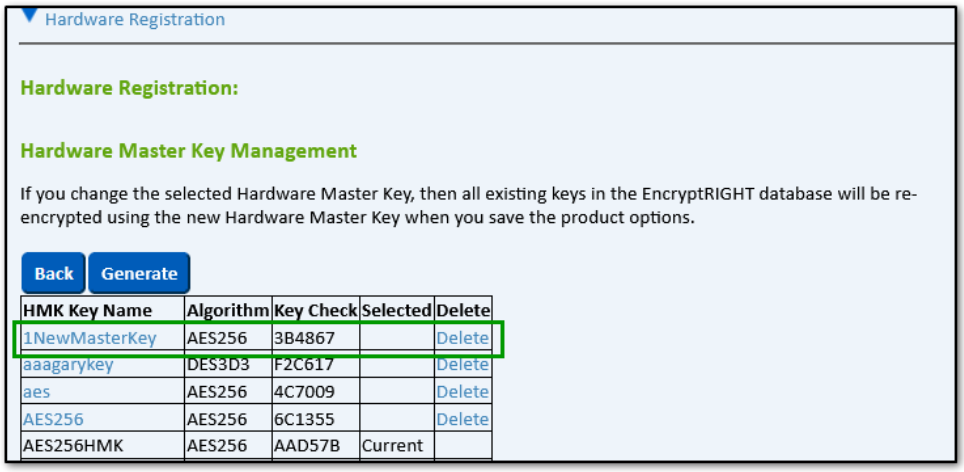
To change the HMK:

1. In EncryptRIGHT, select **Admin > Options > Hardware Registration**.
2. Beside your active Token Slot, click the **blue key name** in the Hardware Master Key column.
3. Either **choose an existing key** from the list, or click **Generate** to make a new one.

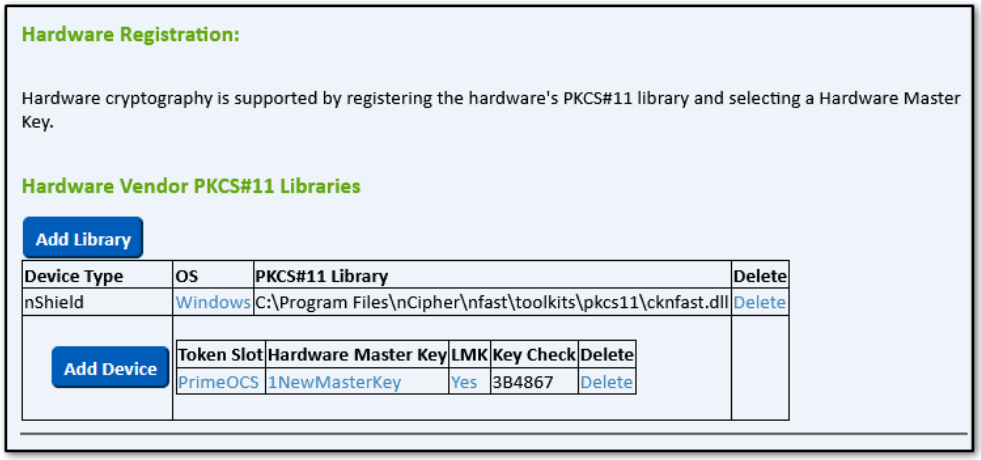


- Select a **Key Algorithm** from the drop down list.
- Specify a **unique name** for the new key.

- Click **Generate**. The new key will now be available for selection.



- Click the **key name** to select it and view the new key added to the device.



4. Click **Save** at the top of the screen. You will receive notification that all hardware keys will be re-encrypted.

5. Click **Yes** to complete the operation.