Prime Factors

EncryptRIGHT Application Layer Data Protection Platform

v4.60

Integration Guide

u.trust GP HSM Se-Series

6.2.0

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH
	Krefelder Straße 220
	52070 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-02-25
Status	PUBLISHED
Document No.	IG-2026-0001

Table of Contents

1 Introduction

This guide is part of the resources provided by Utimaco to facilitate secure application-layer data protection practices. It details the integration of Prime Factors' EncryptRIGHT platform with Utimaco's u.trust GP HSM Se-Series, enabling strong cryptographic key management and enhanced security for sensitive data.
All official documentation for Utimaco's u.trust GP HSM Se-Series can be accessed on Utimaco's website at *https://utimaco.com/.*
The guide provides a step-by-step walkthrough of the integration process.

1.1 About This Guide

This guide explains how to integrate the Prime Factors' EncryptRIGHT Application Layer Data Protection Platform with Utimaco u.trust GP HSM Se-Series to enable hardware-based key management and secure application-layer encryption for sensitive data.

1.2 Target Audience

This guide is intended for Prime Factors' EncryptRIGHT Application Layer Data Protection Platform and Utimaco General Purpose Hardware Security Module (GP HSM) administrators.

1.3 Purpose of the Integration

The integration of the EncryptRIGHT application layer data protection platform with the u.trust GP HSM Se-Series enables enhanced security, delivering hardware based generation and lifecycle management of cryptographic keys used to protect sensitive data and the centralized database that holds the data protection policy definitions, associated keys, and user access privileges.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
GP HSM	General Purpose Hardware Security Module

Abbreviation	Meaning
PKI	Public Key Infrastructure
TDE	Transparent Data Encryption
PKCS	Public Key Cryptography Standards
PKCS#11	PKCS Part 11: The Cryptographic Token Interface Standard
SO	The PKCS#11 Cryptographic Slot Security Officer
DB	Database
JRE	Java Runtime Environment
MBK	Master Backup key
P11CAT	The PKCS#11 Graphical Interface Tool
CXI	Cryptographic eXtended Interface
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
API	Application Programming Interface
PCI DSS	Payment Card Industry Data Security Standard
GDPR	General Data Protection Regulation

Abbreviation	Meaning
HIPAA	Health Insurance Portability and Accountability Act
LAN	Local Area Network
PCI-e	Peripheral Component Interconnect Express
HMK	Hardware Master Key
KEK	Key Encryption Key
LMK	Local Master Key

Table 1: Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`

Convention	Use	Example
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Table 2: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message indicates the expected result after the successful execution of an instruction.

2 Product Overview

2.1 Overview of EncryptRIGHT

EncryptRIGHT is an application layer data protection software solution that protects data in storage, in transit, and in use. It delivers encryption, tokenization, data masking and redaction, signing and hashing, as well as control access to critical data based on defined user roles and privileges. EncryptRIGHT abstracts security capabilities from applications, using an external policy engine that any application can access. Security policies are written into the centralized engine and are then synchronized with clients that execute and enforce the policy locally, collocated with the application through Native APIs. EncryptRIGHT can also execute and enforce policy centrally through Web API calls from practically any application running in any environment in the cloud.

EncryptRIGHT leverages strong role-based access controls to define who should be able to access sensitive data, assign appropriate data access permissions, and easily orchestrate unlocking the protected data in a need-to-know manner – delivering static or dynamic data masking that allows each user to access data only to the extent to which they are authorized.

At the heart of EncryptRIGHT is the security database which holds the data protection policy definitions, associated cryptographic keys, and user privileges definitions. Each record is hashed and encrypted, enabling the use of an HSM to add hardware protection to keys and cryptographic processes.

2.2 Overview of u.trust GP HSM Se-Series

The u.trust GP HSM Se-Series is a next-generation, high-performance Hardware Security Module designed to serve as a scalable and crypto-agile root of trust for a wide range of applications, combining secure hardware with the SecurityServer firmware that powers all cryptographic operations. The HSM hardware—available as PCIe modules or LAN appliances—provides tamper-resistant protection, FIPS 140-2 Level 3 certification, high throughput (up to 40,000 RSA-2048 signatures per second), and support for up to 31 isolated containers to enable true multi-tenancy. This hardware foundation works in tandem with SecurityServer, which is the secure firmware layer that runs inside the HSM. While the hardware ensures physical and cryptographic robustness, SecurityServer provides the operational environment, including cryptographic APIs (such as PKCS#11), key management, policy enforcement, and the execution framework for custom extensions via an SDK. In essence, the Se-Series is the physical trusted platform, and SecurityServer is the secure operating layer enabling cryptographic functionality. Together, they provide a flexible, scalable, and future-proof solution with support for custom

algorithms, application separation through containerization, and readiness for post-quantum cryptography.

2.3 Joint Value Proposition

Prime Factors and Utimaco help customers meet regulatory requirements such as PCI DSS, GDPR, HIPAA, and data breach disclosure regulations. As an application layer data encryption, tokenization, and masking solution, EncryptRIGHT facilitates how sensitive data is protected across customer deployments. The solution delivers comprehensive centralized data security policy management that enables local execution and enforcement through client instances serving applications one-to-one, or through Web APIs. Integration with the Utimaco u.trust GP HSM Se-Series delivers robust key generation and lifecycle management of underpinning keys used to protect data across customer deployments and to secure the data protection policy engine.

3 Integration Requirements and Prerequisites

Ensure that the system environment you will be using meets the following hardware and software requirements.

This guide assumes that the user has already installed and configured the required software.

3.1 Tested Versions

Operating System	EncryptRIGHT Version	Utimaco SecurityServer version	Utimaco HSM
	v4.60	v6.2.0	u.trust GP HSM Se-Series

Table 3: List of tested versions

3.2 Hardware and Software Requirements

3.2.1 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM Se-Series LAN with firmware SecurityServer 6.2.0 or higher
Utimaco PCI-e HSM	u.trust GP HSM Se-Series PCI-e with firmware SecurityServer 6.2.0 or higher

Table 4: List of hardware requirements

3.2.2 Software Requirements

Software	Software Requirements
HSM Interface	SecurityServer PKCS#11 Provider
HSM Utility	SecurityServer PKCS#11 Tool (p11tool2)
EncryptRIGHT	v4.60 or later

Table 5: List of Software Requirements

3.3 Prerequisites

Before you begin, please ensure that you have:

- Created a user account in Confluence.
- Installed and set up the operating system listed in Tested Versions.
- Installed and set up the HSM listed in Tested Versions.
- Replaced the HSM default admin with a new admin user.
- Created and stored the MBK on each HSM. Refer to the SecurityServer documentation to set up the MBK.
- Set up and configured the SecurityServer. Refer to the SecurityServer documentation to set up the HSM.
- Set up and configured the PKCS#11 library according to your environment. Refer to the SecurityServer documentation for instructions on setting up and configuring the PKCS#11 library.
- Created the Security Officer (SO) user and Crypto user.

4 Installation and Configuration

The following section outlines the procedures required to configure Utimaco u.trust GP HSM Se-Series and Prime Factors' EncryptRIGHT Application Layer Data Protection Platform.

4.1 Setting Up Utimaco u.trust GP HSM Se-Series

If you have not already done so, create and request an Utimaco Support Portal Account at https://support.hsm.utimaco.com/support. This will allow you to download the software components needed for this installation.

On Linux:

1. Copy the downloaded software to the appropriate location on the Partner Product Server.
2. Create a utimaco folder under the /opt directory and create 2 directories `/opt/utimaco/bin` and `/opt/utimaco/lib`.

```
# mkdir -p /opt/utimaco/bin
# mkdir /opt/utimaco/lib
```

3. Copy the pkcs11 library file `libcs_pkcs11_R3.so` from the Utimaco CryptoServer software to the `/opt/utimaco/lib` directory and make the file executable.

```
cp ~/path_to_application_folder/lib/libcs_pkcs11_R3.so /opt/utimaco/lib
chmod +x /opt/utimaco/lib/libcs_pkcs11_R3.so
```

4. Copy the `csadm` and `p11tool2` files from the Utimaco CryptoServer software to the `/opt/utimaco/bin` directory and make both files executable.

```
# cd ~/path_to_application_folder
# cp csadm p11tool2 /opt/utimaco/bin
# chmod +x /opt/utimaco/bin/csadm /opt/utimaco/bin/p11tool2
```

5. Create the directory `/etc/utimaco`. Locate the Utimaco PKCS#11 configuration file in your SecurityServer directory, `Software\Linux\Crypto_APIs\PKCS11_R3\sample`.

Copy the Utimaco PKCS#11 configuration file `cs_pkcs11_R3.cfg to /etc/utimaco` directory.

```
# mkdir /etc/utimaco
# cd ~/path_to_application_folder/Software/Linux/Crypto_APIs/PKCS11_R3/sample
# cp cs_pkcs11_R3.cfg /etc/utimaco
```

On Windows:

On Windows, `cs_pkcs11_R3.cfg` will be automatically created and available in the `C:\ProgramData\Utimaco\PKCS11_R3` folder as part of the SecurityServer software installation. Edit the `cs_pkcs11_R3.cfg` file and make the appropriate changes to the file. A sample `cs_pkcs11_R3.cfg` file is mentioned below.

```
library = C:\oracle\extapi\64\hsm\utimaco\6.1.1.0\cs_pkcs11_R3.dll
 slot = 0
 pin = Oracle123
 [Global]
 # For Unix:
 Logpath = /tmp
 # For Windows:
 # Logpath = C:/ProgramData/Utimaco/PKCS11_R3
 # Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
 Logging = 1
 # Prevents expiring session after inactivity of 15 minutes
 KeepAlive = true
 # Set the Device to connect with
 #[CryptoServer]
 # Device specifier
 Device = <HSM_IP>
```

For detailed guidance on commands and their parameters, please refer to the Utimaco SecurityServer documentation. The device could be a u.trust GP HSM Se-Series, available in either PCIe or LAN form factors. Depending on the type, the device configuration line will follow one of these formats:

- **LAN-based HSM:** Device = `288@ipaddress`
- **PCIe-based HSM:** Device = `/dev/cs2.0`

Make sure to select the appropriate format based on your specific hardware setup.

`library` specifies the path where the `cs_pkcs11_R3.dll` file is located.

`Slot` indicates the slot number associated with the created `USER`.

`Pin` represents the password assigned to the `USER`.

To simplify your testing process, it's recommended that you enable the PKCS#11 log file by adjusting the logging settings. Specifically:

- Set the LogPath to a writable directory (not a specific file).
- Set the Logging log level to 1 for basic logging. Increase it to 4 for more detailed output during testing.

This will generate a log file named `cs_pkcs11_R3.log` within the specified LogPath directory. Reviewing this log can help with troubleshooting if you encounter issues. Once testing is complete, it's advisable to reduce Logging log level to 1 or 2 to limit output to only critical or important messages.

4.2 Setting Up EncryptRIGHT

Installation instructions for EncryptRIGHT are provided in the EncryptRIGHT Setup and Security Configuration Guide included with your download.

Hardware Registration

To set up the u.trust GP HSM Se-Series 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 u.trust GP HSM Se-Series/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 a u.trust GP HSM Se-Series to an existing EncryptRIGHT installation, log on to your EncryptRIGHT Primary Server first and then go to **Admin > Options > Hardware Registration**.

Figure 1 : EncryptRIGHT admin menu and dashboard interface

2. If the hardware library is not automatically detected then you will need to supply the library location. Otherwise, skip to step 3.

- Supply the location of the u.trust GP HSM Se-Series PKCS#11 library. In most cases, clicking Default Library will supply the correct location. If you 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 a u.trust GP HSM Se-Series on multiple machines of the same operating system, their installation location will need to be the same on each system.
- If you have the u.trust GP HSM Se-Series 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 not in the same location, then the LD_LIBRARY_PATH on each machine will need to be set to the appropriate directory for that machine and just the .so file name in the EncryptRIGHT field.
- If you will be using u.trust GP HSM Se-Series 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. You cannot browse to the location of a library on another operating system.

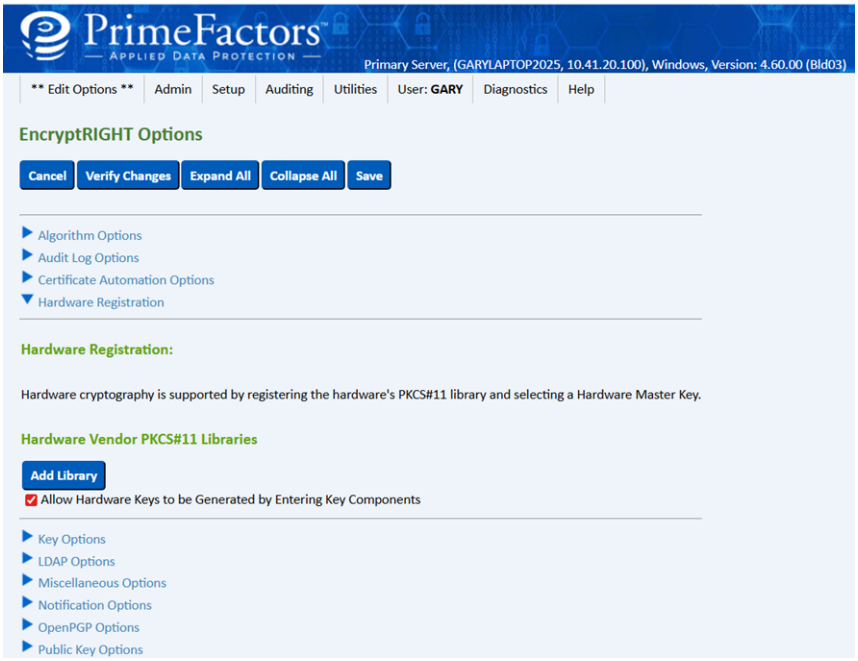

Figure 2 : EncryptRIGHT options

- Select Add Library.

Figure 3 : Edit PKCS#11 library

- Select Next.

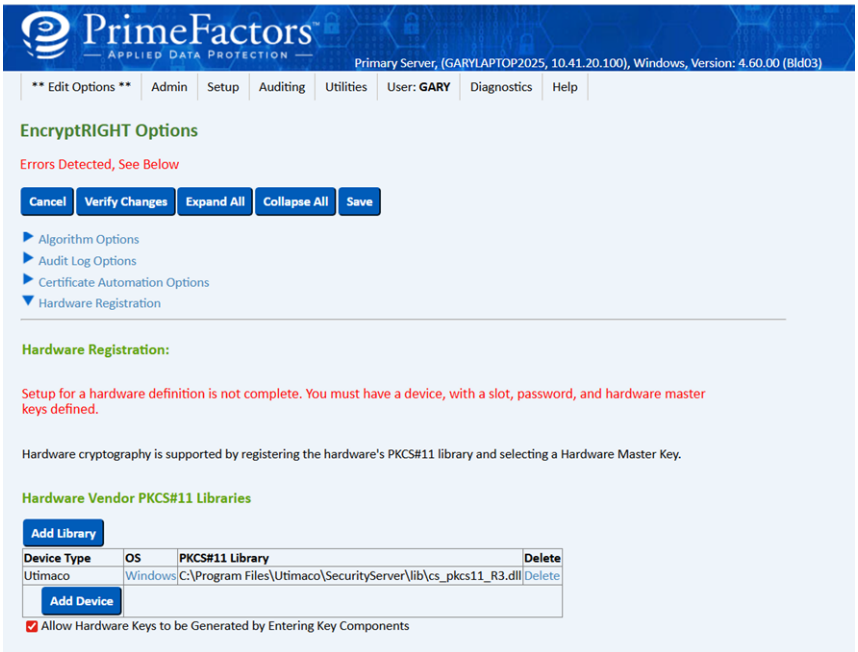

Figure 4 : Hardware vendor PKCS#11 libraries

- Select Add Device.

3. At this point EncryptRIGHT is able to communicate with the hardware library. You will need to select the slot and provide a password that your administrator has provided.

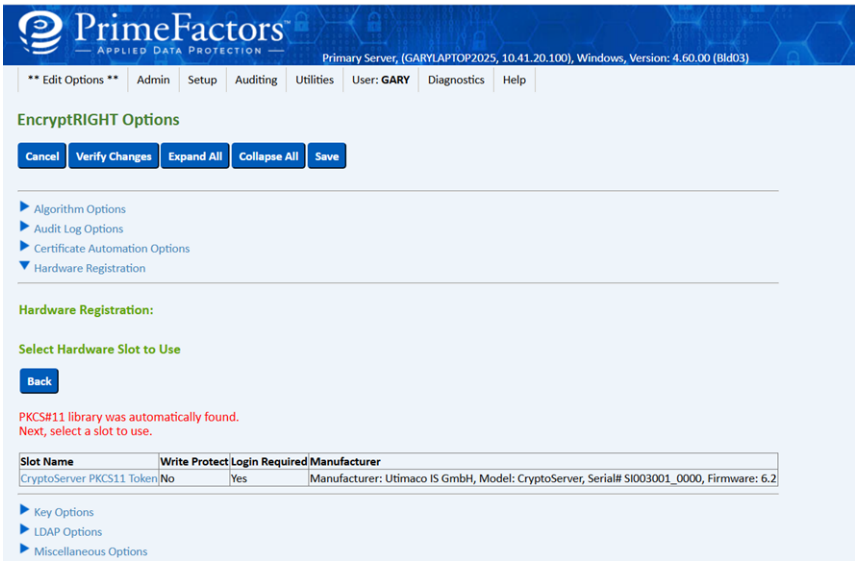

Figure 5 : Hardware registration

- Select the Slot Name to use.

Figure 6 : Hardware registration

- Enter the password

4. EncryptRIGHT uses a Hardware Master Key (HMK) that is used to setup and access all the hardware keys used that are managed by EncryptRIGHT. Normally this is a randomly generated key within the hardware and only known and used by the hardware. Data keys generated for your use will be encrypted under this KEK key and stored within the EncryptRIGHT ZSS file. When data keys are used, the HMK encrypted key value is given to the hardware API and decrypted in the hardware for use.

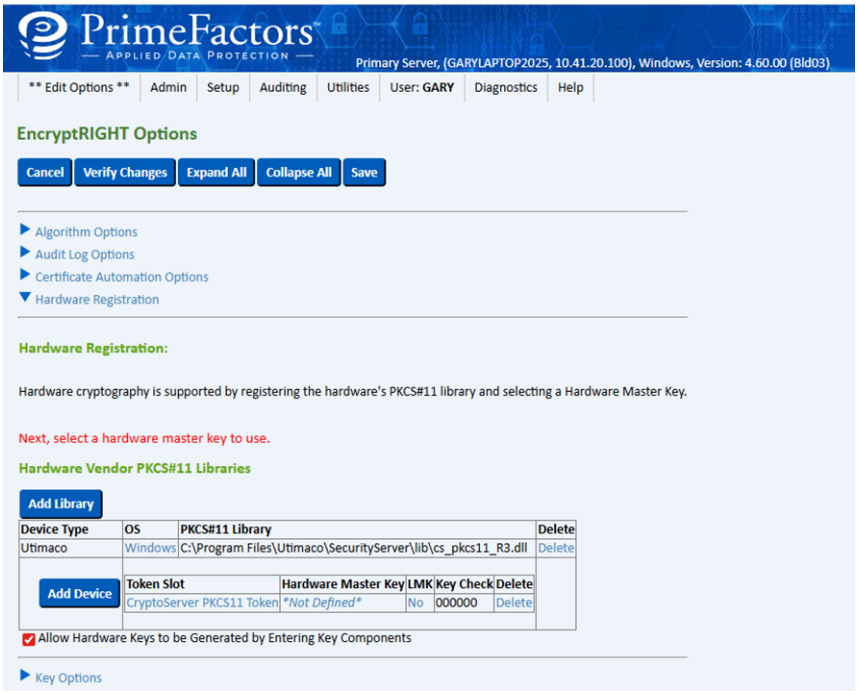

Figure 7 : Hardware vendor PKCS#11 libraries

- Select the *Not Defined* field to continue. Any existing HMK keys are listed and you may choose one, or generate a key HMK key.

Figure 8 : Hardware Master Key management

- If you choose to generate a new HMK key, press Generate.

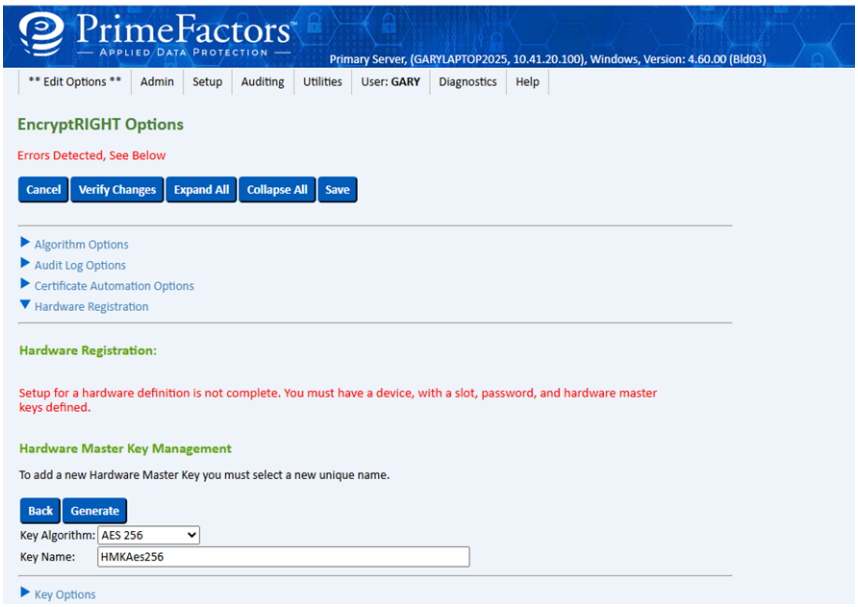

Figure 9 : Hardware Master Key management

- Select the Algorithm and enter a new key name. Press Generate.

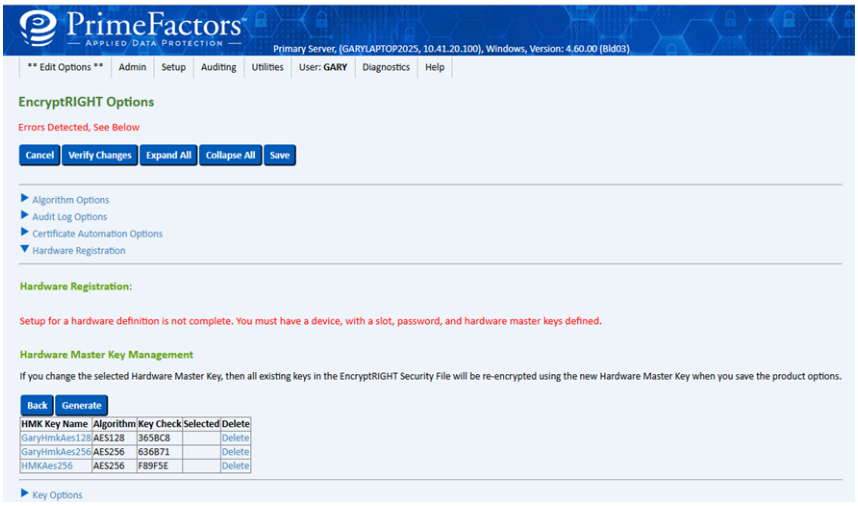

Figure 10 : Hardware Master Key management

- Select the new HMK key to use it.

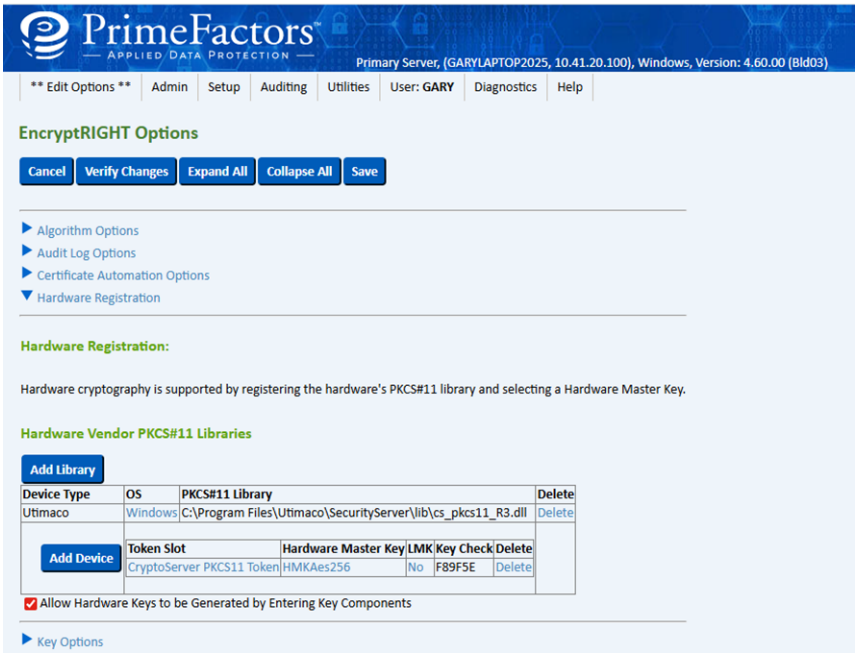

Figure 11 : Hardware vendor PKCS#11 libraries

- Press Save to save the configuration changes.

5 Integration Steps

The following section outlines the procedures required to configure both Utimaco u.trust GP HSM Se-Series and Prime Factors EncryptRIGHT components for seamless integration.

5.1 Configuration on Utimaco u.trust GP HSM Se-Series

Create users SO (Security Officer) and USR (the Crypto user) and initialize a slot.

The slot must be initialized using the p11tool2.

First, create the SO using *p11tool2*. Then, using the *p11tool2* command, initialize the Slot you want to use and the slot user, as shown below.

```
# ./p11tool2 slot=<slot no.> Label=<token label> Login=ADMIN,ADMIN.key
InitToken=<SO pin>
```

Initialize the SO user.

```
# ./p11tool2 slot=<slot no.> LoginSO=<SO pin> InitPin=<Cryptouser pin>
```

Make sure that the Utimaco GP HSM is accessible from the partner product control plane.

5.2 Configuration on EncryptRIGHT

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 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.

5.2.1 Enable HSM Protection for LMK

Selecting this option adds additional security by binding any EncryptRIGHT installation to an HSM environment. This can help protect against someone making a copy of an EncryptRIGHT

Primary Server's file system and trying to use EncryptRIGHT in another environment. If the installation cannot communicate with the HSM, it will not be able to decrypt the internal database EncryptRIGHT uses and will not be able to load any of the configuration required to encrypt and decrypt data.

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 Yes.

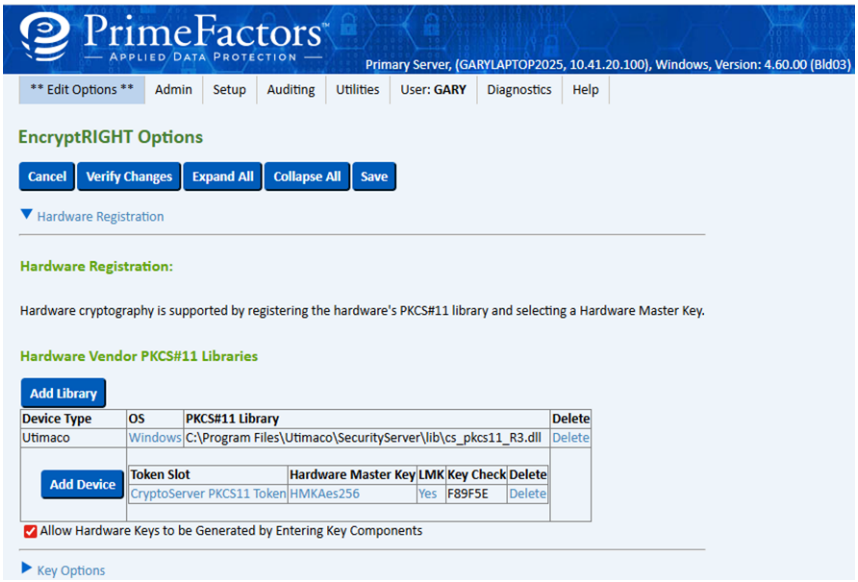

Figure 12 : Hardware vendor PKCS#11 libraries

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

5.2.2 Disable HSM Protection for LMK

The HSM 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 will then see a message confirming that LMK encryption was removed.

Figure 13 : EncryptRIGHT dashboard

5.2.3 Manage Hardware Master Keys

The 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.

Figure 14 : Hardware registration

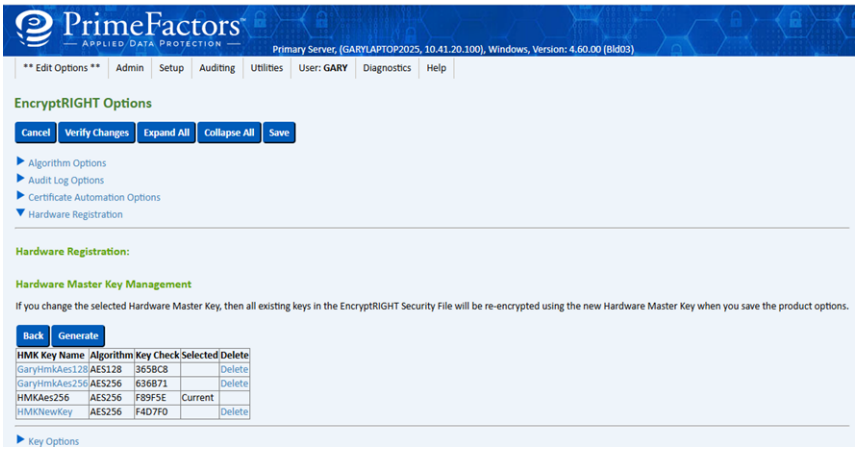

Figure 15 : Hardware Master Key management

- 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.

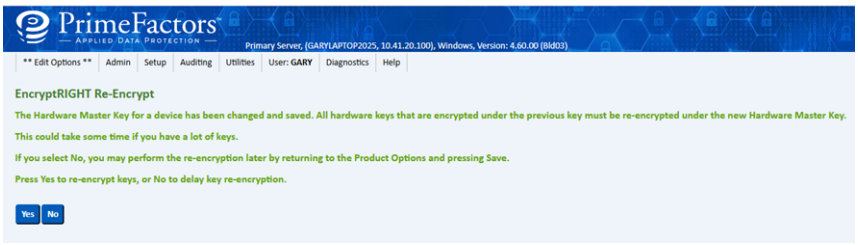

Figure 16 : EncryptRIGHT Re-Encryption prompt for Hardware Master Key update

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

Figure 17 : EncryptRIGHT PKCS#11 Hardware Key re-encryption status

EncryptRIGHT will keep the previous HMK, you can see this by displaying the hardware HMK list. You need to keep this key until all other installations have been updated with the newly re-encrypted data keys.

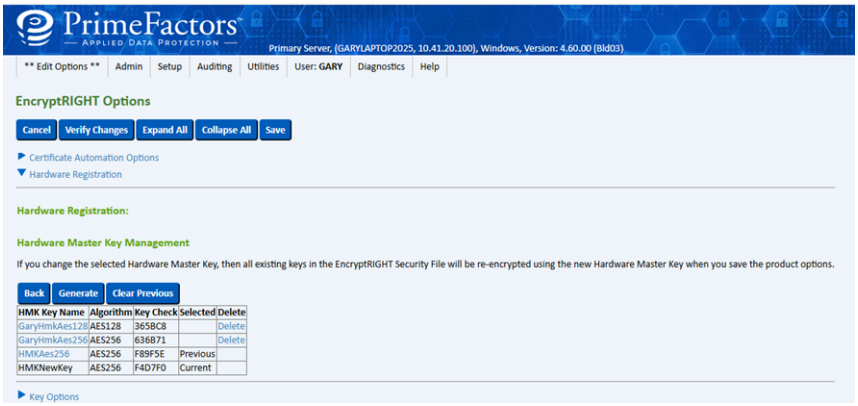

Figure 18 : EncryptRIGHT Options – Hardware Master Key management

The **Clear Previous** button indicates that all keys have been re-encrypted and the previous HMK can be deleted once all your EncryptRIGHT installations (Redundants, Expansions, Clients) are synchronized with the new information. You do not need to clear the previous HMK key right away. In fact, you should at least wait until backups of all EncryptRIGHT installations have occurred. When you feel confident that there is no reason you'll need to restore from previous backups, then the old HMK may be cleared and then deleted, if desired.

6 Verification and Testing

6.1 Logs and Validation Steps

6.1.1 PKCS#11 Logs

Enabling PKCS#11 logging to facilitate easier testing and troubleshooting is recommended. This can be done by configuring the Logging Loglevel and LogPath parameters in the configuration file.

- LogPath should point to a writable directory (not a specific file) where log files can be stored.
- Logging Loglevel controls the verbosity of the logs:
- Set it to 1 for basic logging.
- For detailed testing and debugging, increase the level to 4.

The generated log file will be named `cs_pkcs11_R3.log` and located in the directory specified by LogPath. Reviewing this log file can help identify and resolve issues that arise during testing.

Once testing is complete, it is advisable to reduce the Logging Loglevel to 1 or 2 to limit logging to only critical or important messages, thereby optimizing performance and reducing unnecessary log data.

6.1.2 EncryptRIGHT Logs

If failures are experienced in relation to hardware keys, the customer is asked to turn on Full Tracing and provide associated logs to Prime Factors so Support team can reproduce and analyze. To enable Full Tracing, set the `Logging` parameter to `4` in the EncryptRIGHT configuration (`.cfg`) file.

7 Troubleshooting

7.1 Log Locations and Interpretation

PKCS#11 Logs:

Enabling PKCS#11 logging to facilitate easier testing and troubleshooting is recommended. This can be done by configuring the Logging Loglevel and LogPath parameters in the configuration file.

- LogPath should point to a writable directory (not a specific file) where log files can be stored.
- Logging Loglevel controls the verbosity of the logs:
- Set it to 1 for basic logging.
- For detailed testing and debugging, increase the level to 4.

The generated log file will be named cs_pkcs11_R3.log and located in the directory specified by LogPath. Reviewing this log file can help identify and resolve issues that arise during testing.

Once testing is complete, it is advisable to reduce the Logging Loglevel to 1 or 2 to limit logging to only critical or important messages, thereby optimizing performance and reducing unnecessary log data.

EncryptRIGHT Logs:

If failures are experienced in relation to hardware keys, the customer is asked to turn on Full Tracing and provide associated logs to Prime Factors so Support team can reproduce and analyze. To enable Full Tracing, set the `Logging` parameter to `4` in the EncryptRIGHT configuration (`.cfg`) file.

8 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Straße 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

Any queries related to Prime Factors' EncryptRIGHT

- 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.