Paraview

Para Vault

6.8

Integration Guide

u.trust GP HSM Se-Series

6.3.0

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	2026-08-28
Status	PUBLISHED
Document No.	IG-2026-0096

Table of Contents

1 About This Guide 4
1.1 Target Audience 4
1.2 Purpose of the Integration 4
1.3 Abbreviations 4
1.4 Document Conventions 6
2 Product Overview 7
2.1 Overview of the Para Vault 7
2.2 Overview of Utimaco u.trust GP HSM Se-Series 7
2.3 Joint Value Proposition 7
3 Integration Requirements and Prerequisites 8
3.1 Tested Versions 8
3.2 Hardware and Software Requirements 8
3.3 Prerequisites 9
4 Installing and Configuring Utimaco SecurityServer Software 10
4.1 Downloading and Installing the Utimaco Software 10
4.2 Configuring cs_pkcs11_R3.cfg 10
4.3 Creating the SO User and Initializing the Slot 11
5 Integrating Para Vault with the Utimaco HSM 13
5.1 Configuring Para Vault to Enable HSM Protection 14
5.2 Enabling HSM Protection on a New Para Vault 15
5.3 Migrating an Existing Para Vault's Server Key to the HSM 15
6 Troubleshooting 17
7 Contact and Support Information 18
8 Appendices 19
8.1 References 19

1 About This Guide

This guide describes how to integrate a Utimaco u.trust GP HSM with Para Vault: the HSM generates and holds Para Vault's server key within the hardware security boundary, so that Para Vault relies on the HSM to obtain the key at startup.

1.1 Target Audience

This guide is intended for Para Vault administrators and Utimaco HSM administrators.

1.2 Purpose of the Integration

This integration ensures that privileged account passwords are protected and used securely and automatically, reducing risk and meeting compliance requirements: Para Vault's server key is protected by HSM hardware, and the key is never written to disk in plaintext.

1.3 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
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

Abbreviation	Meaning
JRE	Java Runtime Environment
MBK	Master backup key
P11CAT	the PKCS#11 graphical interface tool
CXI	Cryptographic eXtended Interface
FIPS	Federal Information Processing Standards
AES	Advanced Encryption Standard
CA	Certificate Authority
GCM	Galois/Counter Mode
IP	Internet Protocol
LAN	Local Area Network
PCIe	PCI Express Interface
PIN	Personal Identification Number
URL	Uniform Resource Locator

Table 1: Abbreviations

1.4 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`
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 the Para Vault

Para Vault is the core of the privileged access management solution. It contains a highly secure database that centrally encrypts and safeguards sensitive data such as privileged account credentials. To protect the database and the data within it, Para Vault uses a multi-layer encryption key hierarchy. Every item stored in the database is encrypted with its own randomly generated encryption key; at the top of the key hierarchy, Para Vault uses a unique server key and a unique recovery key. The server key is required to start Para Vault; following the highest security standard, this key is stored in the Utimaco Hardware Security Module (HSM).

2.2 Overview of Utimaco u.trust GP HSM Se-Series

The Utimaco u.trust GP HSM Se-Series is a hardware security module developed by Utimaco IS GmbH. It is a physically protected, specialized computer unit designed to perform sensitive cryptographic tasks and securely manage and store cryptographic keys and data. The u.trust GP HSM can be used as a universal, independent security component for heterogeneous computer systems.

2.3 Joint Value Proposition

The combination of Para Vault and Utimaco’s u.trust GP HSM delivers a highly secure privileged access management solution by protecting Para Vault's server key within a dedicated hardware security module. The HSM generates and securely stores the cryptographic key used to protect privileged credentials, ensuring that sensitive key material is never stored in plaintext on disk. This integration enhances the security of privileged account data, supports compliance requirements, and reduces the risk of unauthorized access through hardware-backed key protection.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Operating System	Partner Product	Utimaco SecurityServer Version	Utimaco HSM
Linux (containerized deployment)	Para Vault 6.8	6.3.0	u.trust GP HSM Se-Series

Table 3: Tested versions

3.2 Hardware and Software Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM Se-Series LAN with firmware SecurityServer 6.3.0 or higher
Utimaco PCI-e HSM	u.trust GP HSM Se-Series PCI-e with firmware SecurityServer 6.3.0 or higher

Table 4: List of hardware requirements

Software	Software Requirements
HSM Interface	SecurityServer PKCS#11 Provider
HSM Tool	PKCS#11 Tool version 2 (p11tool2)
Para Vault image	An HSM-capable Para Vault image (includes PKCS#11 hardware-protection capability; see Prerequisites)

Software	Software Requirements
Host tools	openssl ≥ 1.1.0 (used by epv-hsm to encrypt/decrypt the PIN); Docker/ Docker Compose

Table 5: List of software requirements

3.3 Prerequisites

Before you begin, confirm that:

- The Utimaco u.trust GP HSM has been deployed and configured.
- An MBK has been created and saved for each HSM (see the CryptoServer documentation).
- The CryptoServer default administrator has been replaced with a new administrator user.
- The operating system matches the *Tested Versions*.
- The SecurityServer version matches the *Tested Versions*.
- The PKCS#11 library has been installed and configured for the environment (see the CryptoServer documentation).
- You have the administrator privileges required to install software.
- Para Vault has been deployed and is running normally.
- Para Vault uses an HSM-capable image: This image has built-in PKCS#11 hardware-protection capability and includes a hardware-protection configuration section in its configuration template. If the current Para Vault uses an image without this capability, first upgrade to an HSM-capable Para Vault image.
- You have registered an account and obtained download permission from the Utimaco Support Portal.

Installing and deploying Para Vault is out of scope for this document.

4 Installing and Configuring Utimaco SecurityServer Software

4.1 Downloading and Installing the Utimaco Software

If you have not registered yet, first register an account on the Utimaco support portal to download the required software components. If you purchased the HSM from Utimaco, locate the corresponding software package in the accompanying product bundle. Install the latest SecurityServer software according to the SecurityServer manual. It is recommended to uninstall any existing SecurityServer software before installing a new version.

4.2 Configuring cs_pkcs11_R3.cfg

The PKCS#11 library locates the HSM through the configuration file `cs_pkcs11_R3.cfg`. Edit its `Devices` entry according to the HSM form factor:

```
[Global]
Logging = 1
Logpath = <writable log directory>
ConnectionTimeout = 5000
CommandTimeout = 60000
[HSMCluster]
# Network type (LAN appliance):
Devices = 288@<HSM-IP>
# PCIe card: Devices = /dev/cs2.0
```

- Network type (LAN): Devices = <port>@<HSM-IP> (for example, `288@10.10.x.x`); the container network must be able to route to the HSM.
- PCIe card: Devices = `/dev/cs2.0` (local device); the device must be passed through to the container.

During debugging, you can raise Logging to 4 for more detailed logs; set it back to 1 afterward. The log file is cs_pkcs11_R3.log in the Logpath directory.

Deployment on the HSM appliance side (firmware initialization, exposure as a network service, clustering/HA) is handled by HSM operations according to your deployment architecture and the official Utimaco documentation, and is out of scope for this guide.

4.3 Creating the SO User and Initializing the Slot

Use `p11tool2` to initialize the slot and set the SO (Security Officer) and user PINs. This guide creates a token on slot `0` with the label `EPV-HSM`. Para Vault locates the key by token label; the default label is `EPV-HSM` (matching the one here; if you use a different label, override it in Chapter 5 with `--token-label`).

```
# 1) Authorize as administrator, create the SO, and set the initial token PIN
p11tool2 Slot=0 Label=EPV-HSM Login=ADMIN,<ADMIN.key> InitToken=<initial PIN>

# 2) Change the initial SO PIN to the formal PIN
p11tool2 Slot=0 LoginSO=<initial PIN> SetPIN=<initial PIN>,<SO-PIN>

# 3) Initialize the user PIN
p11tool2 Slot=0 LoginSO=<SO-PIN> InitPIN=<initial PIN>

# 4) Change the initial user PIN to the formal PIN
p11tool2 Slot=0 LoginUser=<initial PIN> SetPIN=<initial PIN>,<user-PIN>
# Verify: should return USER_PIN_INITIALIZED = CK_TRUE
p11tool2 Slot=0 LoginUser=<user-PIN> GetTokenInfo
```

`InitToken/InitPIN` set only an "initial PIN"; you must run `SetPIN` again to change it to a formal PIN before you can log in and operate normally. Otherwise, subsequent operations may fail with `CKR_PIN_TOO_WEAK` due to firmware policy.

This step only initializes the slot; it does not create a key. The server key will be generated directly by the HSM in Chapter 5. `<user-PIN>` is the PIN used later when configuring Para Vault.

Security Note: The PINs above are shown as placeholders. In production, it is recommended to use p11tool2's ask mode for interactive PIN entry (to keep PINs out of the command history); see the Utimaco `p11tool2` manual for usage.

5 Integrating Para Vault with the Utimaco HSM

This chapter uses the `epv-hsm` management tool shipped with Para Vault to complete the integration and verification. `epv-hsm` runs on the host where Para Vault runs and provides the following subcommands:

Subcommand	Purpose
`encrypt-pin`	Encrypt the HSM PIN into ciphertext (for use by set-pin)
`set-pin`	Accept the PIN ciphertext and store it as ciphertext (no plaintext on disk)
`check`	Pre-migration checks (PIN / driver mount / orchestration file / container status)
`enable`	Enable HSM protection on a new Para Vault
`migrate`	Migrate an existing Para Vault to HSM protection (idempotent)
`verify`	Component-level verification (key / protection mode / auto-start on restart / data read-write)
`status`	Show the current protection mode and running status

Component-level verification note: The verification in this chapter targets only the Para Vault and HSM components themselves (whether the server key is in the HSM, whether the service can start, and whether data can be read and written normally). It can be self-attested with only Para Vault and the HSM, without relying on any other business system.

5.1 Configuring Para Vault to Enable HSM Protection

Para Vault's HSM configuration is managed by the `epv-hsm` tool; operators do not need to manually edit any Para Vault configuration file. The HSM address is in the Utimaco driver configuration `cs_pkcs11_R3.cfg` (see *Configuring cs_pkcs11_R3.cfg* section); all other parameters (driver path, token label, key label, algorithm) have default values and can be overridden with command-line options during `enable` / `migrate` in advanced scenarios.

For a standard deployment, operators need only three steps:

1. Ensure that the host (or container) running Para Vault can reach the HSM over the network (network type), or that the PCIe device has been passed through; confirm that Para Vault uses an HSM capable image and has mounted the Utimaco PKCS#11 driver library (`libcs_pkcs11_R3.so`) and configuration file (`cs_pkcs11_R3.cfg`). The HSM address is already configured in `cs_pkcs11_R3.cfg` . For details, see *Configuring cs_pkcs11_R3.cfg* section.
2. Store the HSM PIN (as ciphertext: first encrypt it to obtain the ciphertext, then pass it to set-pin, which saves it as ciphertext with 600 permissions — both what the operator handles and what is stored are ciphertext):

```
# 1) Encrypt the PIN; enter it when prompted to obtain a ciphertext string
sudo epv-hsm encrypt-pin

# 2) Pass the ciphertext from the previous step to set-pin for storage
sudo epv-hsm set-pin <ciphertext from the previous step>
```

3. Run the pre-check to confirm the basic prerequisites are in place (PIN configured, HSM driver mounted into the container, orchestration file present, Para Vault container running):

```
sudo epv-hsm check
```

Advanced (usually not needed): The driver path / token label / key label / algorithm all have default values (standard driver path / `EPV-HSM` (see 4.3) / `epv-server-key` / AES-GCM) that take effect internally. Only when they differ from the defaults, override them in the next section during `enable` / `migrate` with the corresponding option, for example `sudo epv-hsm enable --token-label <label> --key-label <label>` .

The HSM configuration only takes effect when Para Vault is rebuilt during enable / migrate in the next section.

5.2 Enabling HSM Protection on a New Para Vault

In the most secure deployment method, the server key is generated directly within the HSM's secure environment and stored as a non-exportable key in the HSM's PKCS#11 slot for Para Vault to use.

1. Complete the configuration in the *Configuring Para Vault to Enable HSM Protection* section.
2. Enable HSM protection (upon first initialization, the server key is generated inside the HSM). After enabling, this command automatically runs component-level verification:

```
sudo epv-hsm enable
```

3. Keep the recovery key safe: the recovery key is used for disaster recovery and for re-issuing the administrative token. Store it in a distributed manner according to your organization's key custody policy.
4. Confirm the verification result at the end of the command (`enable` runs it automatically; example, tool output is in English):

```
== HSM protection verification ==
[1/4] HSM key check ........... PASS (server key is in the HSM and was used to
start successfully)
[2/4] Protection mode ......... HSM-based hardware protection
[3/4] Auto-start on restart ... PASS (no manual key entry required)
[4/4] Data read-write check ... PASS
Conclusion: Para Vault is protected by the HSM and operating normally.
```

To re-check at any time, you can run `sudo epv-hsm verify` on its own (it triggers one container restart to verify "auto-start on restart").

5.3 Migrating an Existing Para Vault's Server Key to the HSM

To migrate a Para Vault that is already running to HSM hardware protection:

1. Complete the configuration in the *Configuring Para Vault to Enable HSM Protection* section.
2. Perform the migration (the tool automatically obtains the key and switches over, with no manual key entry; the command can be run repeatedly and is idempotent). After the migration completes, this command automatically runs component-level verification:

```
sudo epv-hsm migrate
```

3. Keep the recovery key safe: after the migration completes, the credentials previously used for software protection become the recovery key (for disaster recovery). Store it safely.
4. Confirm the verification result at the end of the command (`migrate` runs it automatically; output is the same as *Enabling HSM Protection on a New Para Vault* section). To re-check at any time, you can run `sudo epv-hsm verify` on its own.

During migration, if the service fails to start because the HSM is unreachable or the PIN is incorrect, the existing software protection is unaffected. After fixing the issue, simply run `sudo epv-hsm migrate` again (idempotent). This completes the integration of Para Vault with the Utimaco u.trust GP HSM.

6 Troubleshooting

Symptom	Action
epv-hsm check fails	Complete the missing items as prompted: configure the PIN with `epv-hsm encrypt-pin` + `set-pin`, confirm the HSM driver is mounted into the container, the orchestration file exists, and the Para Vault container is running.
Enable/migrate hangs or does not start for a long time	Usually the HSM is unreachable: check the `Devices` entry in `cs_pkcs11_R3.cfg` (IP/port or device file), network connectivity/device pass-through; for the LAN type, confirm the container can route to the HSM.
Enable/migrate reports a PIN error	Re-encrypt the correct user PIN with `epv-hsm encrypt-pin` and store it with `set-pin`; confirm that the initial PIN was changed to a formal PIN as described in Section 4.3.
Key label mismatch	Confirm the key label (default `epv-server-key`, or the value provided via `--key-label`) matches the one on the HSM. For a new deployment, use `epv-hsm enable` to have the HSM generate the key.
Re-running after an interrupted migration	`epv-hsm migrate` is idempotent: it automatically detects the current state and continues or skips; existing protection remains unaffected until the switchover completes.
epv-hsm verify "auto-start on restart" fails	Check HSM reachability and driver mount; use `epv-hsm status` to view the protection mode and running status.

7 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.

8 Appendices

8.1 References

Reference	Title / Source
[CSP11Tool2]	CryptoServer p11tool2 Manual / Utimaco IS GmbH
[PKCS#11]	PKCS #11 Cryptographic Token Interface Standard / OASIS

Table 6: References