KNOT DNSSEC

3.1.8

Integration Guide

Security Server

4.45.3.0

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	2026-03-02
Status	PUBLISIHED
Document No.	IG-2026-0031

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle. All Utimaco SecurityServer product documentation is available from Utimaco's website at https://utimaco.com/.

1.1 About This Guide

This guide describes how to enable HSM integration with KNOT DNSSEC. The instructions in this document have been thoroughly tested and provide a straightforward integration process. There may be other untested ways to achieve interoperability.

1.2 Target Audience for This Guide

This guide is intended for administrators of KNOT DNSSEC and of Utimaco HSMs.

1.3 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 1: 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.

1.4 Abbreviations

Abbreviation	Meaning
CD	Compact Disc
CSADM	CryptoServer Command-line Administration Tool
CSAR	Cloud Service Architecture
DNF	Dandified YUM
GUI	Graphical User Interface
GP HSM	General Purpose Hardware Security Module
HSM	Hardware Security Module
Abbreviation	Meaning

Abbreviation	Meaning
IP	Internet Protocol
KNOT DNS	Knot Domain Name System
LAN	Local Area Network
MBK	Master Backup Key
PCI-e	PCI Express Interface
PKCS#11	Public-Key Cryptography Standard #11
SMP	Service Metadata Publisher
SO	Security Officer
TLD	Top-Level domain
YUM	Yellowdog Updater Modified
URL	Uniform Resource Locator

Table 2: Abbreviations

2 Overview

2.1 KNOT DNS

KNOT DNS is a high-performance open-source DNS server. It implements only the authoritative domain name service. KNOT DNS can reliably serve TLD domains as well as any other zones. KNOT DNS benefits from its multi-threaded and mostly lock-free implementation which allows it to scale well on SMP systems and operate non-stop even when adding or removing zones. The server itself is accompanied by several utilities for general DNS operations or for maintaining the server. To enhance your systems security KNOT DNS can store signing keys on the Utimaco GP HSM.

2.2 Utimaco CryptoServer HSM

CryptoServer is a hardware security module or HSM, a physically protected specialized computer designed to securely perform sensitive cryptographic operations, manage, and store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

This integration guide will take you step by step through the process of integrating KNOT DNS with the UtimacoGP HSM using PKCS#11 as the cryptographic provider.

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 required Software.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with KNOT DNS:

Operating System	KNOT Version	Utimaco Security Server Version	Utimaco HSM
Rhel 8.2 Ubuntu 20.4	3.1.8	SecurityServer V4.45.3.0	CryptoServer CSe-Series/ Se-Series

Table 3: Tested versions

3.2 Software Requirements

Software	Version
HSM Interfaces	SecurityServer PKCS#11 Provider
Utimaco Crypto Server Software	V4.45.3.0
KNOT Version	3.1.8

Table 4: Software requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.45.3 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.45.3 or higher

Table 5: Hardware requirements

Create an account in the Utimaco portal and request download access from the following URL: https://support.hsm.utimaco.com

3.4 Prerequisites

Before you begin, please ensure that you have installed/setup:

- Operating system listed in Tested Versions
- SecurityServer listed in Tested Versions
- Familiarize yourself with the KNOT DNS documentation
- Utimaco CryptoServer HSM is set up and configured, see the CryptoServer documentation to set up the HSM.

4 Configuring Utimaco PKCS#11

Create the `/etc/utimaco` directory. We will copy the Utimaco PKCS#11 configuration file `cs_pkcs11_R3.cfg` into this directory. It is located in the CryptoServer-V4.45.3 directory `Linux/x86-64/Crypto_APIS/PKCS11_R3/sample`.

›_ Console

```
# mkdir /etc/utimaco

# cd <install directory>/Software/Linux/x86-

64/Crypto_APIs/PKCS11_R3/sample

# cp cs_pkcs11_R3.cfg /etc/utimaco

# cd /etc/utimaco
```

Edit the `cs_pkcs11_R3.cfg` file located in `/etc/utimaco/` and update the device specifier entry with the IP address of the HSM device being used, e.g. `288@172.23.0.55`.

If required, also make changes for e.g `Logpath = /tmp, Logging = 0`.

For more information regarding the commands and command parameters check the Utimaco documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

`Device = 288@<HSM IP address>` *Hardware (LAN) HSM*

OR

`Device = /dev/cs2.0` *Hardware (PCIe) HSM*

To make testing easier, you can enable the PKCS#11 log file. It can be enabled by adding the entries for Logpath and `Logging` to the configuration file. The added `Logpath` points to a writable directory, not to a file. Logging can have values `0` to

`4` . For testing you can increase it to `4` . When you are done, you should change Logging to `1` or `2` . This will limit the logging to only critical and important messages.

If you encounter problems, check the log file `cs_pkcs11_R3.log` in the under `Logpath` defined directory.

Example values:

```
cs_pkcs11_R3.cfg
```

```
# Path to the logfile (name of logfile is attached by the API)

# For unix:

Logpath = /tmp # For windows:

#Logpath = C:/ProgramData/Utimaco/PKCS11_R3

# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE) Logging
= 4

# Maximum size of the logfile in bytes (file is rotated with a backupfile
if full) Logsize = 10mb

# Created/Generated keys are stored in an external or internal database

KeysExternal = false

# If true, every session establishes its own connection

SlotMultiSession = true

# Maximum number of slots that can be used

SlotCount = 10

# If true, leading zeroes of decryption operations will be kept

KeepLeadZeros = false

# Configures load balancing mode ( == 0 ) or failover mode ( > 0 )

# In failover mode, n specifies the interval in seconds after which a
reconnection attempt to the failed CryptoServer is started.
FallbackInterval = 0

# Prevents expiring session after inactivity of 15 minutes KeepAlive =
false

# Timeout of the open connection command in ms

ConnectionTimeout = 5000

# Timeout of command execution in ms
```

```
CommandTimeout = 60000

# List of official PKCS#11 mechanisms which should be customized

#CustomMechanisms = { CKM_AES_CBC CKM_AES_ECB }

# Enforce thread-safety by using the operating system locking primitives

#ForceOSLocking = true

#[CryptoServer]

# Device specifier (here: CryptoServer is internal PCI device)

# For unix: #Device = /dev/cs2 # For windows:

#Device = PCI:0

[CryptoServer]

# Device specifier (here: CryptoServer is CSLAN with IP address
192.168.0.1)

#Device = 192.168.0.1

#[CryptoServer]
```

5 Setting up the Utimaco HSM

We will access the HSM using the IP address of the GP HSM device.

5.1 Initialize a Slot

KNOT DNS uses the token label to specify the slot to be used. To avoid problems, make sure the token label you are using is unique.

To initialize a slot with a custom label, use the following commands on the machine where you installed the p11tool2 tool.

The first p11tool2 command creates the SO or Security Officer for slot 0 user and the second p11tool2 command initializes the slot 0 user.

5.2 Setting up your PKCS#11 users

Follow the Utimaco documentation for setting up your PKCS#11 users.

For our example we have chosen the HSM PIN as "123456", to be used for our SO and Crypto User.

›_ Console

```
# /opt/utimaco/bin/p11tool2 slot=0 Label=KNOTDemo

Login=KNOTADMIN,KNOTADMIN.key InitToken=123456

# /opt/utimaco/bin/p11tool2 slot=0 LoginSO=123456 InitPin=123456
```

5.3 Check the Slot

Check the PKCS#11 slot. The results should look like the output below.

›_ Console

```
# /opt/utimaco/bin/p11tool2 LoginUser=123456 GetSlotInfo  CK_SLOT_INFO
(slot ID: 0x00000000):

slotDescription     3130332e 362e3333  2e313231 202d2053   |103.6.33.121 -
S |
4c4f545f 30303030  20202020 20202020   |LOT_0000         |
20202020 20202020  20202020 20202020   |                 |
20202020 20202020  20202020 20202020   |                 |
manufacturerID     5574696d 61636f20  49532047 6d624820    | Utimaco IS
GmbH |
   20202020 20202020  20202020 20202020 |                 |
flags: 0x00000005
CKF_TOKEN_PRESENT    : CK_TRUE
CKF_REMOVABLE_DEVICE : CK_FALSE
CKF_HW_SLOT          : CK_TRUE
hardwareVersion        : 5.01
firmwareVersion        : 2.04
```

5.4 List users and verify MBK

Use the `csadm` command `listusers` and confirm the created users.

›_ Console

```
# /opt/utimaco/bin/csadm DEV=192.168.10.10 listusers

Name          Permission    Mechanism      Attributes

KNOTADMIN      22000000      RSA sign        Z[0]

SO_0000        00000200      HMAC passwd     A[CXI_GROUP=SLOT_0000]

USR_0000       00000002     HMAC passwd      Z[0]A[CXI_GROUP=SLOT_0000]
```

Now, check to confirm the Utimaco HSM has an MBK.

›_ Console

```
# /opt/utimaco/bin/csadm DEV=192.168.10.10
LogonSign=KNOTADMIN,KNOTADMIN.key MBKListKeys
slot name len  algo  type  k  generation  date  key check value

-----------------------------------------------------------------

3  MYMBK  32   AES   XOR   2 2012/08/15 13:08:39
CC06067E3C8692DE:D53279C7B862EC54
```

6 Installing KNOT DNS

Follow the steps below to download and install the KNOT DNS and set up the system environment to support the integration. KNOT DNS is distributed as a binary package or is available to install from source code for all Linux platforms.

6.1 Installing using yum/dnf

Run the commands below to install KNOT and its dependencies

›_ Console

```
# dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-
8.noarch.rpm
# dnf install knot
# dnf install https://rpmfind.net/linux/centos/8-
stream/AppStream/x86_64/os/Packages/fstrm-0.6.1-2.el8.x86_64.rpm
# dnf install knot-utils
```

Use

- yum for rhel 7
- dnf for rhel 8
- apt for ubuntu

6.2 Installing using Source Code

Steps for Installing using source code

1. Install the following dependent packages.

- make
- libtool

- pkg config
- autoconf >= 2.65
- python sphinx (optional, for documentation building)

2. Download and install GCC version 4.1 or above.
3. Download KNOT DNS from https://gitlab.nic.cz/knot/knot-dns.git .

›_ Console

```
#git clone https://gitlab.nic.cz/knot/knot-dns.git
```

4. Go inside KNOT directory and run the following commands to compile and install KNOT DNS

›_ Console

```
cd  knot   autoreconf -if ./configure make make install ldconfig
```

6.3 Configuring KNOT for Utimaco HSM

1. Copy and use the sample zone file from the path below.

›_ Console

```
# cp /usr/share/doc/knot/samples/example.com.zone  /var/lib/knot/
```

2. The default knotd logs are saved in syslog. If you want to store the knotd logs as a separate file, you need to manually create the file with the appropriate permission and specify its location in the `/etc/knot/knot.conf` file in the log section.

chmod 777 /tmp/cs_pkcs11_R3.log

3. Open knot.conf file and make the following changes for Utimaco:

›_ Console

```
# This is a sample of a minimal configuration file for Knot DNS.
# See knot.conf(5) or refer to the server documentation.

 server:
    rundir: "/run/knot"
    user: knot:knot
    automatic-acl: on

    background-workers: 2
#   listen: [ 127.0.0.1@53, ::1@53 ]

 log:
- target: /var/log/knotd.log
any: debug
control: debug
zone: debug
server: debug

  database:
storage: "/var/lib/knot"

 remote:
#  - id: secondary
#    address: 192.168.1.1@53
#
#  - id: primary
#    address: 192.168.2.1@53

 template:
- id: default
storage: "/var/lib/knot"
file: "%s.zone"
```

›_ Console

```
keystore:
- id: UtimacoHSM
backend: pkcs11
config: "pkcs11:slot-id=0;pin-value=123456 /usr/local/lib/
libcs_pkcs11_R3.so"

 policy:
- id: MyRSAPolicy
algorithm: RSASHA256
ksk-size: 2048
zsk-size: 2048
ksk-lifetime: 1h
zsk-lifetime: 10m
propagation-delay: 5s
dnskey-ttl : 30s
#zone-max-ttl : 30s
keystore: UtimacoHSM

 zone:
#    # Primary zone
#  - domain: example.com
#    notify: secondary

#    # Secondary zone
#  - domain: example.net
#    master: primary


- domain:example.com
storage: /var/lib/knot
file: example.com.zone
dnssec-signing: on
dnssec-policy: MyRSAPolicy
```

4. After you changed the `knot.conf` file start the knot service using the commands below:

›_ Console

```
Systemctl daemon reload

Systemctl start knot
```

Or if you are using source code:

›_ Console

```
Knot -c <path to knot configuration file>/knot.conf
```

6.4 Verify that domain Signed in Zone File

Verify that the zone file looks like below, before domain signing:

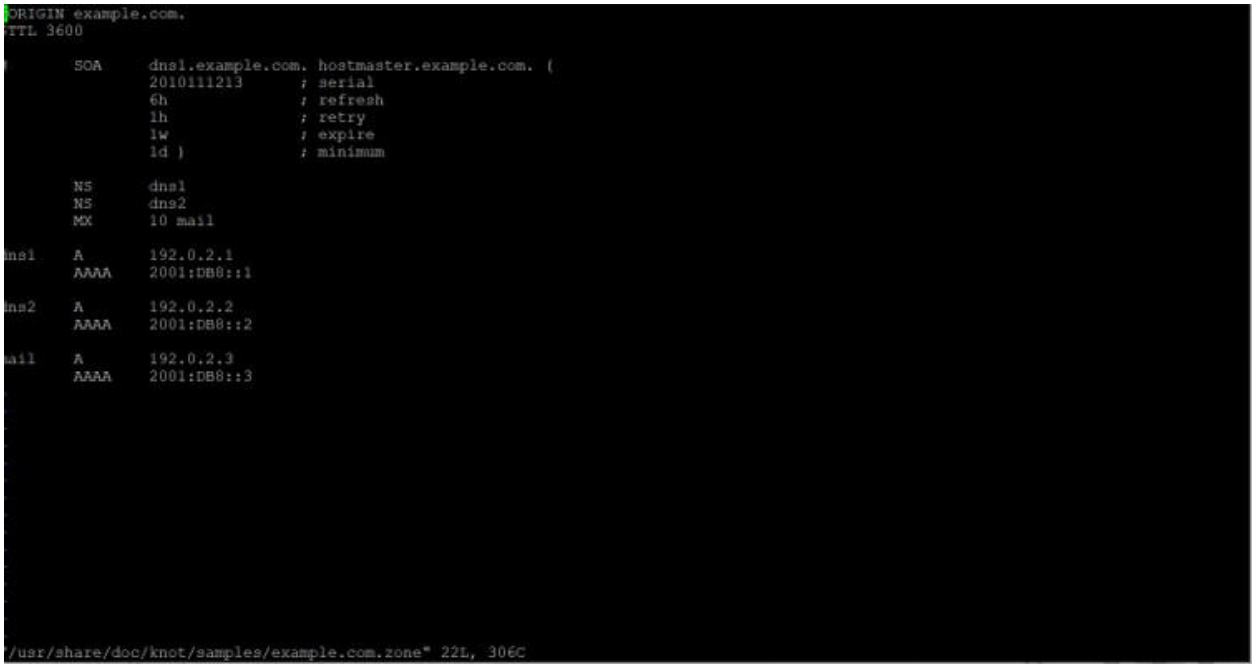

Figure 1 : Zone file window

Verify that zone file looks like below after domain signing:

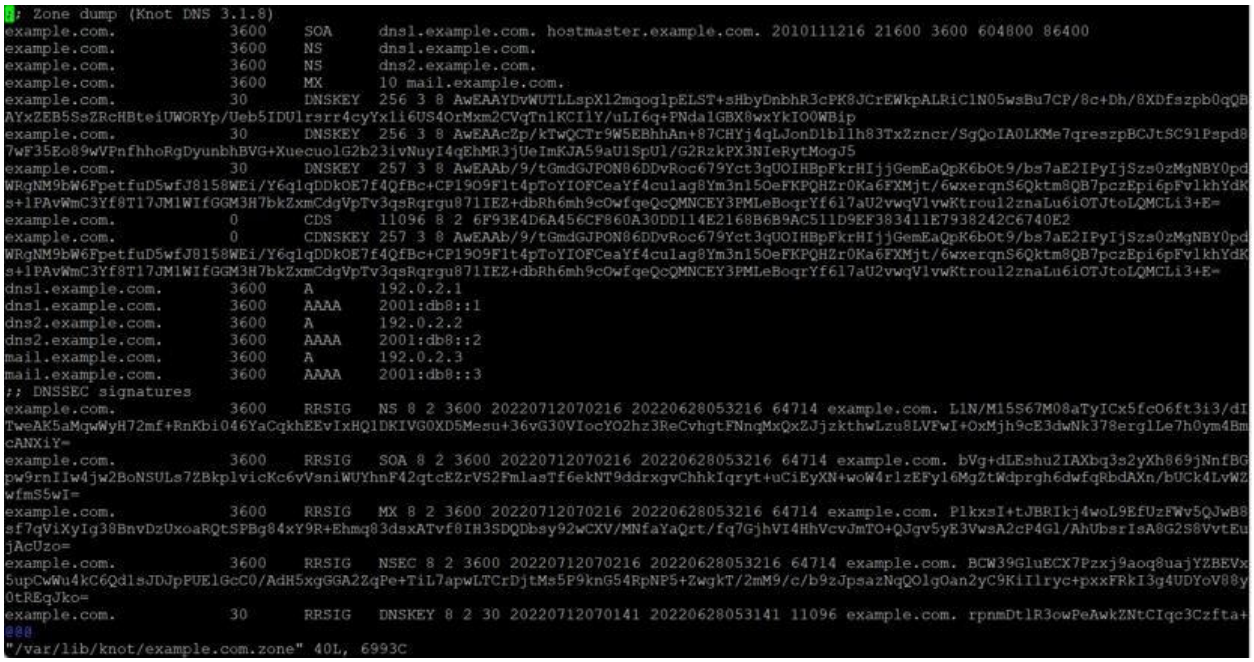

Figure 2 : Zone file window

This concludes that the integration of KNOT DNS with Utimaco HSM has been completed successfully.

7 Troubleshooting

Error	Diagnosis
error: [example.com.] DNSSEC, failed to initialize signing context (PKCS #11 token not available)	Verify that there is connectivity between KNOT and Utimaco HSM. Also verify that the Slot is available to KNOT.
error: [example.com.] failed to parse zone file '/var/lib/knot/example.com.zone' (operation not permitted)	Make sure that the zone file has all the entries in correct format and there is no unallowed entries in it.
Irrespective of whichever slot has been initialized in p11tool2 command, knot dns will only use slot 0 for signing key generation..	This is expected behavior as knot dns will only use slot 0

Table 6: List of errror and its diagnosis

8 Further Information

This document is part of the information and support that is provided by Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website:

https://utimaco.com/

9 References

Reference	Title/Company	Document No.
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSTrSh]	CryptoServer Troubleshooting/Utimaco IS GmbH	M011-0008-en
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSP11Tool2]	CryptoServer_p11tool2_Manual.pdf	2012-0004
[CSPKCSM]	CryptoServer - PKCS#11 P11CAT Manual	M013-0001-en
[CSLAN5]	CryptoServerLAN_Manual_Systemadministrators.pdf	2018-0004