OpenVPN

2.6.6

Integration Guide

CryptoServer HSM

SecurityServer 4.60.0.0

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	2026-07-20
Status	PUBLISHED
Document No.	IG-2026-0074

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 provides an integration guide explaining how to integrate a Utimaco SecurityServer Hardware Security Module (HSM) with OpenVPN. Utimaco SecurityServer securely generates and stores the private key and certificate of a client used by OpenVPN for authentication.

1.2 Target Audience for This Guide

This guide is intended for administrators of OpenVPN 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	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

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 marks the result expected after the successful execution of an instruction.

1.4 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
CA	Certificate Authority
CD	Compact Disc
CSADM	CryptoServer Command-line Administration Tool
CSR	Certificate Signing Request
GUI	Graphical User Interface
HSM	Hardware Security Module
IP	Internet Protocol

Abbreviation	Meaning
LAN	Local Area Network
MBK	Master Backup Key
P11CAT	PKCS#11 CryptoServer Administration Tool
PCIe	PCI Express Interface
PIN	Personal Identification number
PKI	Public Key Infrastructure
PKCS#11	Public-Key Cryptography Standard #11
RSA	Rivest-Shamir-Adleman
SO	Security Officer
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network

Table 2: List of abbreviations

2 Overview

2.1 OpenVPN

OpenVPN is a virtual private network system that implements techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It implements both client and server applications.

For customers that require additional security, OpenVPN can be used to integrate with Hardware Security Modules (HSMs) such as the Utimaco SecurityServer HSM. This provides the ability to configure OpenVPN to use the authentication key and certificate stored on and managed by the HSM.

2.2 Utimaco SecurityServer HSM

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

2.3 Utimaco u.trust Anchor

u.trust Anchor is the next generation hardware security module platform developed by Utimaco IS GmbH. u.trust Anchor is a physically protected specialized computer unit designed for true multi-tenancy, performing sensitive cryptographic tasks, and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Integration Requirements and Prerequisites

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

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with OpenVPN.

Operating System	OpenVPN Version	Utimaco Security Server Version	Utimaco HSM
Windows Server 2019	2.6.6	SecurityServer 4.60.0.0	CryptoServer CSe-Series/Se-Series u.trust Anchor Se*k and u.trust Anchor CSAR

Table 3: List of tested versions

3.2 Software Requirements

Software	Software Requirements
Java	Version 8, Update 271 or higher
OpenVPN	2.6.6
HSM Interfaces	SecurityServer PKCS#11 Provider

Software	Software Requirements
HSM Utility	SecurityServer PKCS#11 Tool (p11tool2)

Table 4: List of software requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.60.0.0 or higher u.trust Anchor Se*k and u.trust Anchor CSAR Series LAN with firmware 4.60.0.0 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.60.0.0 or higher u.trust Anchor Se*k and u.trust Anchor CSAR Series PCI-e with firmware 4.60.0.0 or higher

Table 5: List of hardware requirements

Set up an account on the Utimaco support portal and request download access at the following URL https://support.hsm.utimaco.com/ .

3.4 Prerequisites

Before you begin, please ensure that:

- The operating system is listed in *Tested Versions*.
- The SecurityServer is listed in *Tested Versions*.
- The SecurityServer Default Admin has been replaced with a new admin user.

- The MBK has been created and stored onto each HSM. Refer to the SecurityServer documentation to set up the MBK.
- The SecurityServer is set up and configured. Refer to the SecurityServer documentation to set up the HSM.
- The PKCS#11 library is set up and configured as per your environment. Refer to the

SecurityServer documentation to set up and configure the PKCS#11 library.

- Download OpenVPN from *https://openvpn.net/community-downloads/* and install it by following steps from *https://openvpn.net/community-resources/installingopenvpn/.*

The steps for installation of OpenVPN are out of scope of this document. Please follow above links for more information about OpenVPN installation and configuration.

- Familiarize yourself with the OpenVPN documents and setup process.

4 Installing and Configuring Utimaco SecurityServer Software

4.1 Download Utimaco Software

If you have not already done so, please create and request an Utimaco Support Portal Account. This will allow you to download the software components needed for this installation.

If you have purchased an HSM from Utimaco, locate the included product bundle, which contains the Windows software packages.

Install the latest version of the SecurityServer software as described in the SecurityServer Manual for the HSM. We recommend that you uninstall any SecurityServer software before installing the new software.

4.2 Update cs_pkcs11_R3.cfg

On Windows, as part of CryptoServer software installation, cs_pkcs11_R3.cfg will be automatically created and will be available under the `C:\ProgramData\Utimaco\PKCS11_R3` folder.

cs_pkcs11_R3.cfg

```
[Global]
# 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 more information regarding the commands and command parameters please check the Utimaco CryptoServer 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 your testing easier, it would be good to enable the PKCS#11 log file. That can be enabled by editing the **Logging Loglevel**. Set the **LogPath** and **Logging Loglevel** to 1. For testing you may want to increase it to 4.

The added **LogPath** points to a writable directory, not to a file.

If you encounter problems, check the log file named `cs_pkcs11_R3.log` in the **LogPath** defined directory. When you are done testing, you should change **Logging** to 1 or 2. This will limit the logging to only critical and important messages.

4.3 Create SO User and Initialize a Slot

You must initialize a slot with a custom label using p11tool2.

First, using p11tool2 create the SO or Security Officer and then using the p11tool2 command initialize the slot that you want to use, as well as the slot user.

›_ Console

```
> p11tool2 slot=<slot_no.> Label=<token_label> Login=ADMIN,<ADMIN.key>
InitToken=ask

> p11tool2 slot=<slot_no.> LoginSO=ask SetPin=ask,ask

> p11tool2 slot=<slot_no.> LoginSO=ask InitPIN=ask

> p11tool2 slot=<slot_no.> LoginUser=ask SetPIN=ask,ask
```

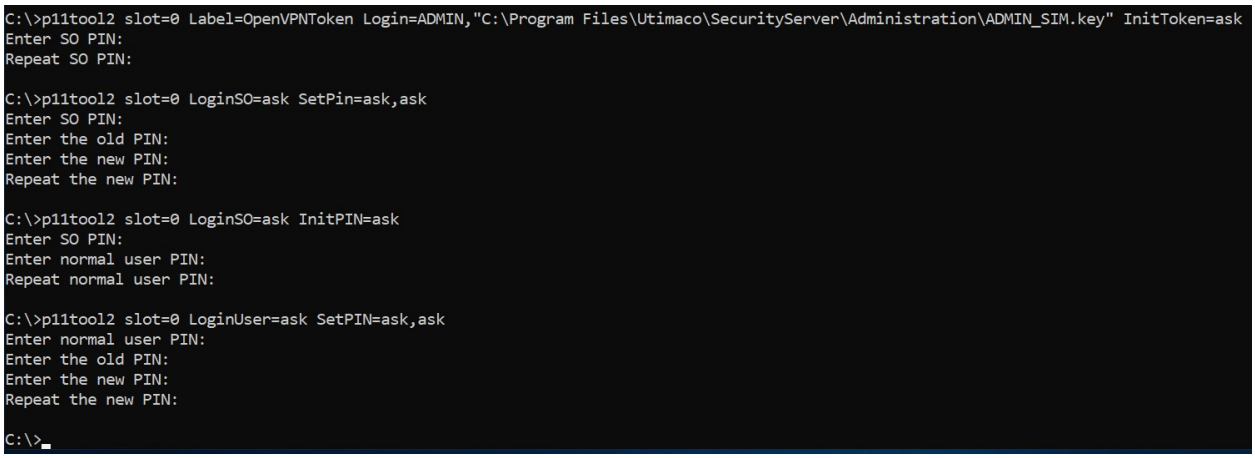

Figure 1 : Slot initialization output

Alternatively, you can also use the p11CAT tool to initialize a token and create a SO user. After that you can set a normal user PIN.

5 Integrating OpenVPN with Utimaco HSM

5.1 (Optional) Install and Configure Certificate Authority

Steps below are only for demonstration. Follow OpenVPN documentation for more details about the CA configuration for production environment.

1. Go to directory `C:\Program Files\OpenVPN\easy-rsa` and run `EasyRSA-Start.bat`.

›_ Console

```
> EasyRSA-Start.bat
```

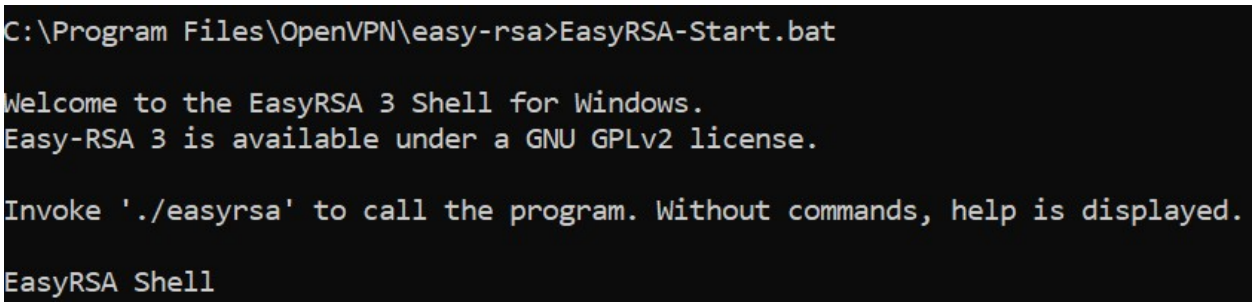

Figure 2 : EasyRSA shell

2. Initializes the PKI directory for a new PKI.

›_ Console

```
> ./easyrsa init-pki
```

```
# ./easyrsa init-pki

WARNING
=======
Using Windows-System-Folders for your PKI is NOT SECURE!
Your Easy-RSA PKI CA Private Key is WORLD readable.

To correct this problem, it is recommended that you either:
* Copy Easy-RSA to your User folders and run it from there, OR
* Define your PKI to be in your User folders. EG:
  'easyrsa --pki-dir="C:/Users/<your-user-name>/easy-rsa/pki" <command>'


Notice
------
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* C:/Program Files/OpenVPN/easy-rsa/pki

* Using Easy-RSA configuration: Not found

* IMPORTANT: Easy-RSA 'vars' template file has been created in your new PKI.
             Edit this 'vars' file to customise the settings for your PKI.
             To use a global vars file, use global option --vars=<YOUR_VARS>

* Using x509-types directory: C:/Program Files/OpenVPN/easy-rsa/x509-types


EasyRSA Shell
```

Figure 3 : init-pki command output

3. Creates a new CA.

›_ Console

```
> ./easyrsa build-ca nopass
```

```
# ./easyrsa build-ca nopass

* Using Easy-RSA configuration:
  C:/Program Files/OpenVPN/easy-rsa/pki/vars

WARNING
=======
Using Windows-System-Folders for your PKI is NOT SECURE!
Your Easy-RSA PKI CA Private Key is WORLD readable.

To correct this problem, it is recommended that you either:
* Copy Easy-RSA to your User folders and run it from there, OR
* Define your PKI to be in your User folders. EG:
  'easyrsa --pki-dir="C:/Users/<your-user-name>/easy-rsa/pki" <command>'


* Using SSL: openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)

Using configuration from C:/Program Files/OpenVPN/easy-rsa/pki/73e5f399/temp.5.1
...+.........++++++++++++++++++++++++++++++++++++++++*.+..+...+....+......+.........+..+.
...+.+...+.....+.+.....+......+.+...+..+.........+........+.......+..............+..+.
....+..........+...+..+...+......+......+.........+.........+.....+....+.+..+..........
......+............+...+.......+..............+.+...+.........+..++++++
............+.......+...+...+.........+...++++++++++++++++++++++++++++++++++++*...+..
.+.....+....+..+................+.....+..........+..+...+....+...+............+...+.....
+..+.......+.....+...+.+.....+.+...........+............+.....+.+......+..............
..+...+..+......+......+...+.......+...+..............+........+...+..................
...+..+.+........+...........+.........+....+.........+...+..+.+.....+......+....+.....
.+...+.+.........+...........+...+......+.+.....+.+..+.+..+.........+............+.....
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

Figure 4 : Building CA

```
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:OpenVPN

Notice
------
CA creation complete. Your new CA certificate is at:
* C:/Program Files/OpenVPN/easy-rsa/pki/ca.crt


EasyRSA Shell
```

Figure 5 : Building CA

4. Generate a keypair and certificate for the server.

›_ Console

```
> ./easyrsa build-server-full server nopass
```

```
EasyRSA Shell
# ./easyrsa build-server-full server nopass

* Using Easy-RSA configuration:
  C:/Program Files/OpenVPN/easy-rsa/pki/vars

WARNING
=======
Using Windows-System-Folders for your PKI is NOT SECURE!
Your Easy-RSA PKI CA Private Key is WORLD readable.

To correct this problem, it is recommended that you either:
* Copy Easy-RSA to your User folders and run it from there, OR
* Define your PKI to be in your User folders. EG:
  'easyrsa --pki-dir="C:/Users/<your-user-name>/easy-rsa/pki" <command>'


* Using SSL: openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)

....+..++++++++++++++++++++++++++++++++++++++++*.........+..+.........+...+...+...+.......+.
.....+.+...+.....+.......+...+..+....+.........+..+....+...+.....+.......+...+..+....+.....
.+...+...++++++++++++++++++++++++++++++++++++++*..+.....+.+......++++++++++++++++++++++++++
......+.+..+...+.......+...+............+...+.....+...+.........+.+.........+..+...+.......
............+...+..+.........+......+............+............+.+........+.+.....+....+....
..+..+...+.......+..................+.........+..+.........+....+..+.+...+...........+...+.+
.........+....+......+..+.........+.+.....+.......+......+..+..........+........+.........+
..+..........+......+..+...+.......+...........+...........+....+...+..+......+....+.....+
......+......+......+.+..+.......+...+..+.+........+....+...........+...+.....+.+.....+...
.+..+..........+...+......+.....+..........+...+.....+.+.........+...+..+.................+.
.........+......+.............+.+...+.....+.+...+.....+...+.......+...+...+..+...+......+.
....+..+.............+....+..+..........+..+...+....+.....+....+..+.......................
....+...........+....+...........+......+.+..+..................+.......+........+.......+.
..+.+.............+........+......+.......+.............+..+.+..+...........+.......+.
.+...+.......+.....+............+..+....+...+...+...+..+...+.......+........+.+........+..
......+............+.............+...+....+.....+.+.....................+.........+...+...
+.....+.................+.......+..+.+...........+...+.......+...+......+..+...+..........
```

Figure 6 : Creating server key and certificate

```
Keypair and certificate request completed. Your files are:
* req: C:/Program Files/OpenVPN/easy-rsa/pki/reqs/server.req
* key: C:/Program Files/OpenVPN/easy-rsa/pki/private/server.key

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate
for '825' days:

subject=
    commonName                = server


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes

Using configuration from C:/Program Files/OpenVPN/easy-rsa/pki/37cedf3d/temp.4.1
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'server'
Certificate is to be certified until Jan 29 07:01:58 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/issued/server.crt
```

Figure 7 : Creating server key and certificate

5. Generate dh parameter required by server during TLS handshake while connecting with clients.

›_ Console

```
> ./easyrsa gen-dh
```

```
# ./easyrsa gen-dh

* Using Easy-RSA configuration:
  C:/Program Files/OpenVPN/easy-rsa/pki/vars

WARNING
=======
Using Windows-System-Folders for your PKI is NOT SECURE!
Your Easy-RSA PKI CA Private Key is WORLD readable.

To correct this problem, it is recommended that you either:
* Copy Easy-RSA to your User folders and run it from there, OR
* Define your PKI to be in your User folders. EG:
  'easyrsa --pki-dir="C:/Users/<your-user-name>/easy-rsa/pki" <command>'


* Using SSL: openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)

Generating DH parameters, 2048 bit long safe prime
.............................+.............................+.....................
.....................................................................................
.....................................................................................
```

Figure 8 : Generation of dh parameter

```
.....................................................................................
+*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*+
+*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*
DH parameters appear to be ok.

Notice
------

DH parameters of size 2048 created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/dh.pem


EasyRSA Shell
```

Figure 9 : Generation of dh parameter

6. Add or update the following lines in `C:\Program Files\OpenVPN\configauto\server.ovpn` file.

server.ovpn

```
ca ca.crt
cert server.crt
key server.key
dh dh.pem
```

7. Restart OpenVPN from services.

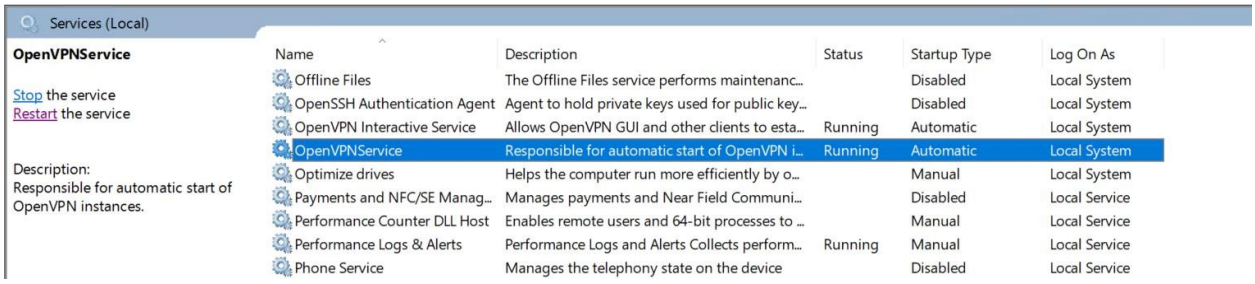

Figure 10 : OpenVPN service

5.2 Install and Configure Libp11

1. Download and install OpenSSL 3 if not installed, refer to *https://slproweb.com/products/Win32OpenSSL.html* for windows build. Here OpenSSL is installed in `C:\OpenSSL-Win64`.
2. Download libp11 from *https://github.com/OpenSC/libp11/releases*.
3. Download and Install Visual Studio, refer to *https://visualstudio.microsoft.com/vs/older-downloads/*.
4. Open the Native x64 VS Command Prompt and go to the directory where libp11 is extracted.
5. Run the following command to build and install libp11 with openssl.

›_ Console

```
nmake /f Makefile.mak OPENSSL_DIR=c:\OpenSSL-Win64 BUILD_FOR=WIN64
```

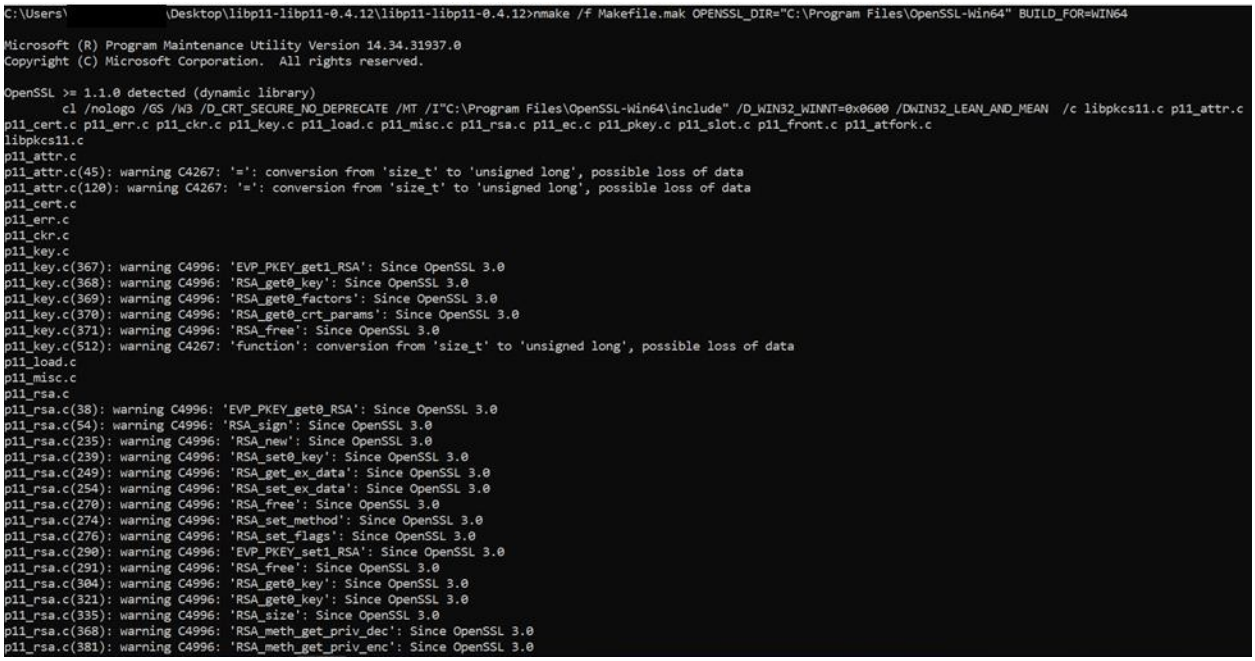

Figure 11 : Output of nmake command

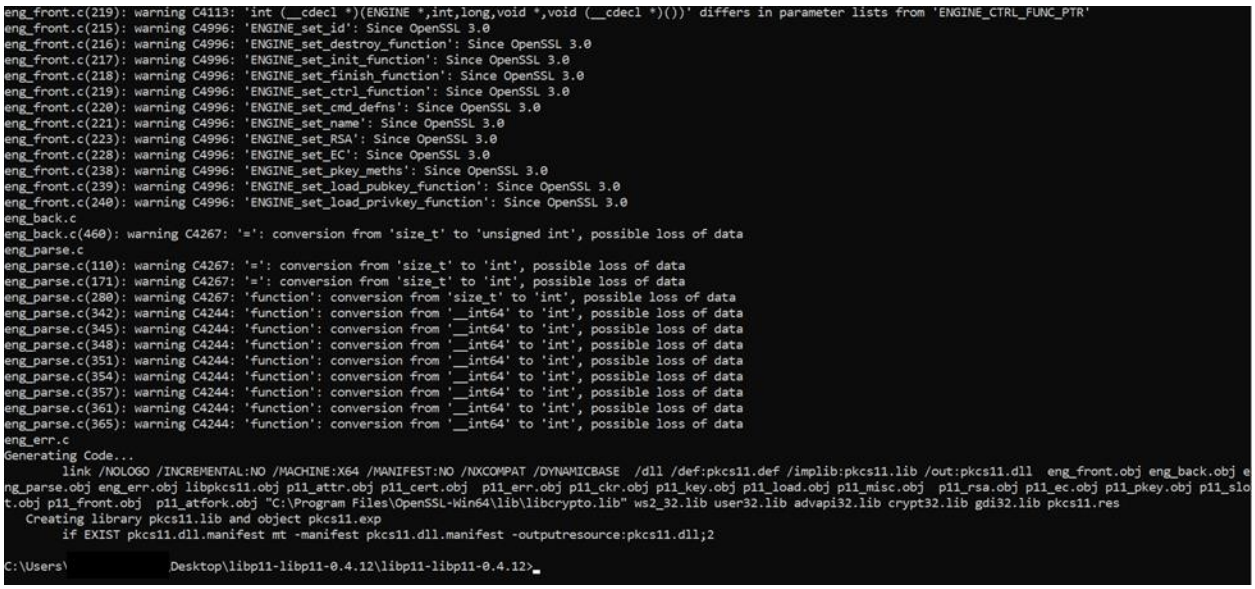

Figure 12 : Output of nmake command

6. Verify pkcs11.dll is available inside `<libp11>/src/ folder`.

7. Edit `openssl.cnf` from `C:\Program Files\Common Files\SSL\openssl.cnf` and add the following line in the first line of the file.

openssl.cnf

```
openssl_conf = openssl_init
```

8. Enter the following lines under last section of `openssl.cnf` file.

openssl.cnf

```
[openssl_init]
engines=engine_section
[engine_section]
pkcs11 = pkcs11_section
[pkcs11_section]
engine_id = pkcs11
dynamic_path = C:\\Users\\openssl-user\\Downloads\\libp11-
0.4.12\\src\\pkcs11.dll
MODULE_PATH = C:\\Program
Files\\Utimaco\\SecurityServer\\Lib\\cs_pkcs11_R3.dll
init = 0
```

Dynamic path and Module path will get changed according to the user environment.

9. Run the command below to verify if the OpenSSL Engine is available or not.

›_ Console

```
# openssl engine pkcs11 -t
```

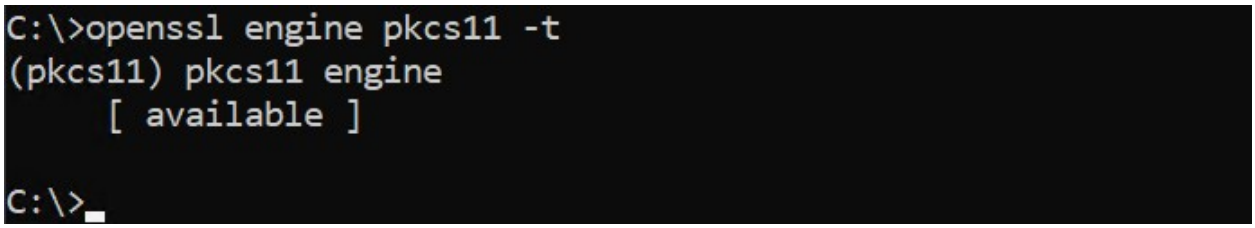

Figure 13 : Verification of pkcs11 engine

5.3 Generate Client Key and Certificate on Utimaco HSM

1. Generate client key using the p11tool2 command.

›_ Console

```
> p11tool2 slot=0 LoginUser=ask

PubKeyAttr=CKA_LABEL=”OpenVPNPublicKey”,CKA_ID=0x45

PrvKeyAttr=CKA_LABEL=”OpenVPNPrivateKey”,CKA_ID=0x45 GenerateKeyPair=RSA
```

Provide the slot PIN when prompted.

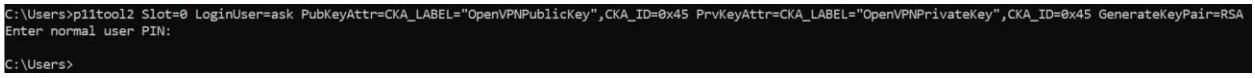

Figure 14 : Generate RSA key command output

2. Generate certificate request for client. Provide the slot PIN when prompted.

›_ Console

```
> openssl req -engine pkcs11 -new -key

“pkcs11:token=OpenVPNToken;object=OpenVPNPrivateKey” -keyform engine -out
OpenVPNClient.req
```

```
C:\OpenSSL-Win64\bin>openssl req -engine pkcs11 -new -key "pkcs11:token=OpenVPNToken;object=OpenVPNPrivateKey" -keyform engine -out OpenVPNClient.req
Engine "pkcs11" set.
Enter PKCS#11 token PIN for OpenVPNToken:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:MH
Locality Name (eg, city) []:Pune
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Utimaco
Organizational Unit Name (eg, section) []:security
Common Name (e.g. server FQDN or YOUR name) []:utimaco.com
Email Address []:support@utimaco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\OpenSSL-Win64\bin>
```

Figure 15 : Certificate request command output

3. Copy the OpenVPNClient.req file to `C:\Program Files\OpenVPN\easy-rsa\pki\reqs`.
4. Go into directory `C:\Program Files\OpenVPN\easy-rsa` and start easy-rsa shell.

›_ Console

```
> EasyRSA-Start.bat
```

```
C:\Program Files\OpenVPN\easy-rsa>EasyRSA-Start.bat

Welcome to the EasyRSA 3 Shell for Windows.
Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easyrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell
```

Figure 16 : EasyRSA shell

5. Sign the client CSR.

›_ Console

```
>./easyrsa sign-req client OpenVPNClient
```

```
EasyRSA Shell
# ./easyrsa sign-req client OpenVPNClient

* Using Easy-RSA configuration:
  C:/Program Files/OpenVPN/easy-rsa/pki/vars

WARNING
=======
Using Windows-System-Folders for your PKI is NOT SECURE!
Your Easy-RSA PKI CA Private Key is WORLD readable.

To correct this problem, it is recommended that you either:
* Copy Easy-RSA to your User folders and run it from there, OR
* Define your PKI to be in your User folders. EG:
  'easyrsa --pki-dir="C:/Users/<your-user-name>/easy-rsa/pki" <command>'


* Using SSL: openssl OpenSSL 3.1.3 19 Sep 2023 (Library: OpenSSL 3.1.3 19 Sep 2023)

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate
for '825' days:

subject=
    countryName               = IN
    stateOrProvinceName       = MH
    localityName              = Pune
    organizationName          = Utimaco
    organizationalUnitName    = security
    commonName                = utimaco.com
    emailAddress              = support@utimaco.com
```

Figure 17 : Client CSR signing

```
Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes

Using configuration from C:/Program Files/OpenVPN/easy-rsa/pki/df08df18/temp.2.1
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'IN'
stateOrProvinceName   :ASN.1 12:'MH'
localityName          :ASN.1 12:'Pune'
organizationName      :ASN.1 12:'Utimaco'
organizationalUnitName:ASN.1 12:'security'
commonName            :ASN.1 12:'utimaco.com'
emailAddress          :IA5STRING:'support@utimaco.com'
Certificate is to be certified until Feb  8 07:12:42 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/issued/OpenVPNClient.crt


EasyRSA Shell
# _
```

Figure 18 : Client CSR signing

6. To import the certificate into HSM, convert the certificate file (`.crt`) into `.der` format using the below command.

›_ Console

```
> openssl x509 -outform der -in OpenVPNClient.crt -out OpenVPNClient.der
```

```
C:\Program Files\OpenVPN\easy-rsa\pki\issued>openssl x509 -outform der -in OpenVPNClient.crt -out OpenVPNClient.der

C:\Program Files\OpenVPN\easy-rsa\pki\issued>_
```

Figure 19 : Convert certificate into .der format

7. Import certificate into HSM using the command below. Provide slot PIN when prompted.

›_ Console

```
> p11tool2 slot=0 LoginUser=ask

CertAttr=CKA_LABEL="OpenVPNClientCert",CKA_ID=0x45,CKA_PRIVATE=False

PubKeyAttr=CKA_LABEL="OpenVPNClientCertPublicKey",CKA_ID=0x45
ImportCert=OpenVPNClient.der
```

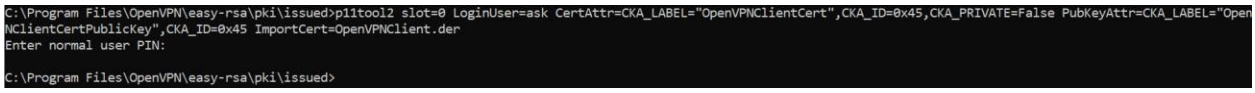

Figure 20 : Import certificate command output

8. List objects of HSM using the command below. Provide the slot PIN when prompted.

›_ Console

```
> p11tool2 slot=0 LoginUser=ask ListObjects
```

```
C:\Program Files\OpenVPN\easy-rsa\pki\issued>p11tool2 slot=0 LoginUser=ask ListObjects
Enter normal user PIN:


CKO_CERTIFICATE:

+ 1.1
  CKA_CERTIFICATE_TYPE          = CKC_X_509
  CKA_UNIQUE_ID                 = A84DE7A8-587B-4035-AB87-C2B3B6DCF854
  CKA_LABEL                     = OpenVPNClientCert
  CKA_ID                        = 0x45 (E)
  CKA_SUBJECT                   =
               0x30818831 0B300906 03550406 1302494E |0  1 0   U    IN|
                 310B3009 06035504 080C024D 48310D30 |1 0   U    MH1 0|
                 0B060355 04070C04 50756E65 3110300E |   U    Pune1 0 |
                 06035504 0A0C0755 74696D61 636F3111 |  U    Utimaco1 |
                 300F0603 55040B0C 08736563 75726974 |0   U    securit|
                 79311430 12060355 04030C0B 7574696D |y1 0   U    utim|
                 61636F2E 636F6D31 22302006 092A8648 |aco.com1"0   * H|
                 86F70D01 09011613 73757070 6F727440 |        support@|
                 7574696D 61636F2E 636F6D            |utimaco.com     |



CKO_PUBLIC_KEY:

+ 2.1
  CKA_KEY_TYPE                  = CKK_RSA
  CKA_UNIQUE_ID                 = 628256AD-56E8-4150-90AE-7E22DEB3F65C
  CKA_LABEL                     = OpenVPNPublicKey
  CKA_ID                        = 0x45 (E)
```

Figure 21 : List objects command output

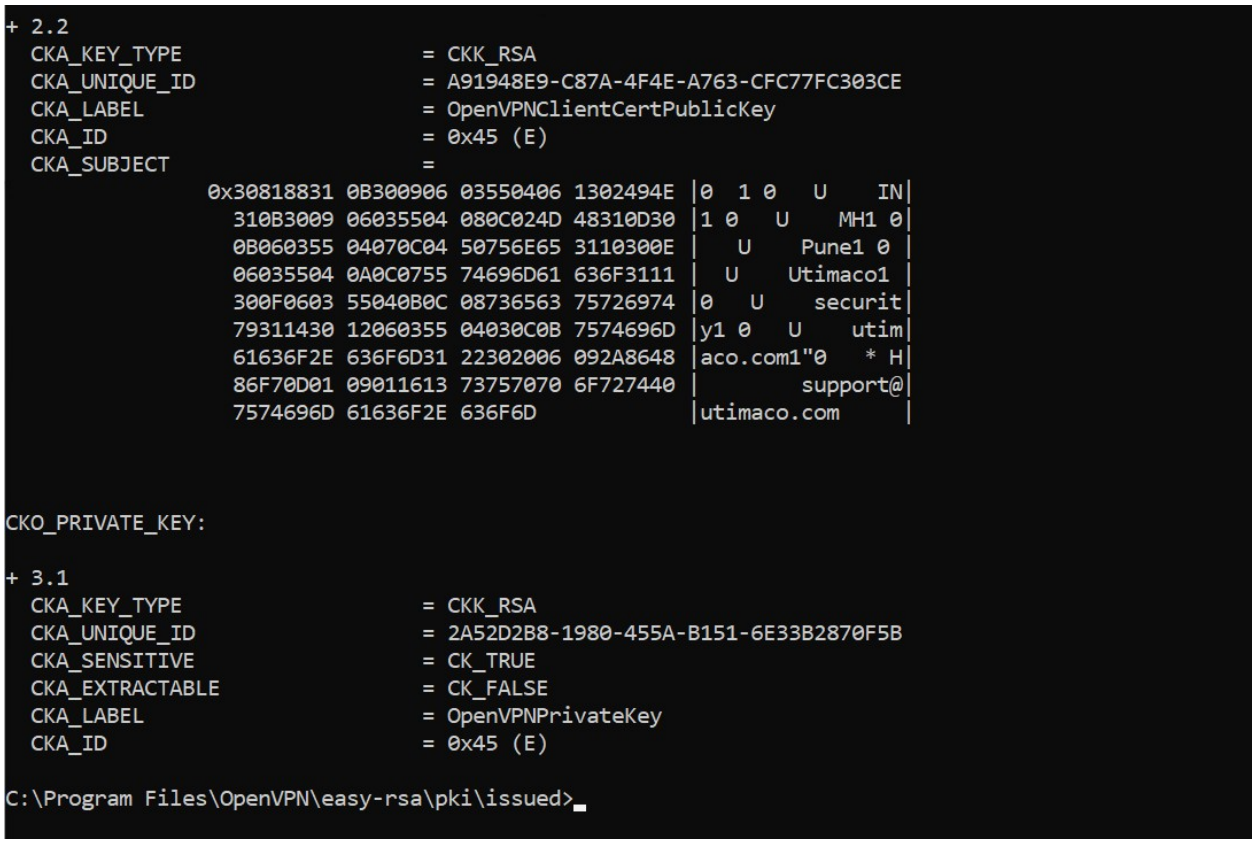

Figure 22 : List objects command output

5.4 Configure OpenVPN Client to use Key and Certificate from Utimaco HSM

1. List the certificate to get the serialized id using below command.

›_ Console

```
> openvpn --show-pkcs11-ids “C:\Program

Files\Utimaco\SecurityServer\Lib\cs_pkcs11_R3.dll” --verb
```

```
C:\Program Files\OpenVPN\bin>openvpn --show-pkcs11-ids "C:\Program Files\Utimaco\SecurityServer\Lib\cs_pkcs11_R3.dll" --verb
2023-11-06 13:01:15 PKCS#11: Adding PKCS#11 provider 'C:\Program Files\Utimaco\SecurityServer\Lib\cs_pkcs11_R3.dll'

The following objects are available for use.
Each object shown below may be used as parameter to
--pkcs11-id option please remember to use single quote mark.

Certificate
       DN:             C=IN, ST=MH, L=Pune, O=Utimaco, OU=security, CN=utimaco.com, emailAddress=support@utimaco.com
       Serial:         3045FC9769AE47C98E17C5CFC9E5FDDE
       Serialized id:  pkcs11:model=CryptoServer;token=OpenVPNToken;manufacturer=Utimaco%20IS%20GmbH;serial=SI003001_0000;id=E

C:\Program Files\OpenVPN\bin>
```

Figure 23 : List pkcs11 ids

Copy the serialized id from above command output.

2. Right-click on OpenVPN GUI in system tray select **client** and click on **Edit Config**.

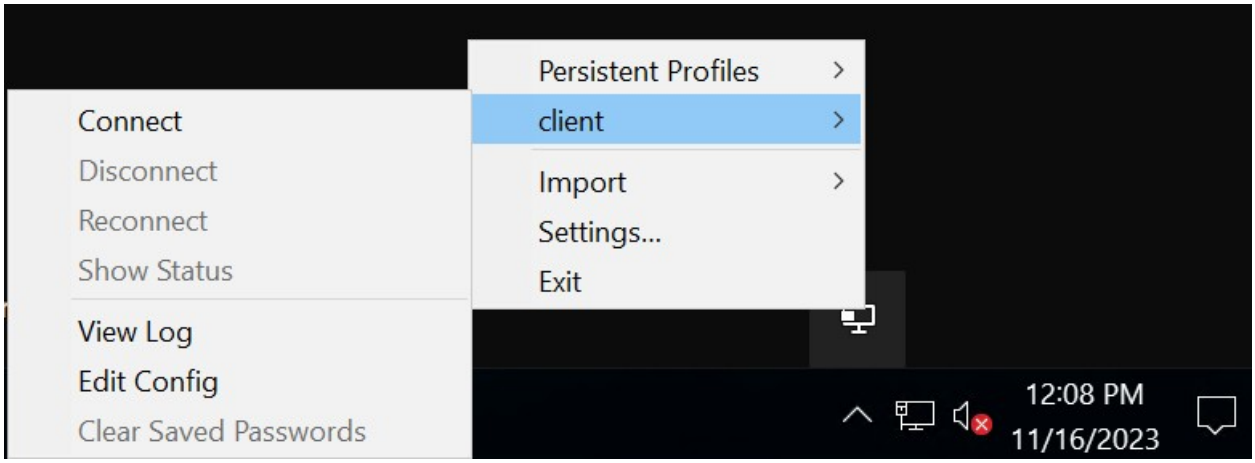

Figure 24 : Edit Config window

3. Client Config file will open. Add below lines to this file and save.

client.ovpn

```
pkcs11-providers "C:\\Program

Files\\Utimaco\\SecurityServer\\Lib\\cs_pkcs11_R3.dll"

 pkcs11-id

pkcs11:model=CryptoServer;token=OpenVPNToken;manufacturer=Utimaco%20IS%20GmbH;
serial=SI003001_0000;id=E'
```

Table 6: Add entries into client config file

4. Right-click on OpenVPN GUI in system tray select **client** and click on **Connect**.

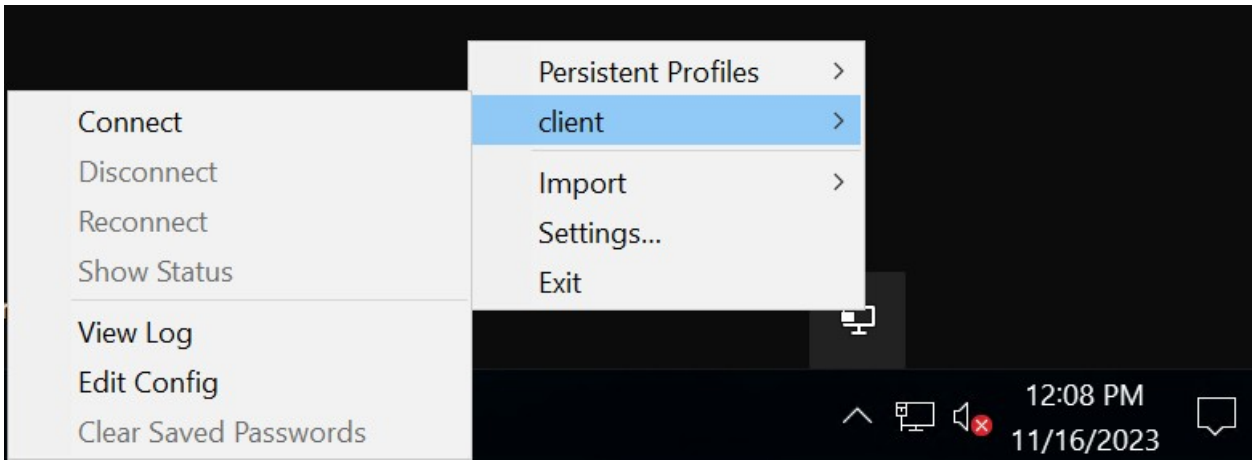

Figure 25 : Client Connect window

5. A window will appear. Provide the slot PIN when prompted for token password and click on **OK**.

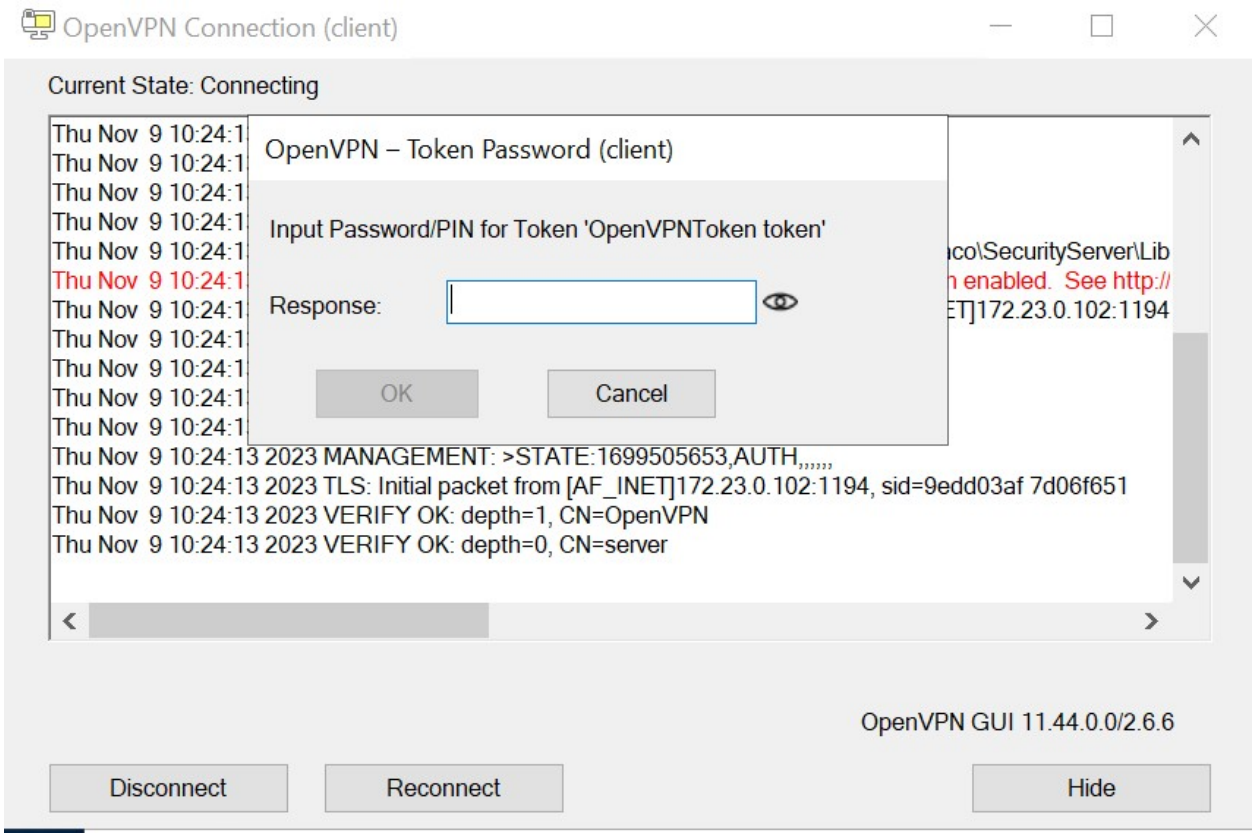

Figure 26 : Connection establishment output

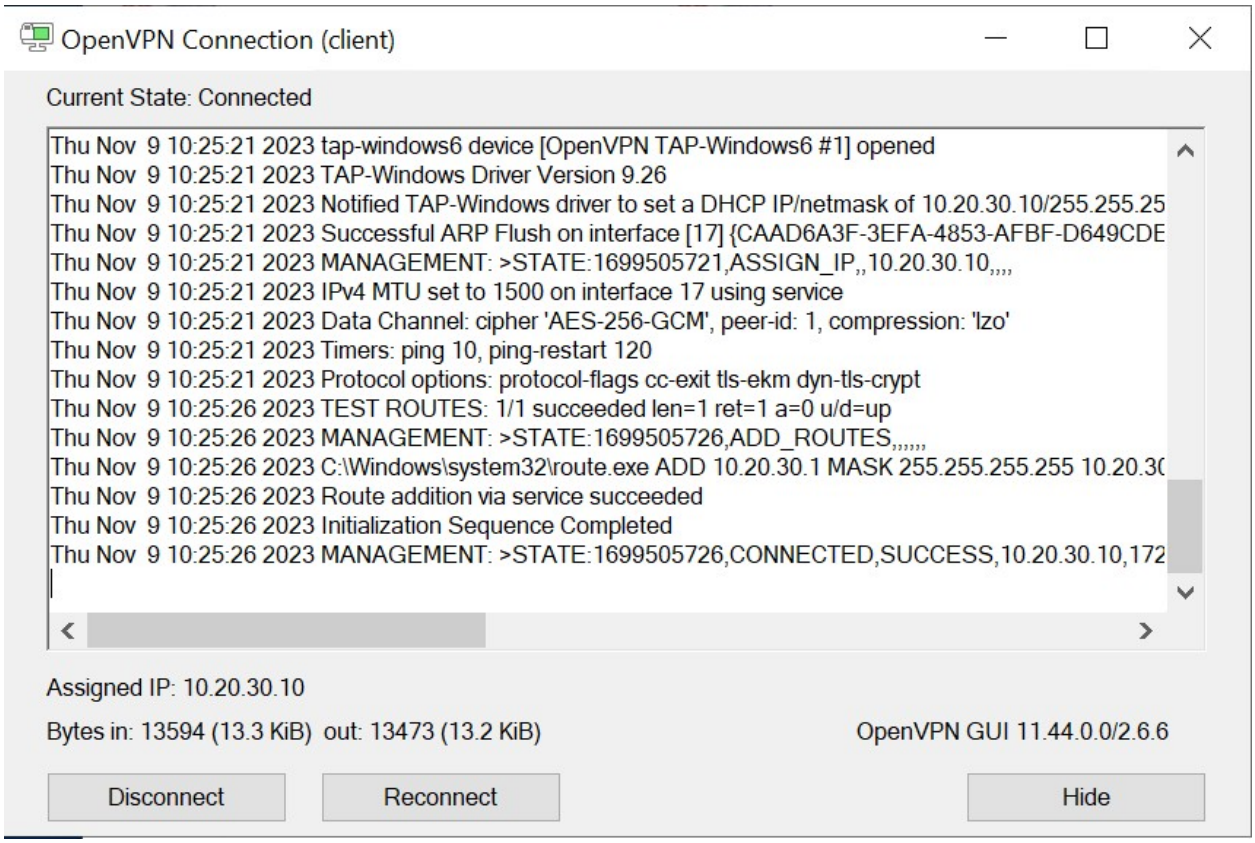

Figure 27 : Connection establishment output

6. After it is connected successfully, the OpenVPN GUI icon will turn green as shown below.

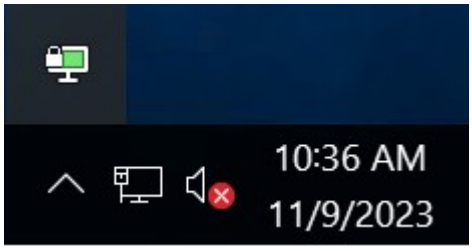

Figure 28 : OpenVPN GUI on successful connection

This completes the Integration of OpenVPN with Utimaco SecurityServer.

6 Troubleshooting

Error	Diagnosis
LoginUser= failed: p11_login: C_Login [type=1] returned Error 0x00000102 (CKR_USER_PIN_NOT_INITIALIZED)	PKCS#11 Slot is not initialized.
all tap-windows6 adapters on this system are currently in use or disabled.	Check the adapters into network settings and diagnose the problem. Reinstall the driver or add the new adapter.

Table 7: List of errors and their diagnoses

7 Further Information

This document forms a part of the information and support which 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/*.

8 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

Table 8: References

9 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 Str. 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.