Ascertia

ADSS Server

v5.1.0.1

Integration Guide

CryptoServer HSM

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	2026-07-28
Status	PUBLISHED
Document No.	IG-2026-0087

Table of Contents

1 Introduction

This document will guide you through the configuration of an ADSS Server to use a Utimaco Hardware Security Module as a PKCS#11 module. It is assumed that the reader has successfully installed, configured and administrated a server with the Ascertia ADSS. Please refer to Ascertia's documentation concerning any problems with the setup of the ADSS.

This guide is based on ADSS Server v5.1.0.1 using a Microsoft Windows SQL Server 2014 Express Edition running on Windows Server 2012 R2 Standard (x64). Thus, all paths and commands used are adapted to this environment. You might need to adapt the paths and commands shown in this guide to fit your system.

This document is intended to be used as a quick guide in conjunction with Ascertia's ADSS Server manuals and Utimaco's PKCS#11 documentation. For more detailed information on specific topics, please refer to the corresponding guides available.

2 Requirements

2.1 Ascertia ADSS Server

To successfully integrate an HSM, you have to have your ADSS Server installed correctly. For a complete installation guide, please refer to *ADSS-Server-Installation-Guide.pdf* and the other guides available. Ascertia's documentation can be found in `<ADSS_Server_Installation_Directory>\doc\`.

Ascertia also provides manuals online at *http://manuals.ascertia.com/ADSS-Admin-Guide/*.

2.2 Java

Go to *https://www.java.com/en/download/manual.jsp* to download and install the latest release of Java.

You should install the 32-bit version to ensure the IAIK PKCS#11 Wrapper works correctly.

To test the successful installation on your `PATH`, open a new command prompt and run:

›_ Console

```
java -version
```

2.3 Utimaco CryptoServer

To use your Utimaco HSM as a PKCS#11 module, you must take the following steps. Note that this is a quick guide which should be used in conjunction with Utimaco's PKCS#11 manual. Utimaco's PKCS#11 documentation can be found at: `<Utimaco_CryptoServer_Installation_Directory>\CryptoServer\Software\PKCS11_R2\doc\.`

2.3.1 Module Preparation

To use your HSM as a PKCS#11 module, you need to edit Utimaco's PKCS#11 configuration file. If you have installed the HSM Simulator, an environment variable called `CS_PKCS11_R2_CFG` has already been created.

If you have not installed the simulator, you should create this variable. To set the environment variable in Windows you must open **System**, then click on **Advanced system settings**, then click the button **Environment Variables** and finally add the path to your configuration file by clicking **New...**:

Variable Name: CS_PKCS11_R2_CFG

Variable Value: <The path to your configuration file>

(e.g. `C:\Program Files\Utimaco\CryptoServer\Lib\cs_pkcs11_R2.cfg`)

2.3.2 Module Configuration

To establish a connection with your HSM you need to edit the configuration file. It is highly recommended to look at Utimaco's manual to adapt the PKCS#11 module to fit your needs. Depending on the device you are using (`PCI/CSLAN/Simulator`) you need to adjust the Device Specifier. It is also recommended to set the log file location and log level. Do not forget to save your edited configuration file.

2.3.3 Token Creation

Since you can now communicate with your HSM, you should create a slot with a cryptographic user before connecting to Ascertia ADSS. You can use p11tool2 or PKCS#11 CryptoServer Administration to do so. See the provided documentation for details on how to manage the PKCS#11 API.

Ascertia ADSS is unable to make use of the HSM if no token is initialized! Therefore, you will not be able to connect to the HSM, without initializing at least one token.

3 Configuration

To connect your ADSS Server with your Utimaco HSM, you need to open the ADSS Server Console. To access the ADSS Server Console, type the following URL in your browser: https://<Machine_Name>:8774/adss/console.

Machine_Name could be: localhost (ADSS Server is on the local system where it is deployed), a local network system name or an IP address or a URL.

In the console, go to **Key Manager** and click on **Crypto Source**. Press the **New** button and fill in the form as shown here:

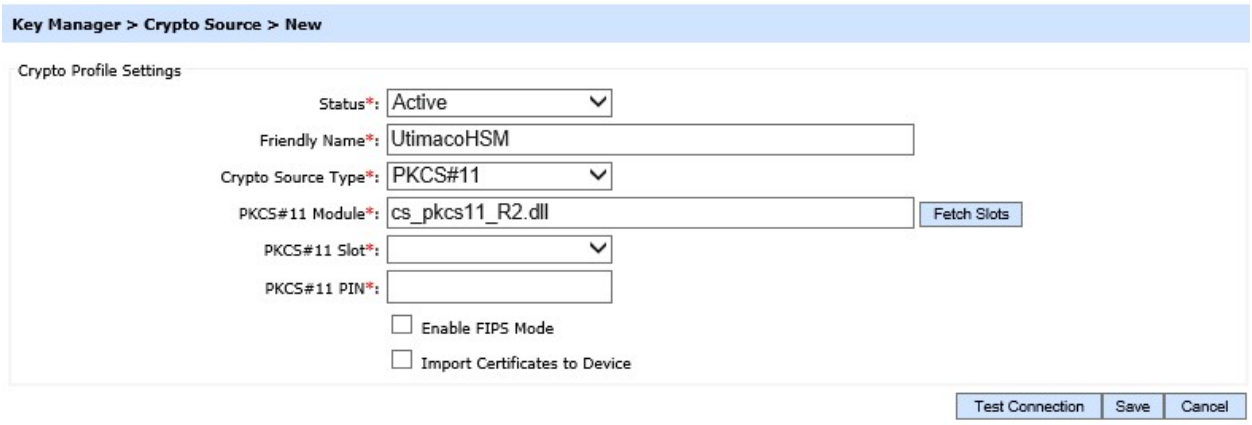

Figure 1 : adss1

Press **Fetch slots** and choose the slot you want to choose from the list. The list should show you all the slots which are visible with your current configuration. Type in the PIN of the cryptographic user. Verify the connection by clicking **Verify Connection**.

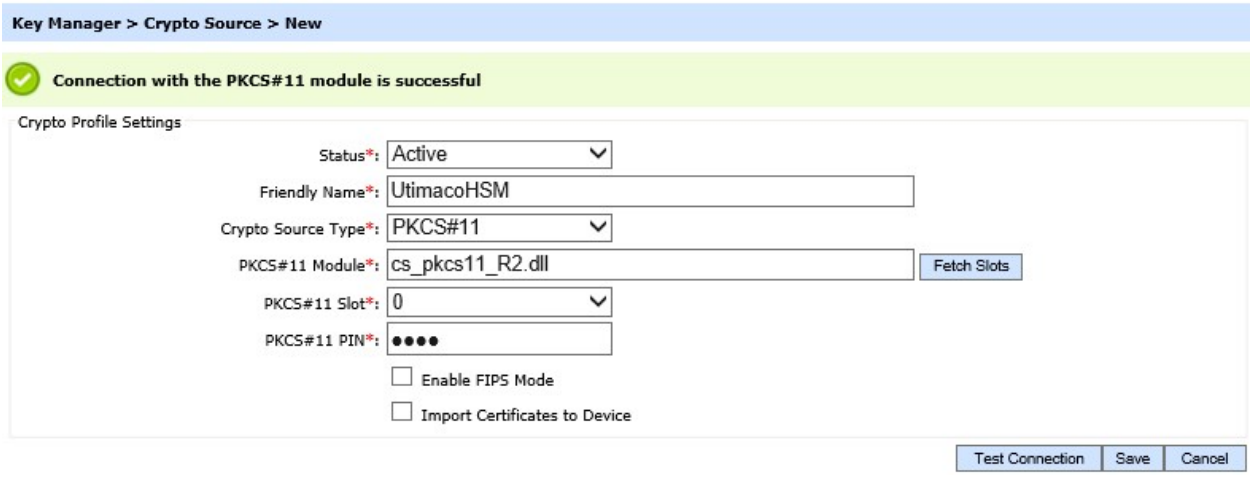

Figure 2 : adss2

Item	Description
Status	Set the status of the crypto profile to either *Active* or *Inactive*. The latter means the crypto device cannot be used to perform cryptographic operations on the keys.
Friendly Name	A unique identifier within the ADSS Server environment. Using a meaningful name for easy reference, such as UtimacoHSM, is recommended.
Crypto Source Type	Choose PKCS#11 as a crypto source.
PKCS#11 Module	Enter the cs_pkcs11_R2.dll library here. You can either use the absolute path to the file or just use its name. Please note that there is a 32-bit and a 64-bit version of this file, so use the correct one.
Fetch Slots	Click this button to see the available slots of your crypto device.
PKCS#11 Slot	The drop down will show you all the available slots. Select the slot you want to use.

Item	Description
PKCS#11 PIN	Enter the PIN number or password for the chosen slot.
Test Connection	Test communication with the configured hardware device.
Enable FIPS Mode	FIPS mode is supported by Utimaco HSMs. However, FIPS mode is not recommended when using smart cards or USB tokens.
Import Certificates to Device	If you want to store the certificates (based on the keys on the PKCS#11 module) on the token - as opposed to storing them on the ADSS Server - this option allows you to do so. Should be checked if you are using smart cards.

After the configuration, you need to restart the ADSS Server to update the running system. You can restart the system in the ADSS Server Console by clicking on **ServerManager** and then pressing **Restart System**.

4 Troubleshooting

4.1 Connection Problems

If you have problems connecting to the HSM, it is a good idea to make sure that your HSM is configured properly.

- Verify your HSM is running.
- Make sure your configuration file is configured according to your HSM (e.g. you typed in the correct IP address).
- Verify that you are using the right cs_pkcs11_R2.dll, there is a 32-bit and a 64-bit version. If you are unsure whether you are using the correct module, use the absolute path when typing in the PKCS#11 module name. If you installed the Utimaco software normally, this should not be a problem.

An easy way to check your connection is by using p11tool2 to check connectivity or PKCS#11 CryptoServer Administration if it is installed.

If you can communicate with the HSM by using these tools, but Fetch Slots fails, restarting your server normally solves the problem.

If you were able to fetch the available slots of your HSM, but Test Connection does not work, you should check if you entered the correct PIN/password for the slot and that the token is initialized. If all input is correct, but Test Connection still fails, it is also recommended to restart your server.

4.2 Supported functionalities

The Utimaco HSM supports all functionalities you can use within ADSS Server, except for the verification of RIPEMD-128 signatures.

4.3 Persisting Problems

For persisting or other problems, do not hesitate to contact us. Further information and contact information can be found below.

5 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 the Utimaco CryptoServer documentation is also available at the Utimaco IS GmbH website: *https://utimaco.com*.

6 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.