Ascertia LTD

ADSS Server

8.3.10

Integration Guide

u.trust GP HSM

SecurityServer 6.4.0

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	2026-09-15
Status	PUBLISHED
Document No.	IG-2026-0079

All rights reserved

No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.

Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them.

All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1 About This Guide

This guide describes the integration of the Ascertia ADSS Server with the Utimaco u.trust GP HSM. It provides an overview of the integration architecture, prerequisites, configuration steps, and validation procedures required to deploy the ADSS Server with the Utimaco u.trust GP HSM. This integration enables the ADSS Server to perform cryptographic operations using keys securely stored within the HSM.

1.1 Target Audience

This guide is intended for ADSS Server administrators responsible for the installation and configuration of ADSS Server with the Utimaco u.trust GP HSM. It is assumed that the reader has a basic understanding of PKI, HSMs, Linux commands, and IT security.

1.2 Purpose of the Integration

The purpose of this integration is to combine the Ascertia ADSS Server with the Utimaco u.trust GP HSM to provide secure key management and hardware-backed cryptographic operations. The Utimaco u.trust GP HSM ensures that cryptographic keys are generated, stored, and used within a tamper-resistant hardware boundary, preventing key exposure and reducing the risks associated with software-based key storage.

The integration enables the ADSS Server to perform digital signing, signature verification, and other cryptographic operations using keys protected by the HSM. It enhances overall security, improves auditability, and supports compliance with industry and regulatory requirements by ensuring that sensitive cryptographic material remains protected throughout its lifecycle.

1.3 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
ADSS	Advanced Document Security Server
PKI	Public Key Infrastructure

Abbreviation	Meaning
PKCS	Public Key Cryptography Standards
PKCS#11	PKCS Part 11: Cryptographic Token Interface Standard
SO	Security Officer
MBK	Master Backup Key
GUI	Graphical User Interface
LAN	Local Area Network
PCIe	Peripheral Component Interconnect Express
CLI	Command Line Interface
DLL	Dynamic Link Library
IP	Internet Protocol

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	Click **Fetch Slots**
`Monospaced`	Code that is given for explanation or as an example, file paths	Edit the `cs_pkcs11_R3.cfg` file and make appropriate changes.
Italic	References and important terms	Refer to the *ADSS Server Product Documentation*

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 Ascertia ADSS Server

The Ascertia ADSS Server is an enterprise-grade digital signature and trust services platform that provides secure digital signing, signature verification, certificate validation, timestamping, and certificate lifecycle management services. It enables organizations to establish trust in electronic documents, data, and transactions through the use of industry-standard cryptographic and PKI technologies.

The ADSS Server supports the deployment of digital trust services across enterprise environments and provides centralized management of cryptographic operations. By helping ensure the integrity, authenticity, and non-repudiation of digital information, it enables organizations to implement secure business processes while supporting compliance with regulatory and security requirements.

2.2 Overview of Utimaco u.trust GP HSM

Utimaco u.trust GP HSM 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. It can be used as a universal, independent security component for heterogeneous computer systems.

2.3 Joint Value Proposition

The integration of Ascertia ADSS Server with Utimaco u.trust GP HSM delivers a secure and compliant digital trust solution by combining advanced digital signing, validation, and timestamping capabilities with hardware-based cryptographic key protection. The Ascertia ADSS Server enables organizations to centrally manage digital signatures, certificate validation, and trusted timestamping services, while Utimaco u.trust GP HSM securely generates, stores, and protects cryptographic keys within tamper-resistant hardware. Together, the solutions enhance the security of digital transactions, safeguard private keys from unauthorized access, support regulatory and industry compliance requirements, and provide a trusted foundation for electronic signatures, authentication, and long-term validation services.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Operating System	Ascertia ADSS Server	Utimaco SecurityServer Version	Utimaco HSM
Windows Server 2022	8.3.10	SecurityServer 6.4.0	u.trust GP HSM CSe-Series/Se-Series
RHEL 9	8.3.10	SecurityServer 6.4.0	u.trust GP HSM CSe-Series/Se-Series

Table 3: Tested versions

3.2 Hardware and Software Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM CSe-Series/Se-Series LAN with firmware SecurityServer 6.4.0 or higher.
Utimaco PCI-e HSM	u.trust GP HSM CSe-Series/Se-Series PCI-e with firmware SecurityServer 6.4.0 or higher.

Table 4: List of hardware requirements

Software	Software Requirements
HSM Interface	SecurityServer PKCS#11 Provider
Ascertia ADSS Server	8.3.10

Table 5: List of software requirements

3.3 Prerequisites

Before you begin, please ensure that you have:

- 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 u.trust GP HSM documentation to set up the MBK.
- Set up and configure the u.trust GP HSM. Refer to the u.trust GP HSM documentation to set up the HSM.
- Set up and configured the PKCS#11 library according to your environment. Refer to the u.trust GP HSM documentation for instructions on setting up and configuring the PKCS#11
  library.
- Created the Security Officer (SO) user and Crypto user.
- The HSM appliance is powered on and accessible on the network at a known IP address and port (default: 4001–4031).
- A user account exists with sufficient privileges to log in and perform key operations. The username and PIN must be available.
- An AES-256 Secret Key Object has been created on the Utimaco u.trust GP HSM and given a label (alias). This guide uses pam-master-key as the label throughout. Note this value — it will be referenced in multiple configuration files.
- The Utimaco vendor client package has been provided by Utimaco support. This package contains the `libcs_pkcs11_R3.so` shared library and the `CryptoServerJCE.jar` file.

4 Installing and Configuring Utimaco u.trust GP HSM Software

The following section outlines the procedures required to configure the Utimaco u.trust GP HSM software.

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.

1. Copy the downloaded software to the appropriate location on the ADSS Server.
2. Locate the Utimaco PKCS#11 configuration file `cs_pkcs11_R3.cfg` in your SecurityServer folder.
    - Linux : `Software/Linux/Crypto_APIs/PKCS11_R3/sample`
    - Windows : `C:\ProgramData\Utimaco\PKCS11_R3`
3. Edit the `cs_pkcs11_R3.cfg` file and make appropriate changes. A sample `cs_pkcs11_R3.cfg` file is mentioned below:

```
library = C:\oracle\xtapi\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 = 4
 # Maximum size of the logfile in bytes (file is rotated with a backup file if
 full)
 Logsize = 3mb
 # Prevents expiring session after inactivity of 15 minutes
 KeepAlive = true
 # Set the Device to connect with
 #[CryptoServer]
 # Device specifier
 Device = <HSM_IP>
```

4. Copy `cs_pkcs11_R3.cfg` to `[ADSS_Server_Install_Path]\conf\hsm\utimaco`.
5. Delete `[ADSS_Server_Install_Path]\conf\hsm\utimaco\cs_pkcs#11_R2.cfg`.

6. Restart the ADSS Server Windows Services\Linux Daemons.

For detailed guidance on commands and their parameters, please refer to the Utimaco u.trust GP HSM 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

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 is 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.

5 Integration Steps on the Ascertia ADSS Server

Follow the steps below to configure the Utimaco u.trust GP HSM as a Crypto Source within the Ascertia ADSS Server.

1. Access the ADSS Server Unity Console as an operator with permission to manage crypto sources.
2. Navigate to **Key Manager > Crypto Sources**, and click **+** to add a new Crypto Source.

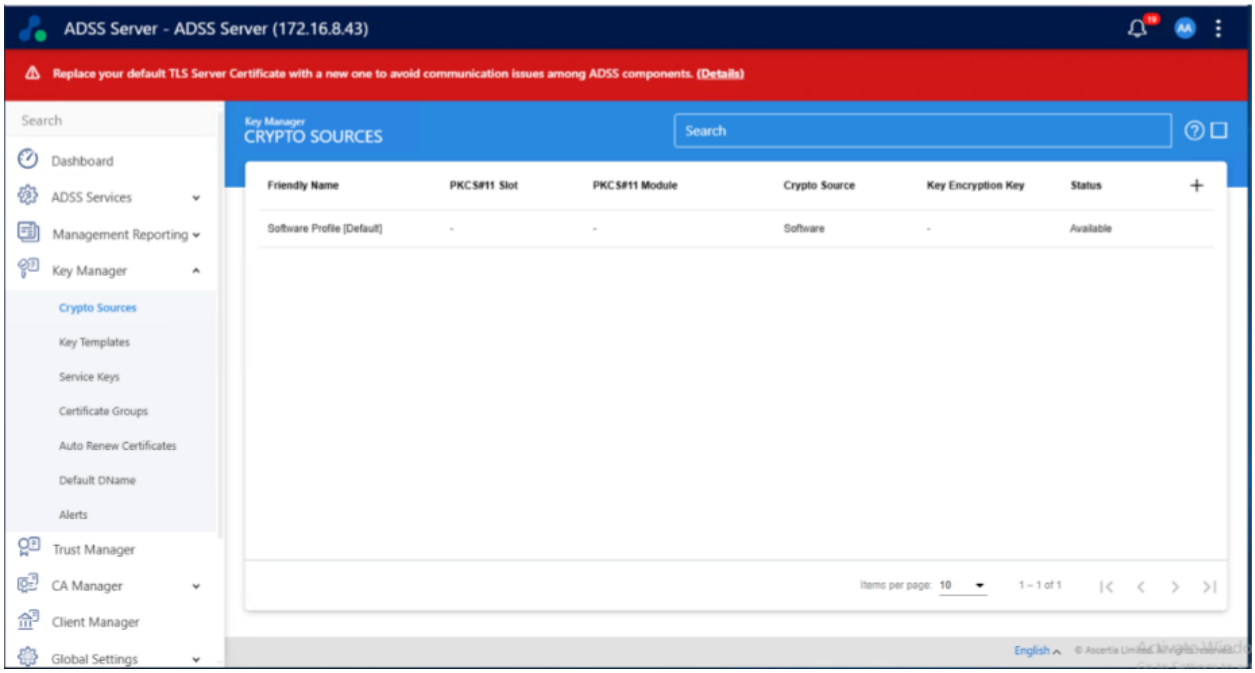

Figure 1 : Crypto Sources

3. The *Add Crypto Profile – Profile Identification* page will display; enter a friendly name for the new crypto profile. Click **>** to proceed to the next step.

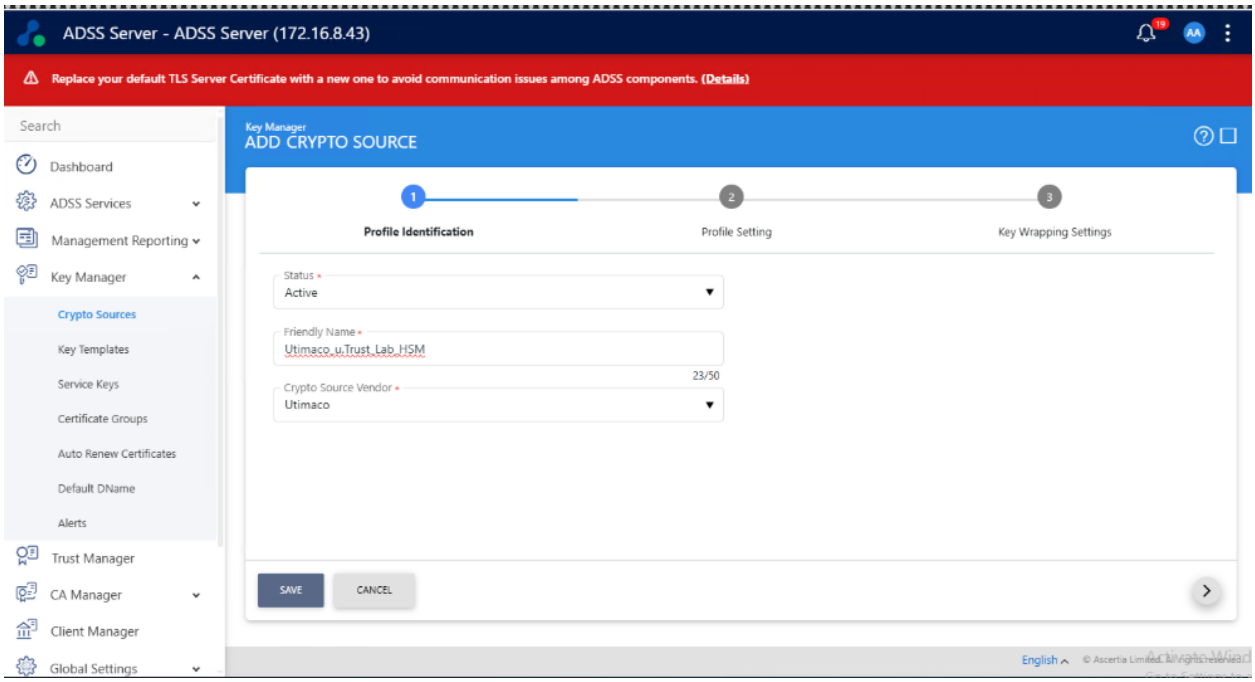

Figure 2 : Add crypto profile – profile identification

4. The ***Add Crypto Profile*** – ***Profile Setting*** page will display. In the PKCS#11 Module field, enter the path to the PKCS#11 dll supplied with the Utimaco HSM; by default this is:
    - Windows : `C:\Program Files\Utimaco\SecurityServer\Lib\cs_pkcs11_R3.dll`
    - Linux: `Software/Linux/Crypto_APIs/PKCS11_R3/lib/libcs_pkcs11_R3.so` in u.trust GP HSM bundle.
5. Click **Fetch Slots**.
6. Set the PKCS#11 slot that was initialized earlier.
7. Enter the PKCS#11 PIN created when the normal Crypto User was created.
8. Click the **Test Connection** button.
9. Click the **>** button to proceed to the next step.

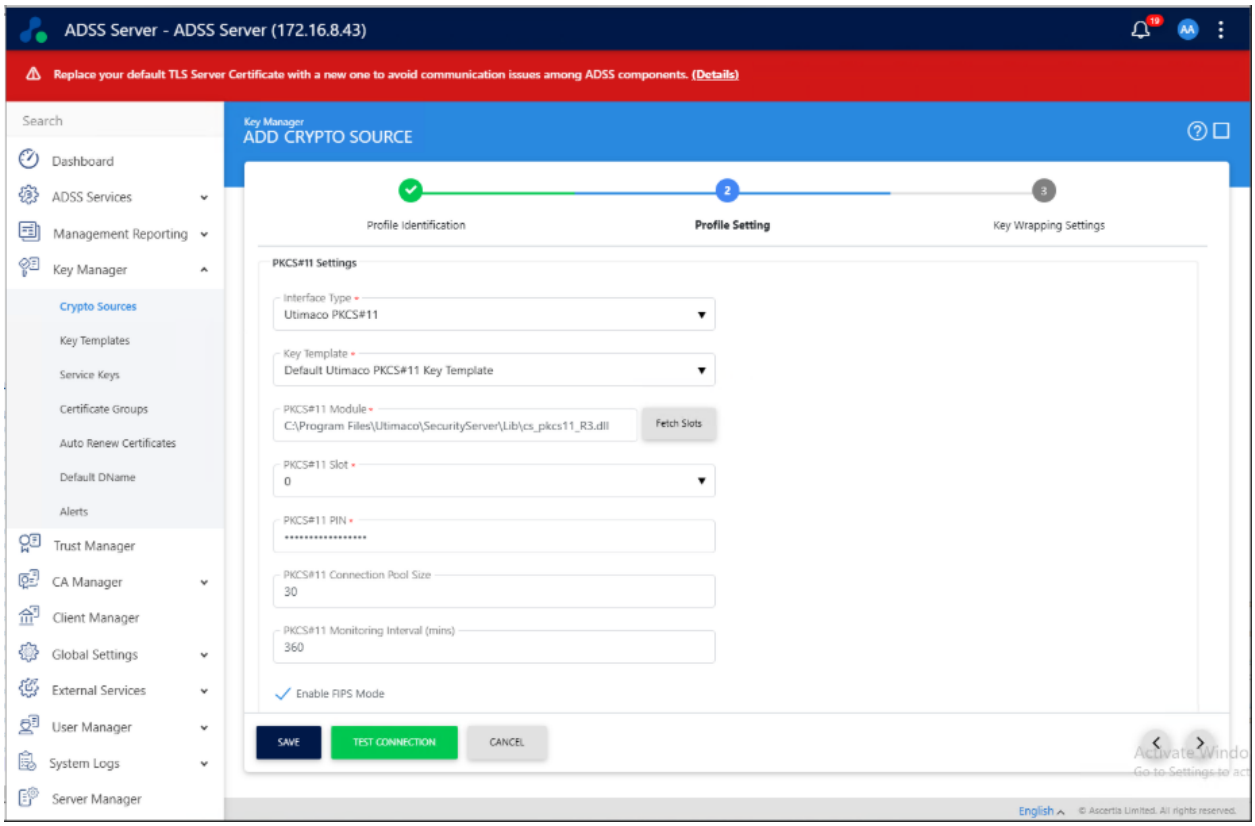

Figure 3 : Add crypto profile – profile setting

10. The ***Add Crypto Profile*** – ***Key Wrapping Settings*** page will display. Accept the default of **No key Wrapping**. Click **Save**.

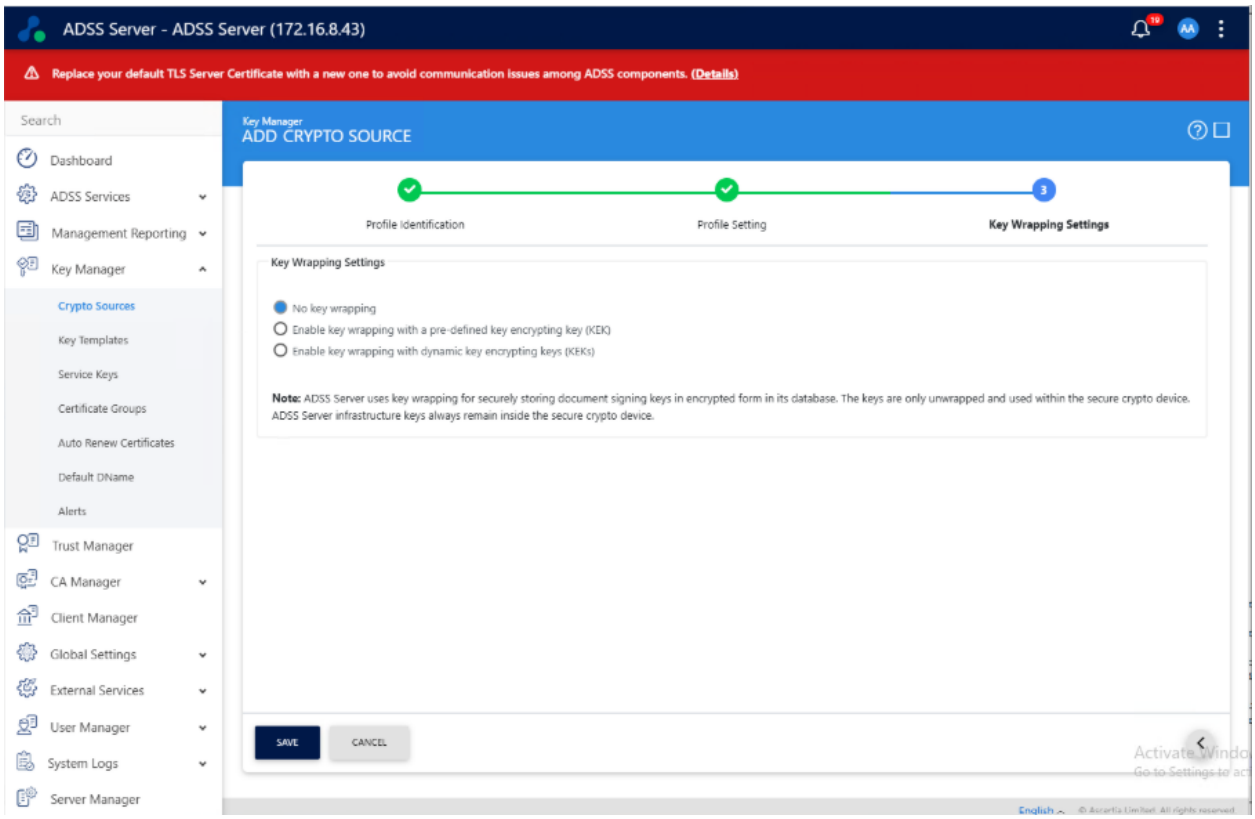

Figure 4 : Add crypto profile – key wrapping settings

11. You will be returned to the ***Crypto Sources*** page. Click the link to use the **Server Manager** to restart the ADSS Server instances.

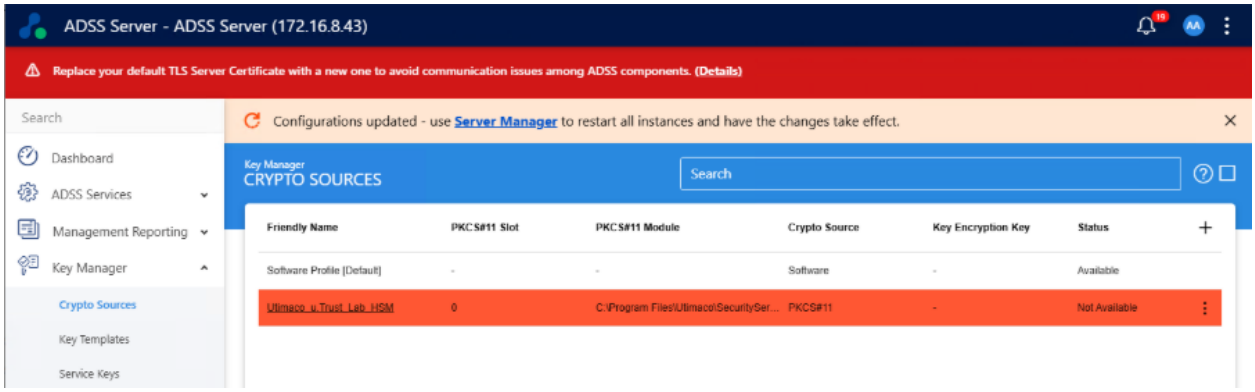

Figure 5 : Crypto sources

12. The **Server Manager** page will display. Click the **Restart All Instances** button.

13. Once the ADSS Server services have restarted, return to **Key Manager > Crypto Sources**. You will see that the new Utimaco HSM is now an available Crypto Source.

14. Refer to the *ADSS Server Product Documentation* to configure the services you wish to use with this new HSM.

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 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.

7 Appendices

7.1 References

Title	Description	Document/Link
Ascertia ADSS Server Product Documentation	Installation, configuration, and administration guidance for Ascertia ADSS Server	https://www.ascertia.com/product-documentation/adss-server/

Table 6: References