

Aventra Oy

Active Process Manager (APM)

4.1.0

Integration Guide

u.trust GP HSM

6.2.0

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	2026-10-28
Status	PUBLISHED
Document No.	IG-2026-0100
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	Introduction	5
1.1	About This Guide	5
1.2	Target Audience	5
1.3	Purpose of the Integration	5
1.4	Abbreviations	5
1.5	Document Conventions	6
2	Product Overview	8
2.1	Overview of Active Process Manager	8
2.1.1	Principle of Operation and Key Concepts	8
2.2	Overview of Utimaco u.trust GP HSM	8
2.3	Joint Value Proposition	9
3	Integration Requirements and Prerequisites	10
3.1	Tested Versions	10
3.2	Supported Platforms	10
3.3	Hardware and Software Requirements	10
3.3.1	Hardware Requirements	10
3.3.2	Software Requirements	11
3.4	Prerequisites	11
4	Installation and Configuration	12
4.1	Setting Up Utimaco SecurityServer Software	12
4.2	Setting Up Active Process Manager	13
4.3	Network and Security Configurations	14
5	Integration Steps on Utimaco u.trust GP HSM	15
6	Integration Steps on APM	17
6.1	Configuration on APM	17
6.1.1	Configuring PKCS11Connector Plug-in	17
6.1.2	Configuring PKCS11Update Plug-in	18
6.1.3	Configuring DataCipher Plug-in	23
6.2	User Access ;anagement	25
6.3	Sample Solutions Explained	25
6.3.1	PKCS11 Key Management Demo	25

7	Verification and Testing	27
7.1	Functional Testing.....	27
7.2	Logs and Validation Steps.....	27
7.2.1	PKCS#11 Logs.....	27
7.2.2	APM Logs	27
7.2.3	P11CAT.....	28
8	Optional Features	29
8.1	High Availability / Redundancy	29
8.2	Scalability Recommendations.....	29
9	Troubleshooting	30
9.1	Common Issues and How to Resolve Them	30
9.2	Log Locations and Interpretation	32
10	Contact and Support Information.....	34
11	References.....	36

1 Introduction

1.1 About This Guide

This guide has been created to provide guidance for using Aventura's Active Process Manager efficiently with Utimaco's SecurityServer General Purpose HSMs.

1.2 Target Audience

This guide is intended for users and administrators of Aventura Active Process Manager (APM) and Utimaco Hardware Security Modules (HSM).

1.3 Purpose of the Integration

By integrating APM with Utimaco HSMs, it is possible to configure cryptographic operations and key management tasks by creating APM solutions using APM's visual solution editor, run the solutions, and integrate the workflows with other integrated systems. APM extends the abilities of the GUI tools provided by Utimaco and makes it easier to set up HSM-related workflows which traditionally have required complex command line scripting or custom-made software.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
APM	Aventura Payment Manager
PKI	Public Key Infrastructure
TDE	Transparent Data Encryption
PKCS	Public Key Cryptography Standards

Abbreviation	Meaning
PKCS#11	PKCS Part 11: The Cryptographic Token Interface Standard
SO	The PKCS#11 cryptographic slot Security Officer
DB	Database
JRE	Java Runtime Environment
MBK	Master backup key
P11CAT	the PKCS#11 graphical interface tool
CXI	Cryptographic eXtended Interface
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
CA	Certificate Authority
RA	Registration Authority
CNG	Cryptography API: Next Generation

Table 1: Abbreviations

1.5 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
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>chsm-create</code>
<i>Italic</i>	References and important terms	See <i>Sample Chapter</i> in the <i>CryptoServer - Sample Manual</i>

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 Active Process Manager

Active Process Manager (APM), developed by Aventra Oy/Ltd based in Finland, is an innovative solution for automating security-related processes. With APM, you can control devices like HSMs, smart cards and smart card printers, and build an automated workflow which integrates your process into data sources and external systems, such as databases and web services. Examples of APM usage scenarios include smart card issuance and key management tasks such as creating cryptographic keys and securely transferring them between systems and devices. APM's configuration and workflows are saved in solution files. Users can create solutions for different purposes, and one solution can have several functions. The solution workflow is created using APM's visual solution editor.

2.1.1 Principle of Operation and Key Concepts

With APM, you can create solutions for various use cases. A solution consists of one or more steps, which represent functions that the end user can start from APM's front-end. Logic that is shared by several front-end functions can be combined into a single step. A solution step is built by inserting plug-ins into the step, using APM's solution editor. A plug-in is a software module designed to perform a specific task, or to maintain a connection to a device or an integrated system. Plug-ins can pass parameters to other plug-ins. When user starts a step by pressing a button on the front-end, APM runs the plug-ins of the step from top to bottom. This standard flow can be altered using solution logic plug-ins, which can execute a group of plug-ins conditionally, branch, or call other steps. APM's included set of plug-ins includes plug-ins for specific purposes, for example the PKCS#11 update plug-in can perform many operations defined in the PKCS#11 standard. By building an APM solution, you can use data source plug-ins to gather the data from various sources/integrations, link the data to the PKCS#11 update plug-in for processing, and combine this workflow with other security-related automated tasks, where – for example – cryptography, smart cards, smart card printers, access control tags and USB tokens are involved. The results of the plug-ins can be directed to various data sources as well.

2.2 Overview of Utimaco u.trust GP HSM

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

2.3 Joint Value Proposition

APM can connect to the Utimaco u.trust GP HSM using the PKCS#11 or CNG interface. While Utimaco's tools included with the u.trust GP HSM provide powerful features to manage and configure the device, APM enables configuring key management tasks and cryptographic operations easily, with a graphical user interface. Tasks such as key generation, wrapping, unwrapping, and derivation have traditionally required heavy command-line scripting or writing customized software. APM's configurable plug-ins make such tasks easier to configure, and APM has powerful features to integrate the tasks in automated workflows which interact with data sources and external systems. APM can also perform cryptographic operations such as signature creation and encryption with the HSM, and it can be used for automating the operations in many scenarios where such operations are needed. For example, APM can process many cryptographic operations in a batch run, fetching the data from an integrated system. In the REST API mode, an external system can trigger APM to process cryptographic operations. APM has features for encoding access cards and tags for physical access controls, and these features can be combined with highly secure HSM-based key management to ensure security of the access control keys in the whole infrastructure.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Operating System	Aventra Oy APM	Utimaco SecurityServer Version	Utimaco HSM
Windows 11	4.1.0	6.2.0	u.trust GP HSM Se-Series

Table 3: Tested versions

3.2 Supported Platforms

APM runs on Windows operating system. Windows 11, and Windows Server 2019 and newer Server versions are supported. SecurityServer tools must be installed on the same Windows workstation or server. The HSM simulator can run on a separate machine (e.g. Linux) as well.

3.3 Hardware and Software Requirements

3.3.1 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM Se-Series LAN with firmware SecurityServer 6.2.0 or higher
Utimaco PCI-e HSM	u.trust GP HSM Se-Series PCI-e with firmware SecurityServer 6.2.0 or higher

Table 4: List of hardware requirements

3.3.2 Software Requirements

Software	Software Requirements
HSM Interface	SecurityServer PKCS#11 Provider
HSM Utility	SecurityServer PKCS#11 Tool (p11tool2)
Partner Product	Active Process Manager, version 4.1.0 or newer

Table 5: List of software requirements

3.4 Prerequisites

Before you begin, please ensure that you have:

- Installed and set up the operating system listed in 4.1 Tested Versions or 4.2 Supported Platforms.
- Installed and set up the HSM listed in 4.3 Hardware and Software Requirements.
- Replaced the HSM default admin with a new admin user.
- Created and stored the MBK on each HSM. Refer to the SecurityServer documentation to set up the MBK.
- Set up and configured the SecurityServer. Refer to the SecurityServer documentation to set up the HSM.
- Set up and configured the PKCS#11 library according to your environment. Refer to the SecurityServer documentation for instructions on setting up and configuring the PKCS#11 library.
- Created the Security Officer (SO) user and Crypto user.

4 Installation and Configuration

The following section outlines the procedures required to configure the Utimaco SecurityServer Software.

4.1 Setting Up Utimaco SecurityServer 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.

On Windows:

On Windows, `cs_pkcs11_R3.cfg` will be automatically created and available in the `C:\ProgramData\UtimacoPKCS11_R3` folder as part of the SecurityServer software installation. Edit the `cs_pkcs11_R3.cfg` file and make the appropriate changes to the file. A sample `cs_pkcs11_R3.cfg` file is mentioned below.

```
library = C:\oracle\extapi\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 = 1
# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true
# Set the Device to connect with
#[CryptoServer]
# Device specifier
Device = <HSM_IP>
```



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's 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.

On Linux:

Setting up SecurityServer on Linux is out-of-scope of this document. Please refer to Utimaco's documentation provided with the tools if you plan to run the HSM simulator on Linux and connect it to APM using over the network.

4.2 Setting Up Active Process Manager

Install Active Process Manager using the installer executable. Follow APM's User Guide for guidance on setting up the basic settings and user privileges. It is recommended to also read the APM tutorial and check out the included sample solutions to get familiar with general functionality of APM. Please contact Aventura for the documentation and samples. You can find contact information at <https://aventra.fi>, a contact form is also available at <https://aventra.fi/products/active-process-manager/>. Aventura provides APM with a free evaluation license upon request.

4.3 Network and Security Configurations

Ensure that the computer running APM can connect the HSM or cHSM on the IP address and port it is running.

It is NOT recommended to store the HSM's PKCS#11 User or SO PINs in plaintext form in the APM solution. Use APM's security features to protect the PIN, or request users to enter it using a Password field in an InputConsole or DataEditor plug-in. Password values are encrypted in APM's Alias files.

5 Integration Steps on Utimaco u.trust GP HSM

Create users SO (Security Officer) and USR (the Crypto user) and initialize a slot.

The slot must be initialized using the p11tool2 or p11cat.

Please refer to Utimaco's user guidance for complete instructions. The basic procedure goes as follows:

1. Log on with the account(s) that give you the User Manager permission.
2. Initialize Token (Init Token under Slot Management) in p11cat and set a SO-PIN.
3. Log out, and log in again as SO.
4. Use the Set PIN function to change the initial SO-PIN.
5. Log in as SO again with the new SO-PIN.
6. Use Init PIN to initialize the user PIN with the initial PIN value.
7. Log out and log on as User.
8. Use Set PIN function to change the initial user PIN. Log out.

Now the slot and token are ready to be used with APM.

Make sure that the u.trust GP HSM is accessible from APM. You can verify it by opening PKCS11Connector plug-in's configuration dialog. You can use one of the included sample solutions. Verify that the PKCS#11 library path is correct, and check that you can find the slot in the Slot name dropdown.

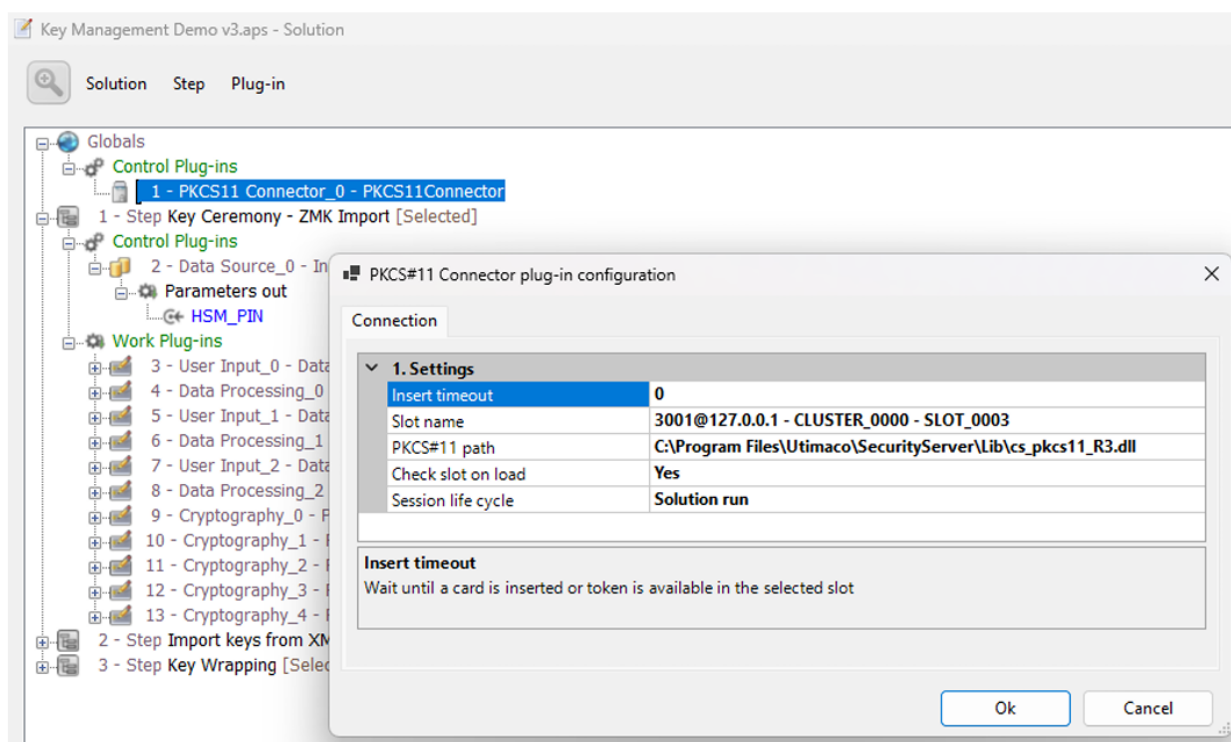


Figure 1 : HSM Connection Verification

6 Integration Steps on APM

6.1 Configuration on APM

APM solutions are built using APM's solution editor, and APM plug-ins perform the configured tasks such as key management operations and cryptographic operations. Please check APM tutorial and User Guide to get familiar with the principle of operation.

The most important plug-ins for Utimaco HSM integration are:

- **PKCS11Connector**: For selecting the PKCS#11 library and a slot, and maintaining a connection with the HSM.
- **PKCS11Update**: For performing specific tasks, for example key generation, signature computation, key wrapping, unwrapping and derivation, etc.
- **DataCipher**: For performing cryptographic operations using Microsoft's CNG interface and Utimaco CryptoServer Key Storage Provider. With DataCipher, you can select a certificate, and the plug-in locates the associated private key to perform signature computation.

Two sample APM solutions are provided for testing the integration, and for basis of building new solutions for key management and cryptography:

- **PKCS11 Key Management Demo** – contains functions for importing a Zone Master Key for importing other keys, and a function for importing AES keys from an XML file using the ZMK.
- **PKCS11 Signing Sample** – demonstrates signing data with RSA algorithm using APM and Utimaco HSM.

6.1.1 Configuring PKCS11Connector Plug-in

The purpose of the PKCS#11 Connector plug-in is to select a PKCS#11 Cryptoki library and a slot for performing operations. The Connector can be used also with PKCS#11 compliant smartcards, and in that case, it can request a user to insert a smartcard into the reader represented by the selected slot. With the **"Session life cycle"** parameter, you can select from three options, how long the PKCS#11 session is kept alive.

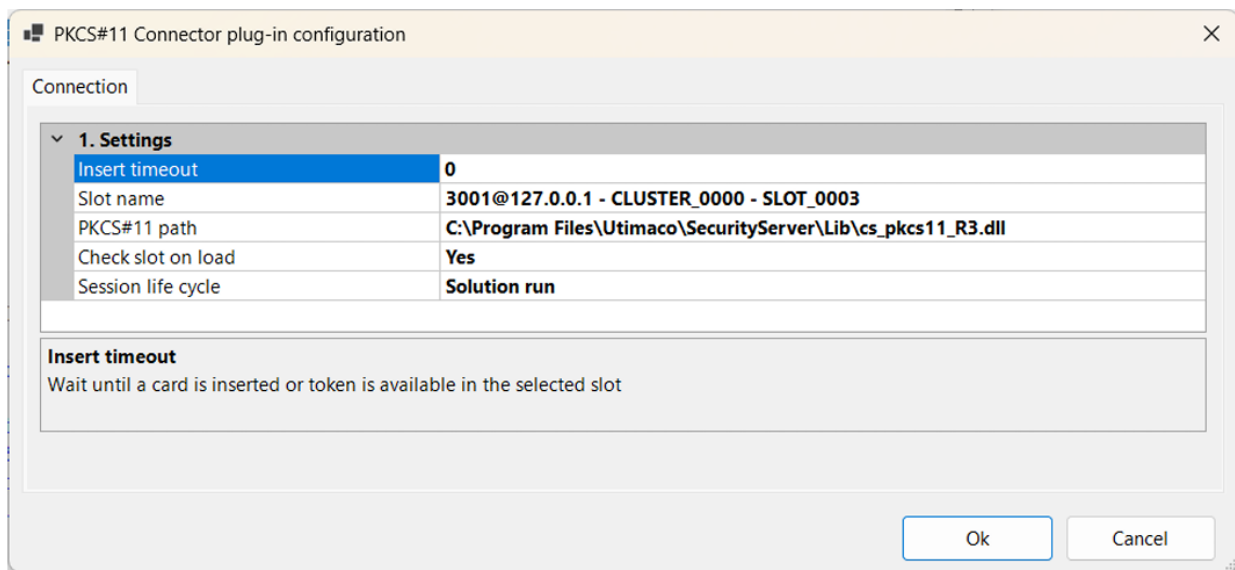


Figure 2 : PKCS11Connector Configuration

6.1.2 Configuring PKCS11Update Plug-in

You can place and configure as many separate PKCS11Update plug-in instances into your solution as you need.

Select type of operation for the dropdown list:

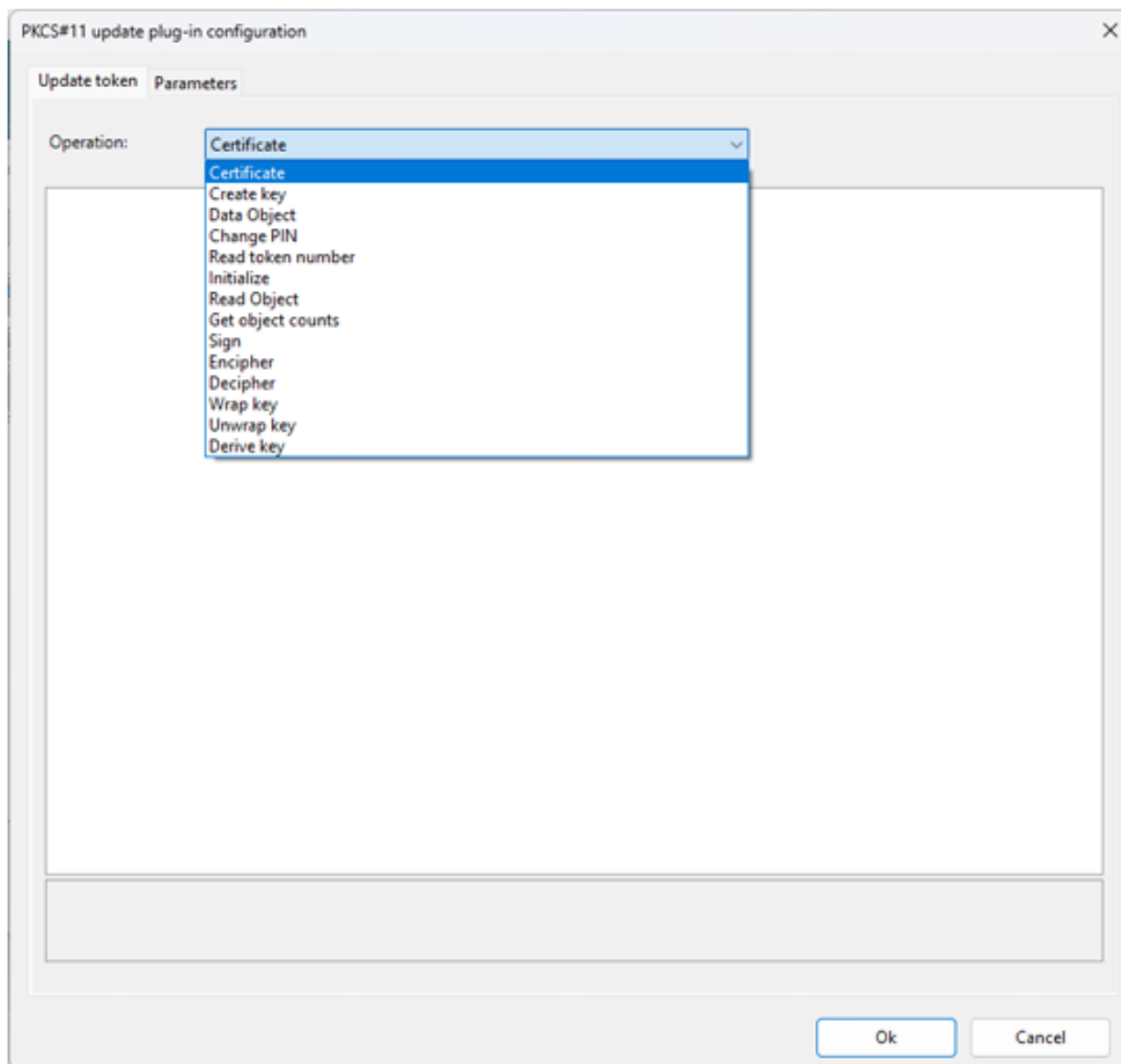


Figure 3 : PKCS11Update Operation Selection

Configure parameters for the operation. In this example **"Create key"** operation is selected and parameters specific for this operation are configurable in the grid below. The plug-in is configured to generate an RSA key pair on the HSM. In the **"1. Log In"** section you can select whether to login SO or User. You can enter the PIN directly in the plug-in or provide it as parameter. In production environments, it is recommended to store the PIN securely or request it from user, and provide it as a linked parameter to the PKCS11Update plug-in.

In the **"2. Key"** section, you can configure options for the key generation and the PKCS#11 attribute list consisting of for example ID, label and key usage flags. Description of each property, and guidance on configuring it, is available at the bottom of the window.

PKCS#11 update plug-in configuration

Update token Parameters

Operation: Create key

1. Log In	
Login SO PIN	No
SO PIN	
Login User PIN	Yes
User PIN	
2. Key	
Key source	On token generation
Key type	RSA
Key ID	1001
PublicExponent	65537
Key size	2048
Include CKA_VALUE_LEN	Yes
Attributes	token=CK_TRUE,private=CK_TRUE,sensitive=CK_TRUE,sign=CK_TRUE
Label	Sample RSA key
External parameters	

Login User PIN
Login to the token as a normal user.

Ok Cancel

Figure 4 : PKCS11Update Create Key Configuration

In another example, we have selected the “Sign” operation, configured it to Login User using a static PIN, selected the **CKM_RSA_PKCS** mechanism, and configured it to locate a key with label “MyRSAPrivateKey” for the operation.

PKCS#11 update plug-in configuration

Update token Parameters

Operation: Sign

1. Log In	
Login SO PIN	No
SO PIN	
Login User PIN	Yes
User PIN	12345678
2. Mechanism and key	
Cipher mechanism	CKM_RSA_PKCS
Signing mechanism	CKM_RSA_PKCS
Key ID	
Key label	MyRSAPrivateKey

Login SO PIN
Login to the token as security officer.

Ok Cancel

Figure 5 : PKCS11Update Sign Operation Configuration

In the Parameters tab, you can configure the data to sign. You can configure several parameters and select whether they are mandatory or optional. You can then link the values from any other APM plug-in above the PKCS11Update plug-in instance in the solution tree. This way, the data to be signed can be provided for example from user input, text file, database or a REST web service. In similar way, you can configure symmetric encryption operations and symmetric or asymmetric decryption operations. Select "Encipher" or "Decipher", select the mechanism (for example CKM_AES_CBC), define ID and/or Label to locate the key and configure parameters to provide the plaintext or ciphertext data for the operation.

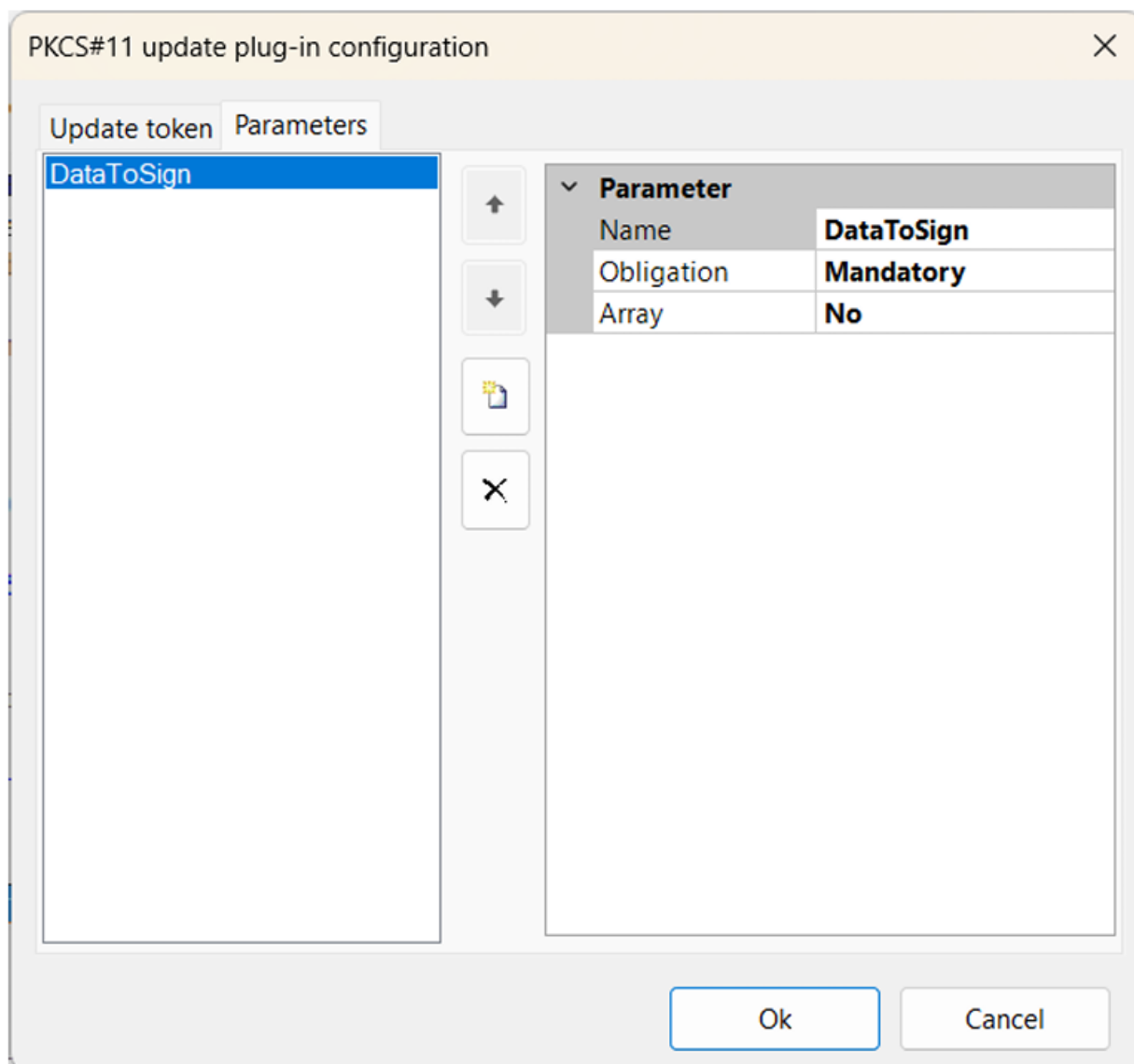


Figure 6 : PKCS11Update Signing Parameters

Another example of using PKCS11Update plug-in, this time for a key unwrapping operation.

PKCS#11 update plug-in configuration

Update token Parameters

Operation: Unwrap key

Login User PIN	Yes
User PIN	
2. Mechanism	
Mechanism	CKM_AES_ECB
3. Unwrapping key	
Unwrapping key type	AES
Unwrapping key ID	01
Unwrapping key label	
4. New key	
Unwrapped key type	AES
Unwrapped key ID	
Unwrapped key label	
New key attributes	token=CK_TRUE,private=CK_TRUE,sensitive=CK_
External parameters	New key label;New key ID

Login SO PIN
Login to the token as security officer.

Ok Cancel

Figure 7 : PKCS11Update Key Unwrap Configuration

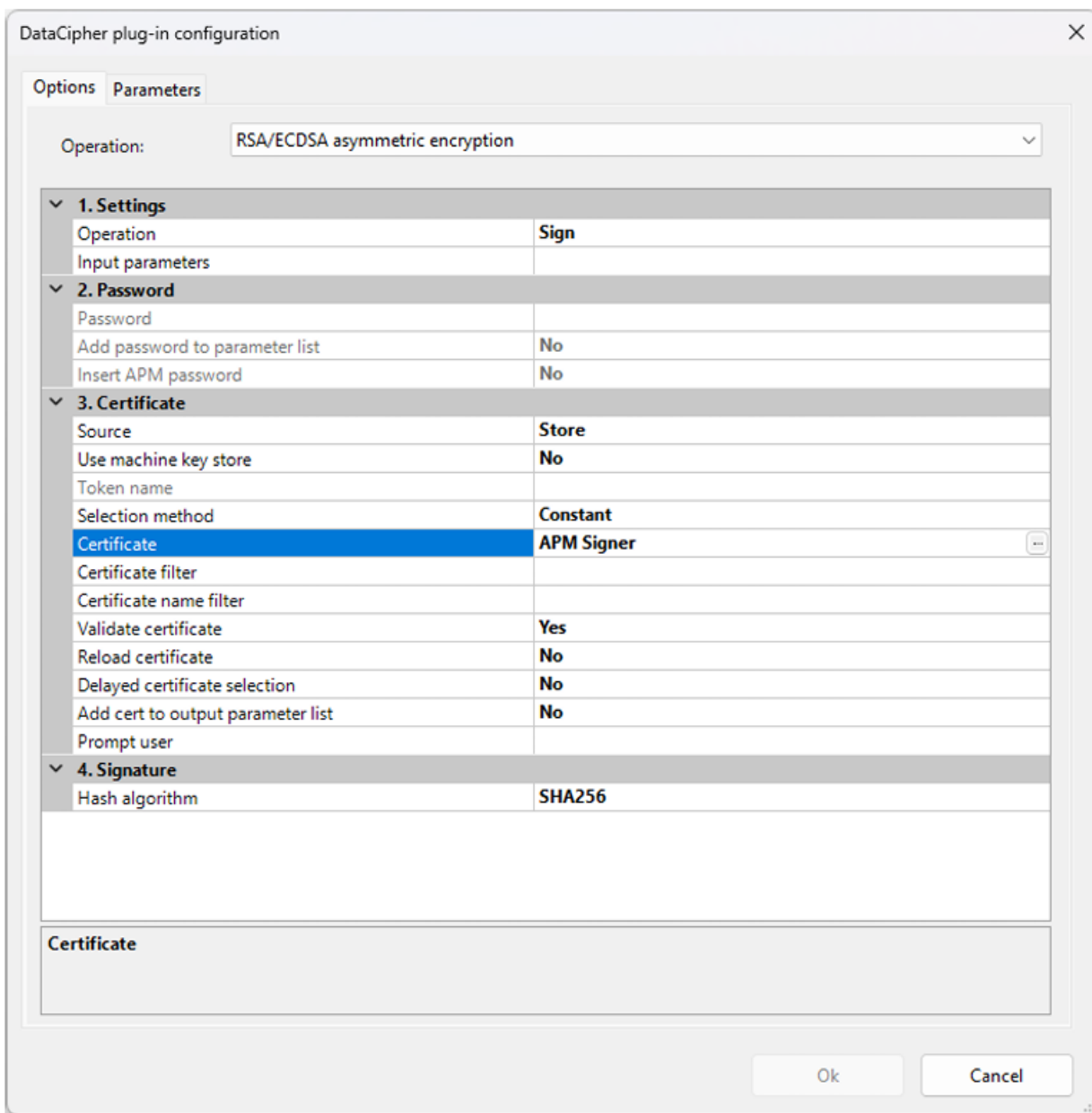
6.1.3 Configuring DataCipher Plug-in

With the DataCipher plug-in, you can sign data using CNG and the Utimaco SecurityServer Key Storage Provider. APM locates the signing key by the certificate selected in the plug-in. You can configure certificate selection in several ways: static selection, selection by user from a selection list or dynamically based on the common name and issuer name.

APM uses the key storage provider associated with the private key. To sign data using a private key on the HSM, configure the KSP according to [CryptoServer_Manual_CSP_CNG]. Select a certificate for which the private key resides on the HSM and is connected to the certificate in the

key store. Add one or more parameters and link the data to be signed to the parameters from other APM plug-ins. Select the hash algorithm.

APM signs values of all defined parameters when the plug-in is executed. APM uses the KSP associated with the private key associated with the selected certificate. This way, APM can use any KSP, regardless of whether the private key is in the software store, on a smartcard, or in an HSM. The algorithm is automatically selected based on the type of the key pair.



The image shows a 'DataCipher plug-in configuration' dialog box with two tabs: 'Options' and 'Parameters'. The 'Parameters' tab is active. At the top, there is a dropdown menu for 'Operation' set to 'RSA/ECDSA asymmetric encryption'. Below this is a table with four sections: '1. Settings', '2. Password', '3. Certificate', and '4. Signature'. Each section contains several rows of configuration options. At the bottom of the dialog is a 'Certificate' section with a large empty text area. 'Ok' and 'Cancel' buttons are at the bottom right.

1. Settings	
Operation	Sign
Input parameters	

2. Password	
Password	
Add password to parameter list	No
Insert APM password	No

3. Certificate	
Source	Store
Use machine key store	No
Token name	
Selection method	Constant
Certificate	APM Signer
Certificate filter	
Certificate name filter	
Validate certificate	Yes
Reload certificate	No
Delayed certificate selection	No
Add cert to output parameter list	No
Prompt user	

4. Signature	
Hash algorithm	SHA256

Certificate

Ok Cancel

Figure 8 : DataCipher Configuration

6.2 User Access ;anagement

APM supports the standard PKCS#11 C_Login command with parameters defined in the standard. It currently does not support Utimaco's proprietary extensions to PKCS#11. Refer to the standard and Utimaco's documentation on which operations require logging on as User and which operations require logging on as SO.

While it is possible to set the PIN directly in the PKCS#11 plug-in configuration window, this is recommended only in test environments. In production scenarios, it is recommended to not store the PIN as plain text. You can, for example, store it as a password-type Alias, select the alias into a hidden password field in an Input Console plug-in and link it to the PKCS11Connector plug-in's corresponding input parameter. Alias values are stored in encrypted form. Other options are to store the PINs encrypted in any data source and use APM's features to decrypt it when needed, or to store it on a smartcard.

APM has its own user privilege management. Run APM as Administrator to define user privileges. Select Settings->User management->Manage to define which users of the workstation have rights to use APM. You can define, for example, whether a user is allowed to only run a solution, or also modify it. You can assign permissions by user account or by AD group. Set permissions for user named *User* to give the same permissions for all users of the workstation. See APM's User Guide for more details.

6.3 Sample Solutions Explained

The sample solutions demonstrate how to perform the following tasks using APM and the Utimaco u.trust GP HSM:

6.3.1 PKCS11 Key Management Demo

The PKCS11 Key Management Demo solution includes three front-end operations:

- Key ceremony – ZMK import demonstrates a key ceremony, where a Zone Master Key (ZMK) is imported to the HSM. Three components of the ZMK are input on the keyboard separately. In a real scenario, this would be done by three different key custodians in person. APM commands the HSM to do the following:
 - Generate an ephemeral (CKA_TOKEN=CK_FALSE) AES key on the HSM.
 - Unwrap the first part of the ZMK to the HSM as a session object.
 - Combine the first and second part of the key within the HSM using C_Derive function and CKM_XOR_BASE_AND_DATA mechanism.

- Derive the final ZMK using the result of the first derive operation, using C_Derive and CKM_XOR_BASE_AND_DATA mechanism, this time setting CKA_TOKEN=CK_TRUE for the resulting object.
- Import keys from the XML file demonstrate how the ZMK is used to import a set of AES keys from an XML file. APM reads the records from the sample XML file one by one, extracts the ciphered key data and key metadata such as key type, ID, algorithm and label from each record, and unwraps each key into a new secret key object into the HSM.
- Key wrapping demonstrates wrapping a key with the ZMK in the HSM, and displaying the encrypted key in the DataEditor plug-in.

The PKCS11 Signing Sample solution has two front-end functions:

- Generate RSA key pair demonstrates generating an RSA pair on the HSM.
- RSA signing test demonstrates using the generated key pair for signing a message. It locates the private key by its label and ID and uses mechanism CKM_SHA384_RSA_PKCS_PSS to sign the message linked from InputConsole plug in.

7 Verification and Testing

7.1 Functional Testing

It is recommended that you verify that your software infrastructure, environment, and connections are working properly using the included sample solutions before building your own APM solutions.

7.2 Logs and Validation Steps

7.2.1 PKCS#11 Logs

Enabling PKCS#11 logging to facilitate easier testing and troubleshooting is recommended. This can be done by configuring the Logging Log level and Log Path parameters in the configuration file.

- Log Path should point to a writable directory (not a specific file) where log files can be stored.
- Logging Log level controls the verbosity of the logs:
 - Set it to 1 for basic logging.
 - For detailed testing and debugging, increase the level to 4.

The generated log file will be named `cs_pkcs11_R3.log` and located in the directory specified by Log Path. Reviewing this log file can help identify and resolve issues that arise during testing. Once testing is complete, it is advisable to reduce the Logging Log level to 1 or 2 to limit logging to only critical or important messages, thereby optimizing performance and reducing unnecessary log data.

7.2.2 APM Logs

In APM, logging can be configured in the Settings dialog. You can define the log file path, log level and other details. APM logs can be useful for resolving problems, as they contain information on how APM calls the PKCS#11 or CNG interfaces, the responses of the interfaces and information of the whole workflow.

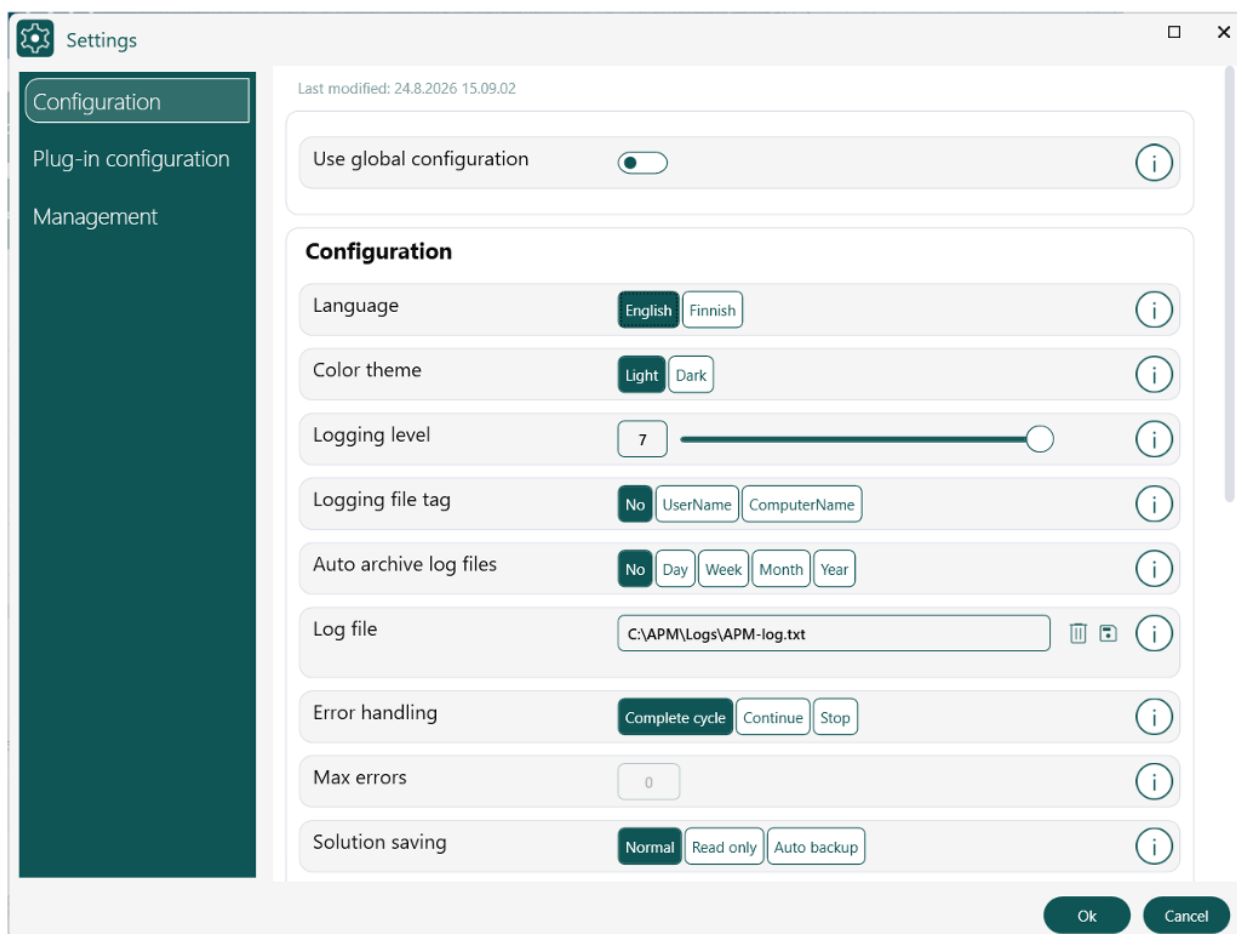


Figure 9 : Logging Configuration

7.2.3 P11CAT

You can use the P11CAT GUI tool provide in Utimaco's HSM software bundle to verify that the keys resulting from the key management operations are found on the token, and the attributes are as configured in APM.

8 Optional Features

8.1 High Availability / Redundancy

Configure high availability / clustering as specified in Utimaco's documentation. Configuring clustering, load balancing, and failover is described in the CryptoServer PKCS#11 R3 Developer Guide. When APM is used as a web service with APM REST API, HA and redundancy can be configured in the network infrastructure level, though this is out of scope of APM's features and guidance.

8.2 Scalability Recommendations

Several APM workstations can access one HSM simultaneously. APM can be used as a web service with APM REST API. This configuration has been proven to handle a large number of requests simultaneously in an environment where 25,000-30,000 workstations are accessing it daily. Performance characteristics are dependent on the APM solution used and the external data sources and systems accessed from APM, so universal performance metrics cannot be determined.

9 Troubleshooting

9.1 Common Issues and How to Resolve Them

APM displays error messages in the main window. Below is an example of an error message, in a situation in which there is an attempt to generate a key pair in a slot with an uninitialized token:

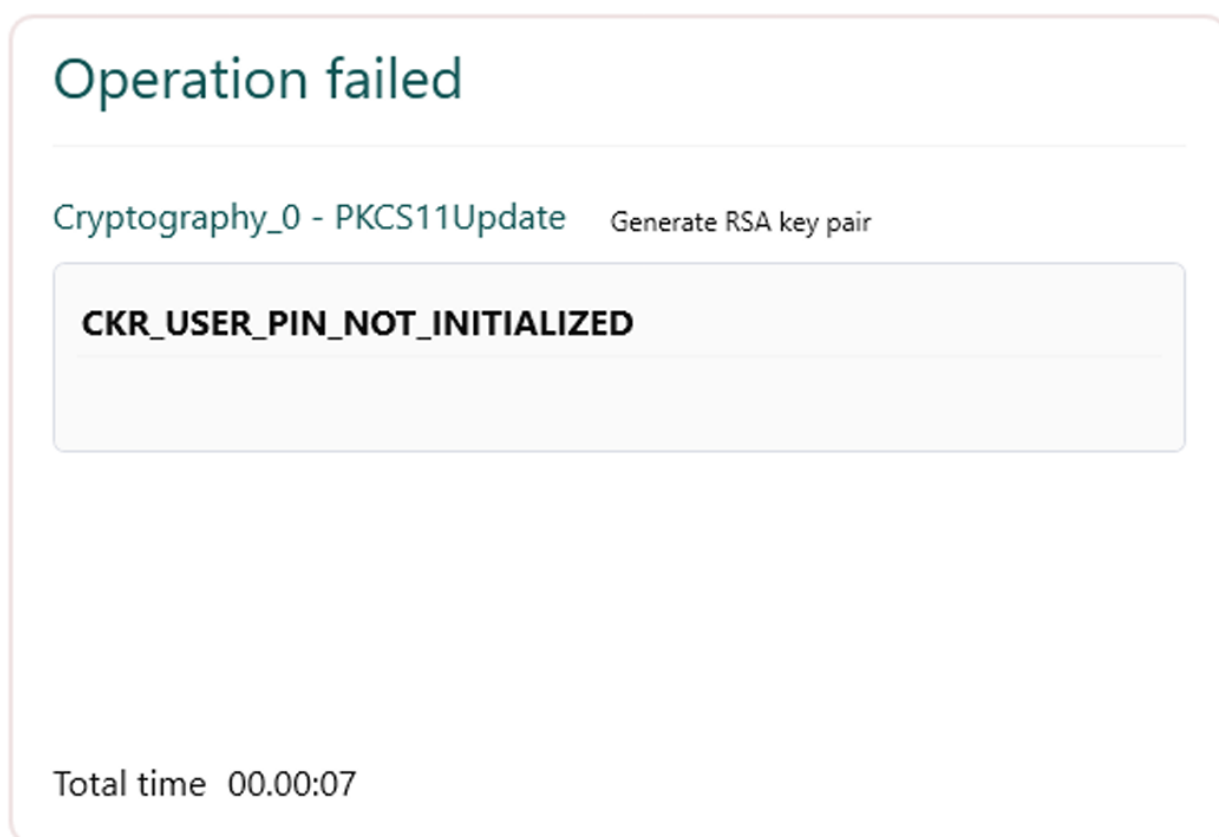


Figure 10 : Token Not Initialized Error

More information, e.g. time when the error occurred and in which plug-in the error occurred, can be found from the log file:

29.09.2026-23.00.37:499 [61340] PLUGIN Step #1, Plugin #3: Cryptography_0 - PKCS11Update Token not initialized

29.09.2026-23.00.37:502 [61340] PLUGIN Global, Plugin #1: PKCS11 Connector_0 - PKCS11Connector Login USER PIN

29.09.2026-23.00.37:507 [61340] PLUGIN Step #1, Plugin #3: Cryptography_0 - PKCS11Update
CKR_USER_PIN_NOT_INITIALIZED

29.09.2026-23.00.37:507 [61340] PLUGIN ERROR Step #1, Plugin #3: Cryptography_0 -
PKCS11Update CKR_USER_PIN_NOT_INITIALIZED

Some common issues are:

Problem	Resolution
Incorrect PKCS#11 module is selected in PKCS11Connector plug-in	Check the path and select the correct PKCS#11 library. By default, it is located at C:\Program Files\Utimaco\SecurityServer\Lib\cs_pkcs11_R3.dll Be sure to use the 64-bit version of the library with APM.
APM cannot connect the HSM	If you are using the simulator, ensure that the simulator is running. Ensure that the Devices parameter is configured correctly in cs_pkcs11_R3.cfg If you are using a network HSM, ensure that firewalls allow the traffic between your workstation and the HSM.
Wrong or uninitialized slot selected in PKCS11Connector plug-in	Select a slot which has been prepared for use as described in Configuration on Utimaco u.trust GP HSM Se-Series 6.1.

Problem	Resolution
HSM's security controls or consistency checks do not allow the operation	Check carefully that, for example, when creating new objects, the CKA_* attribute lists are consistent with the object type and usage. Verify that key wrapping, unwrapping or derivation is allowed in the attributes of the keys involved in key management operations. Verify that the appropriate usage attributes are set for the keys involved in crypto-operations.

9.2 Log Locations and Interpretation

PKCS#11 Logs:

Enabling PKCS#11 logging to facilitate easier testing and troubleshooting is recommended. This can be done by configuring the Logging Loglevel and LogPath parameters in the configuration file.

- LogPath should point to a writable directory (not a specific file) where log files can be stored.
- Login Log level controls the verbosity of the logs:
 - Set it to 1 for basic logging.
 - For detailed testing and debugging, increase the level to 4.

The generated log file will be named `cs_pkcs11_R3.log` and located in the directory specified by Log Path. Reviewing this log file can help identify and resolve issues that arise during testing.

Once testing is complete, it is advisable to reduce the Logging Log level to 1 or 2 to limit logging to only critical or important messages, thereby optimizing performance and reducing unnecessary log data.

APM Logs:

APM's logging options can be configured in the Settings dialog, which can be accessed by clicking the following icon in the upper right corner of the main window:



In the Settings dialog, you can set for example the log path and logging level. The higher the level, the more detailed log will be written. See APM's User Guide, Section 9 for more information. Be aware that the log may contain sensitive information. This can be addressed by setting a lower log level or protecting the log file from unauthorized access.

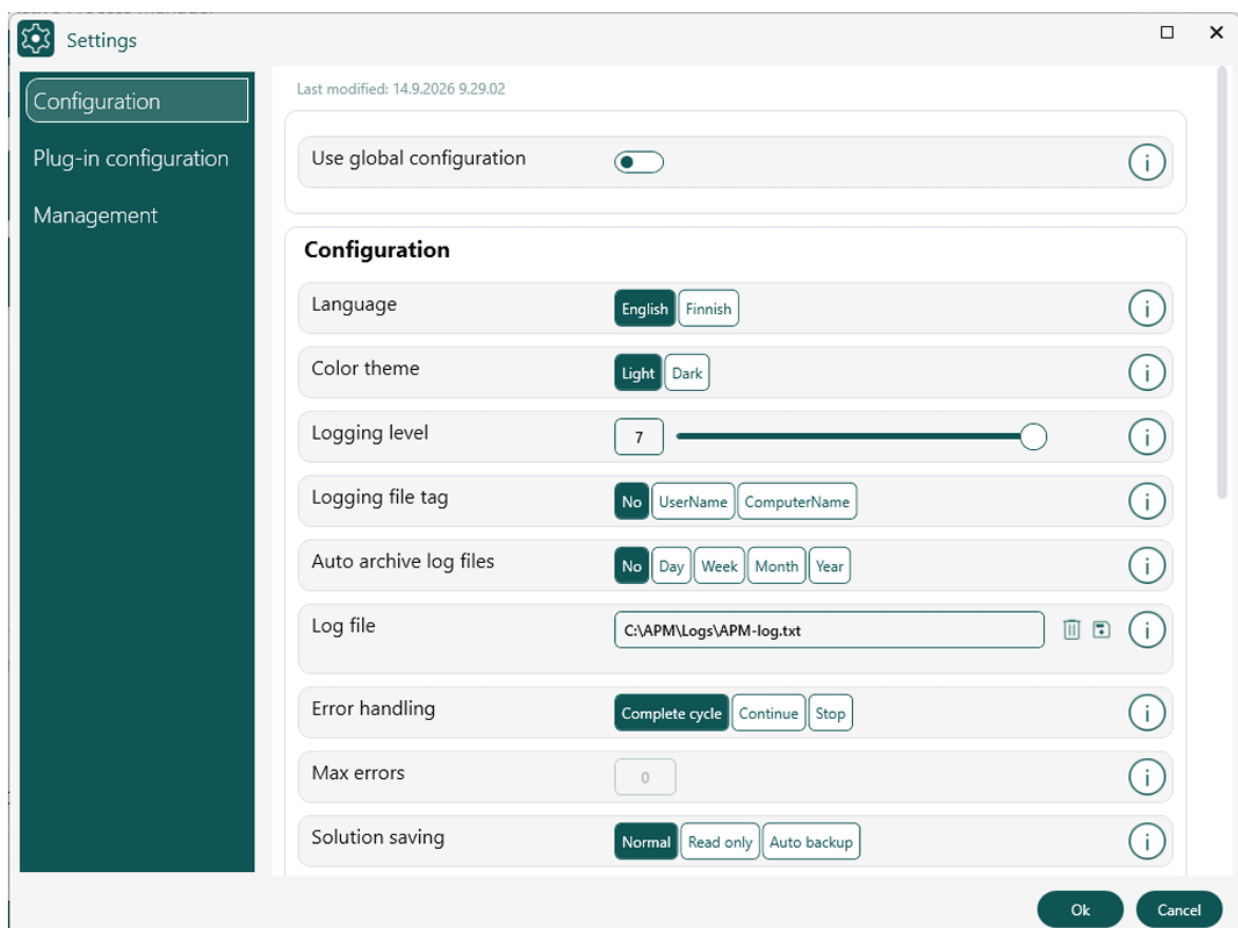


Figure 11 : Logging Settings

10 Contact and Support Information

Utimaco Contact 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.

Aventra Contact Information:

Aventra Oy
Kutomotie 16
00380 Helsinki
Finland

<https://aventra.fi>

Tel: +358 9 4251 1251

Mail: sales@aventra.fi

11 References

Title	Description	Document/Link
Active Process Manager User Guide		Active Process Manager User Guide v2 1.pdf
CryptoServer PKCS#11 R3 Developer Guide		SecurityServer_PKCS11_R3_DevGuide.pdf
CryptoServer CSP and CryptoServer CNG Key Storage Provider 1.x and 2.x Manual for System Administrators		CryptoServer_Manual_CSP_CNG.pdf
Open an RMA Case – Utimaco Portal		https://support.hsm.utimaco.com/ support/rma/new
Utimaco Support Portal		https://support.hsm.utimaco.com/ support/cases/new
Aventra – Simply Secure		https://aventra.fi/

Table 6: References