Adobe

Acrobat Pro

2025.001.20756

Integration Guide

u.trust GP HSM Se-Series

6.2.0

utimaco®

Imprint

Copyright 2025	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	2025-11-18
Status	PUBLISHED
Document No.	IG-2025-0059

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation for your Utimaco u.trust GP HSM Se-Series product can be found in the document directory of the Utimaco u.trust GP HSM Se-Series product bundle. All Utimaco u.trust GP HSM Se-Series product documentation is available on the Utimaco website at https://support.hsm.utimaco.com.

1.1 About This Guide

This guide provides a comprehensive walkthrough for integrating the Utimaco u.trust GP HSM Se-Series Hardware Security Module (HSM) with Adobe Acrobat Pro.

1.2 Target Audience

This guide is intended for administrators of Utimaco HSMs and users of Adobe Acrobat Pro.

1.3 Purpose of the Integration

This integration is primarily aimed at enhancing the security and compliance of digital document workflows. By leveraging Utimaco's Hardware Security Module (HSM), Adobe Acrobat can securely perform cryptographic operations such as digital signing and certificate-based encryption, ensuring that private keys are stored in a tamper-proof environment. This setup provides strong assurance of document authenticity, integrity, and non-repudiation, which is critical for regulated industries. Additionally, the integration supports compliance with standards such as eIDAS and FIPS, and utilizes PKCS#11 interfaces for seamless communication between Acrobat and the HSM, enabling secure and scalable document protection.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
PKI	Public Key Infrastructure

Abbreviation	Meaning
TDE	Transparent Data Encryption
PKCS	Public Key Cryptography Standards
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
PDF	Portable Document Format

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**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

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

2 Product Overview

2.1 Adobe Acrobat

Adobe Acrobat is a software suite for working with PDF documents, enabling users to view, edit, create, sign, and share PDFs. While the free Acrobat Reader allows basic tasks like reading and commenting, paid versions like Acrobat Standard and Pro offer advanced features such as converting other file types to PDF, advanced editing, combining multiple files, collecting e-signatures, comparing document versions, and protecting sensitive information.

2.2 Utimaco u.trust GP HSM Se-Series

u.trust GP HSM Se-Series 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

Adobe Acrobat leverages PKCS#11 modules to interact with hardware tokens, such as Utimaco's u.trust GP HSM Se-Series, to securely sign PDFs by providing a standard interface for Acrobat to access the token's private keys and perform cryptographic operations.

Adobe Acrobat uses a PKCS#11 module to encrypt a PDF by loading the module, which provides a secure interface to the certificate and its private key stored on a hardware token like SecurityServer. Acrobat then selects the appropriate digital ID (certificate) via the PKCS#11 interface to sign the document. This process establishes an encrypted digital signature, ensuring document authenticity and integrity, and allowing only intended recipients with the corresponding private key or certificate to decrypt the document.

3 Integration Requirements and Prerequisites

Ensure the system environment that you are using meets the following hardware and software requirements.

3.1 Tested Versions

The integrations that have been successfully tested:

Operating System	Adobe Acrobat Pro	Utimaco SecurityServer Version	Utimaco HSM
Windows 10	2025.001.20756 (64 bit)	SecurityServer 6.2.0	u.trust GP HSM Se Series

Table 3: List of Tested Versions

3.2 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 Prerequisites

Before you begin, please ensure that you have:

- Installed and set up the operating system listed in Tested Versions.
- Installed and set up SecurityServer, listed in Tested Versions.

- Replaced SecurityServer Default Admin with a new admin user.
- Set up and configured SecurityServer. Refer to the SecurityServer documentation to set up the HSM.
- Set up and configured the PKCS#11 library as per your environment. Refer to the SecurityServer documentation to set up and configure the PKCS#11 library.
- Adobe Acrobat Pro Subscription / License.
- The user with admin privileges to install the Adobe Acrobat Pro package.

3.4 Software Requirements

Software	Software Requirements
Adobe Acrobat Pro	2025.001.20756
HSM Utility	SecurityServer PKCS#11 Tool (p11tool2)
HSM Interfaces	SecurityServer PKCS#11 Provide

Table 5: List of Software Requirements

4 Installation and Configuration

4.1 Setting Up the Utimaco u.trust GP HSM Se-Series

Install the latest version of the Utimaco u.trust GP HSM Se-Series software if it has not already been installed.

1. Locate the configuration file, cs_pkcs11_R3.cfg. On Windows, as part of the Utimaco u.trust GP HSM Se-Series software installation, cs_pkcs11_R3.cfg will be created automatically and will be available in the **C:\ProgramData\Utimaco\PKCS11_R3** folder.
2. Edit the cs_pkcs11_R3.cfg file and make the appropriate changes to the file as shown below.

```
[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 CryptoServer documentation. The device could be a CryptoServer HSM, 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 Be sure to select the appropriate format based on your specific hardware setup.

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 Loglevel 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 Loglevel to limit output to only critical or important messages

4.2 Setting Up Adobe Acrobat

- Visit https://www.adobe.com and sign in using your Adobe ID associated with an active Acrobat Pro subscription.
- Navigate to the Products or Account section and locate Acrobat Pro. Download the installation file.
- Open the downloaded file and follow the on-screen instructions to install Adobe Acrobat Pro.
- After installation, launch Acrobat Pro. Sign in again with your Adobe ID to activate the subscription and unlock full features.

5 Integration Steps

5.1 Configuration on Utimaco u.trust GP HSM Se-Series

5.1.1 Initialize a Slot

1. Log in to the PKCS11 Admin Tool as Admin, create a security officer (SO), and initialize a new token.

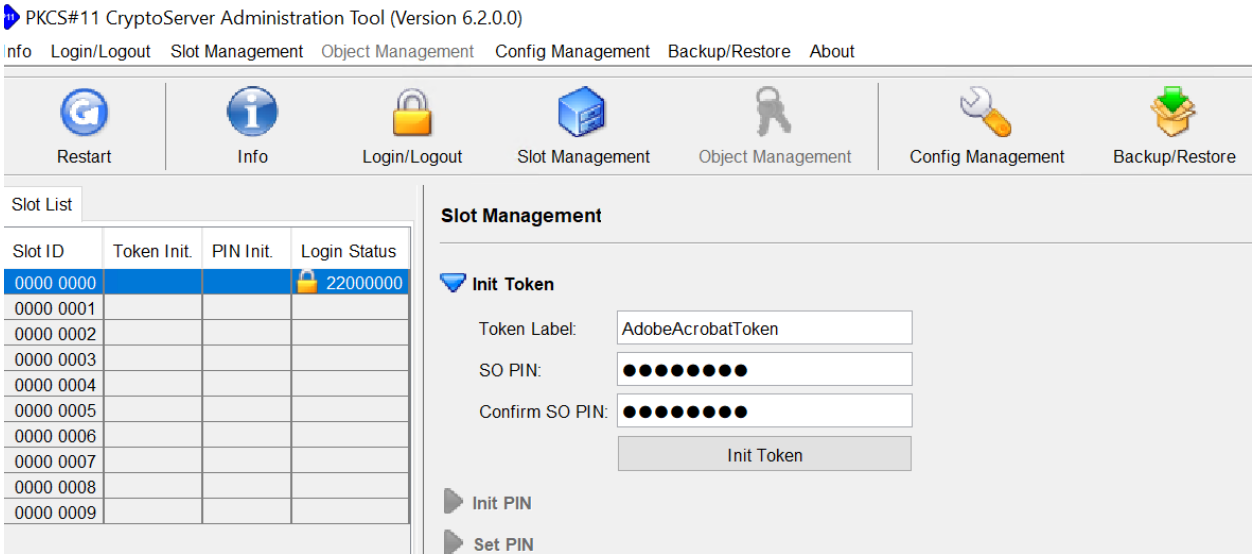

Figure 1 : Initialize the Token

2. Log in to the PKCS11 Admin Tool as SO.
3. Click on the **Slot Management** icon and click the **Set PIN** link.
4. Change the SO PIN.

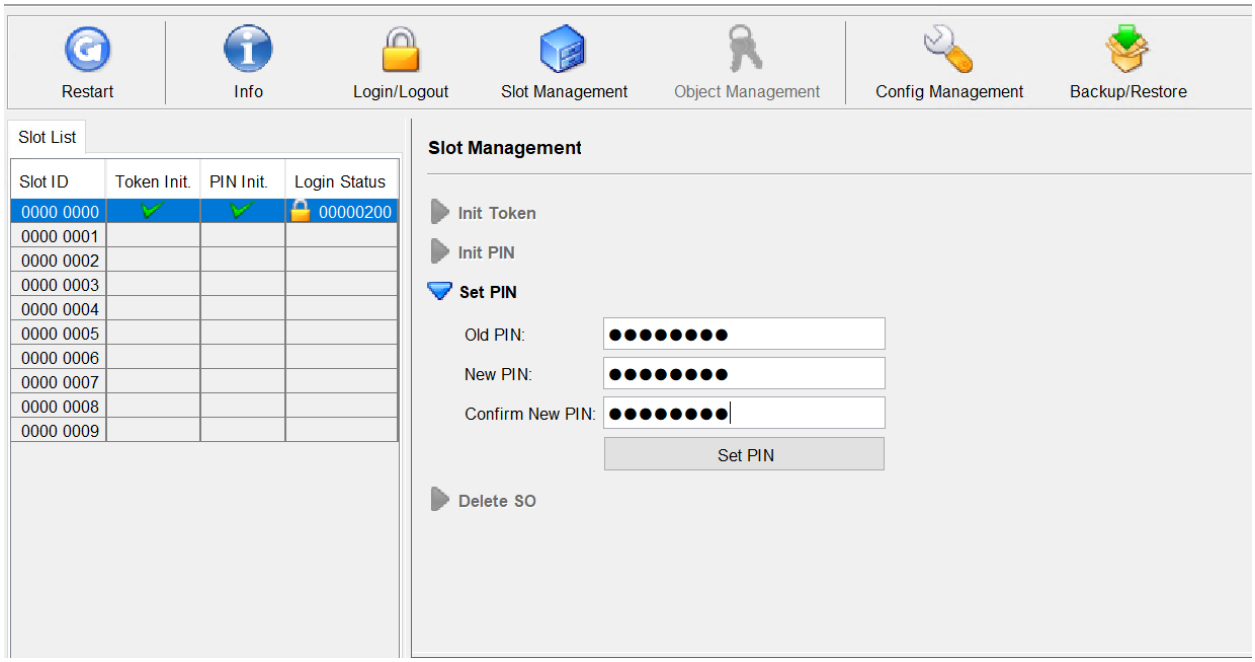

Figure 2 : Change SO PIN

5. Log in to the PKCS11 Admin Tool as the SO user and initialize a crypto user with the PIN.

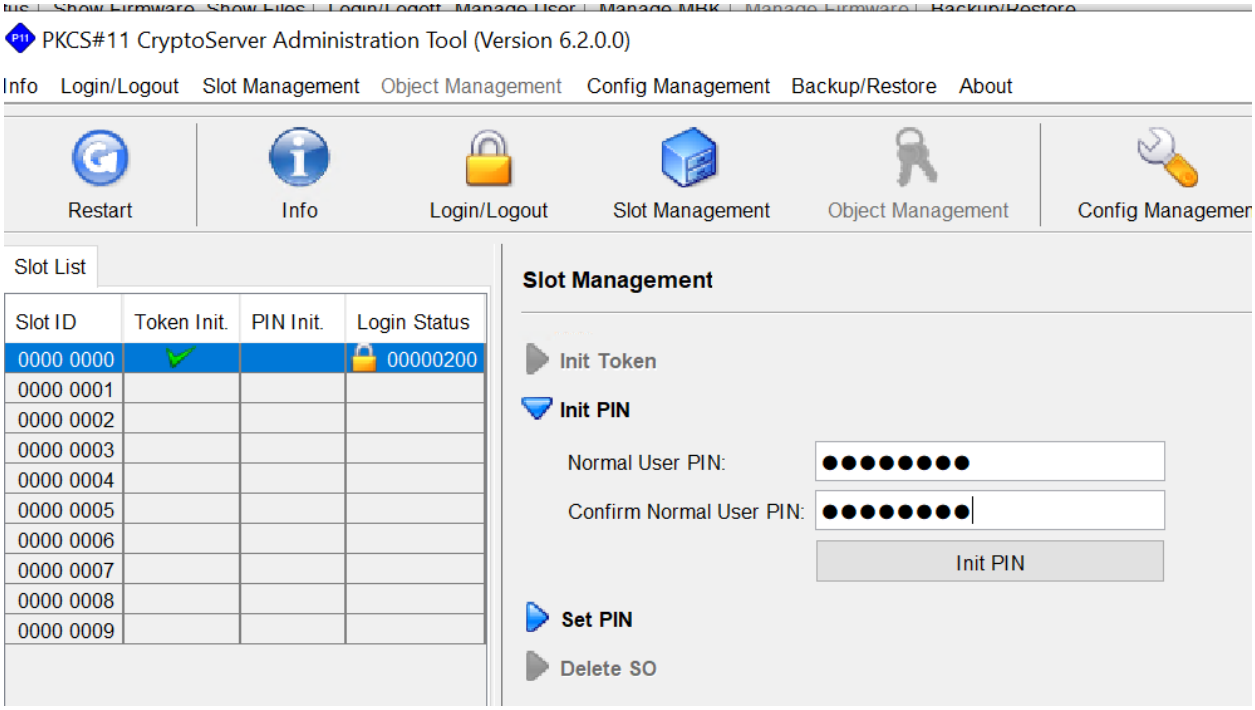

Figure 3 : Initialize a crypto user

6. Change the PIN of the crypto user.

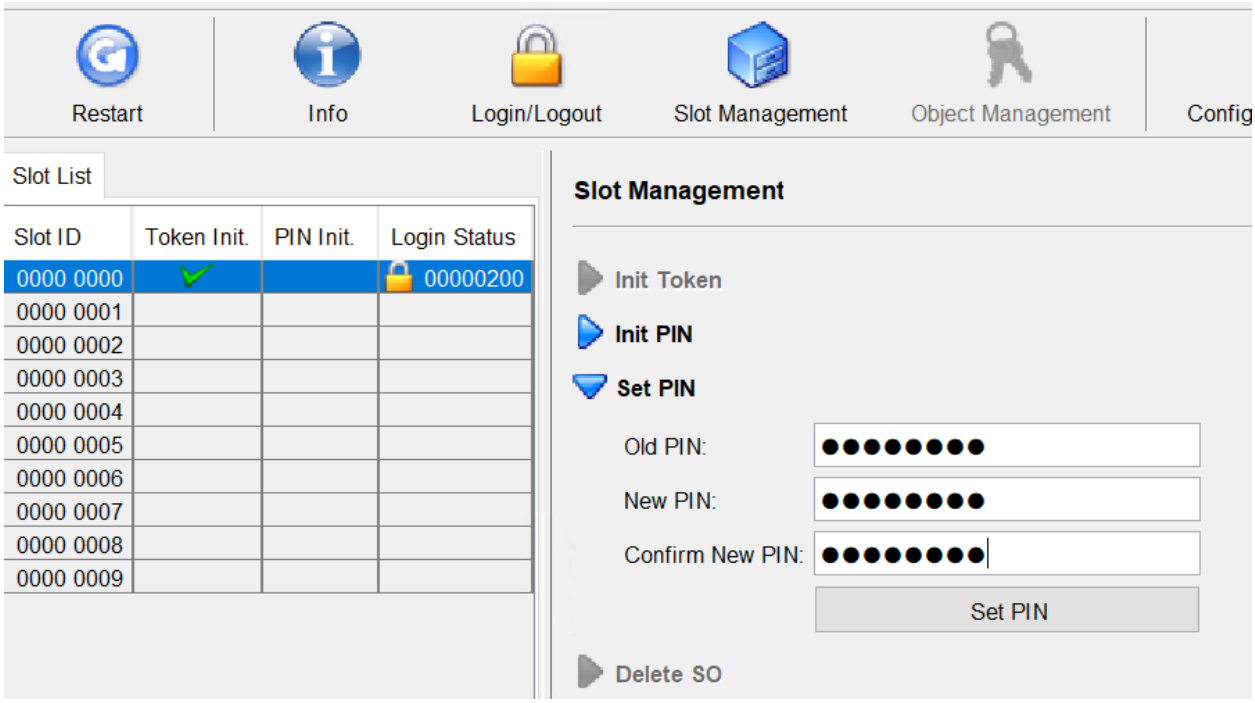

Figure 4 : Change and set PIN for crypto user

7. Log in to the PKCS11 Admin Tool. Click the **Info** icon and click on the **Token Info** link

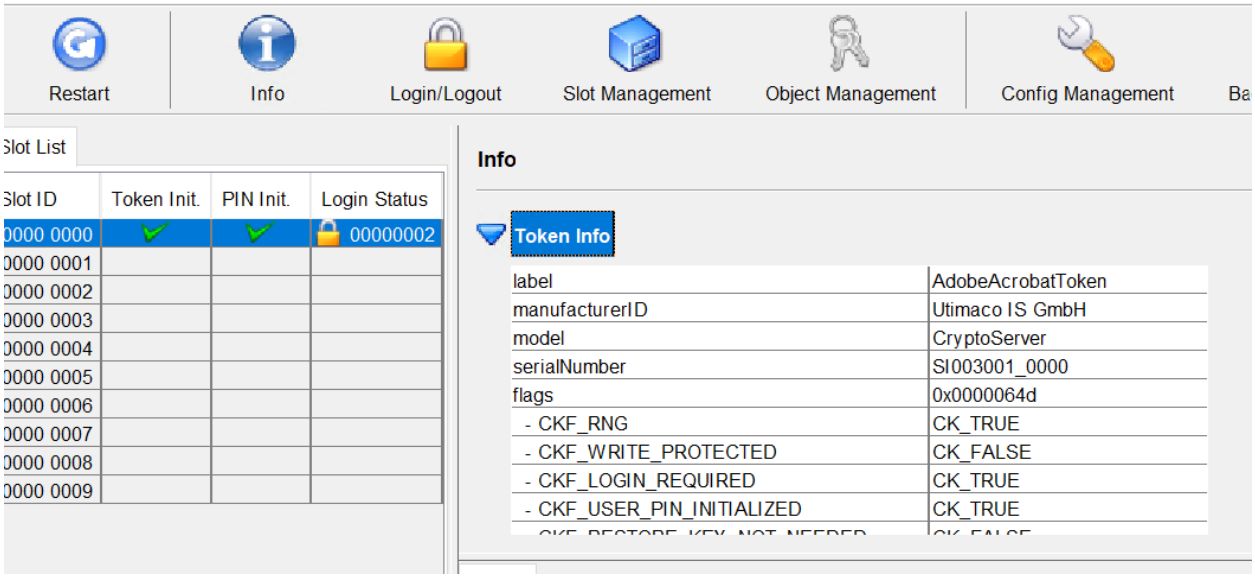

Figure 5 : Token Info

5.2 Configuration on Adobe Acrobat

Adobe Acrobat uses PKCS#11 modules to interact with cryptographic tokens like smart cards or USB devices for digital signatures, allowing users to add a digital ID by attaching the relevant module (a .dll file) in **Preferences > Signatures > Identities & Trusted Certificates > PKCS#11 Modules and Tokens**. When attaching, ensure the correct version of the module for your Acrobat installation (32-bit for 32-bit Acrobat, 64-bit for 64-bit Acrobat) and that the token is properly inserted and detected by the operating system.

1. Open a PDF document in Adobe Acrobat.
2. Go to **Menu > Preferences**.
3. Select **Signatures** from the **Categories** list on the left.
4. Under **Identities & Trusted Certificates**, find the **PKCS#11 Modules and Tokens** section.

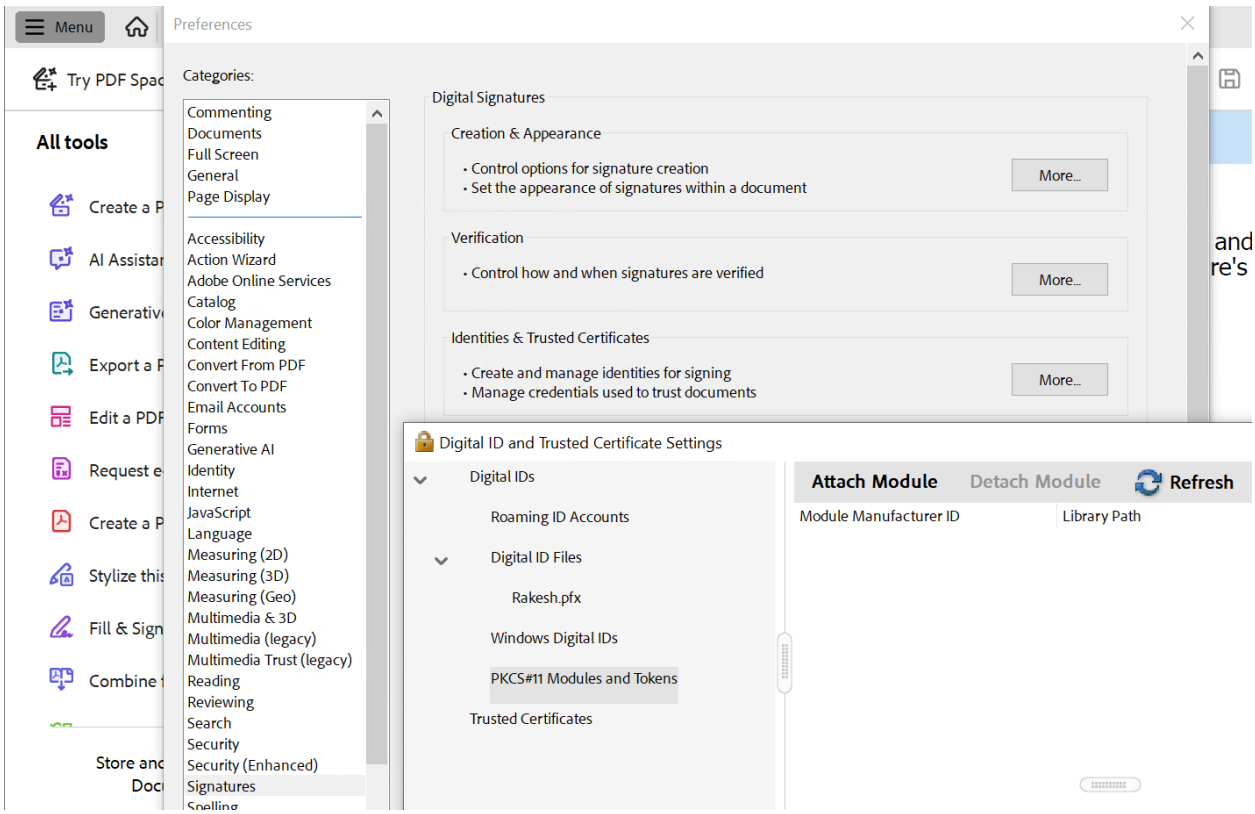

Figure 6 : Token section

5. Click **Attach Module**.
6. A dialog box will appear, asking for the full path to the PKCS#11 module's library file.
7. Enter the path of the SecurityServer module (e.g., C:\Program Files\Utimaco\SecurityServer\Lib\ cs_pkcs11_R3.dll).
8. Click **OK**.

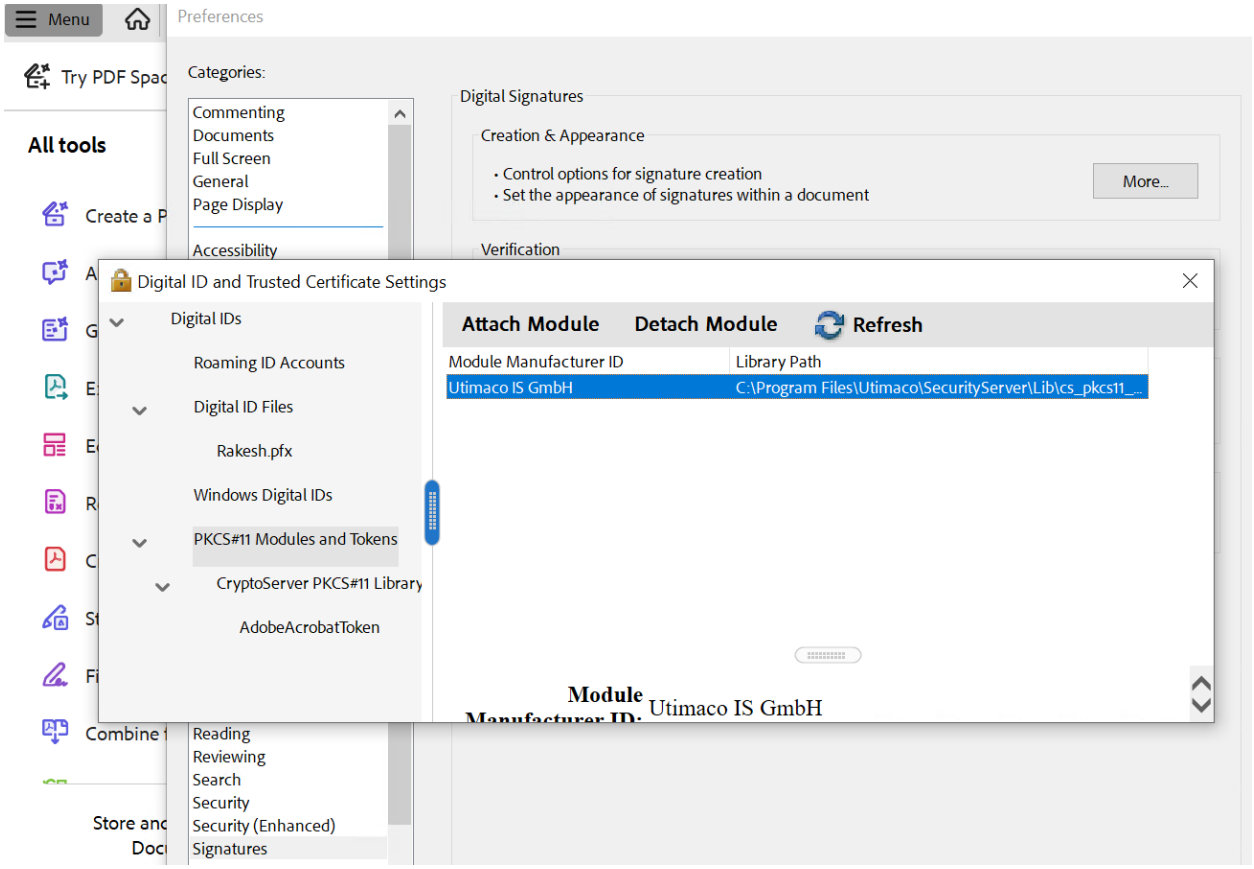

Figure 7 : Attach Module in PDF

5.2.1 Create a Digital ID

1. Open a PDF document in Adobe Acrobat Pro.
2. Go to **Menu > Preferences**.
3. Select **Signatures** from the **Categories** list on the left.

4. Under **Identities & Trusted Certificates,** click on **More** and find the PKCS#11 Modules and Tokens section.
5. Click to expand **CryptoServer PKCS#11 Library R3**.
6. Select the Token and click on the **Login**.
7. Enter the **Password** and click **OK.**

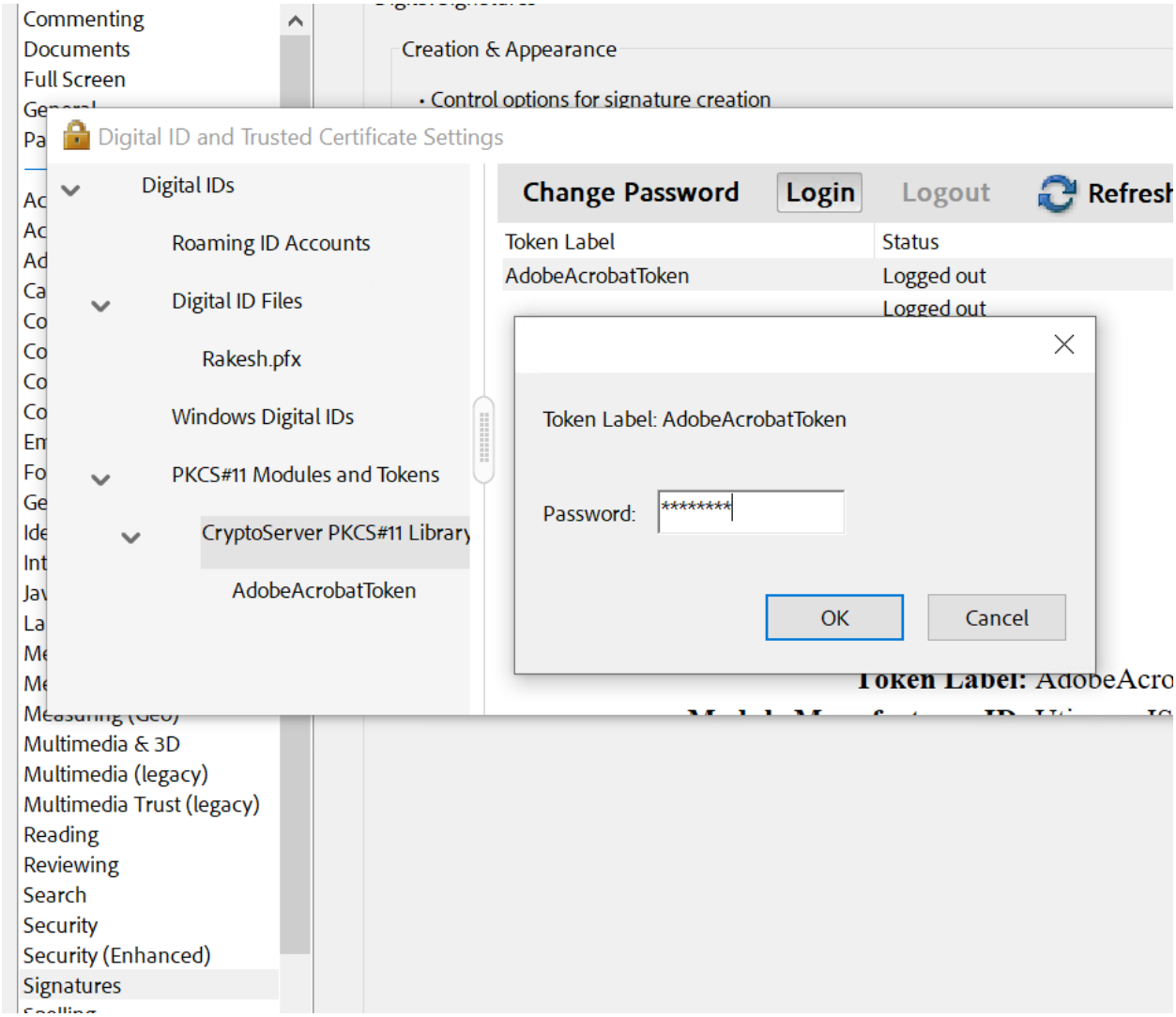

Figure 8 : Login

8. Click the **Add Digital ID** button.
9. Enter the slot **User PIN** to log into the Token.

10. Select **Add a new self-signed digital ID** radio button.

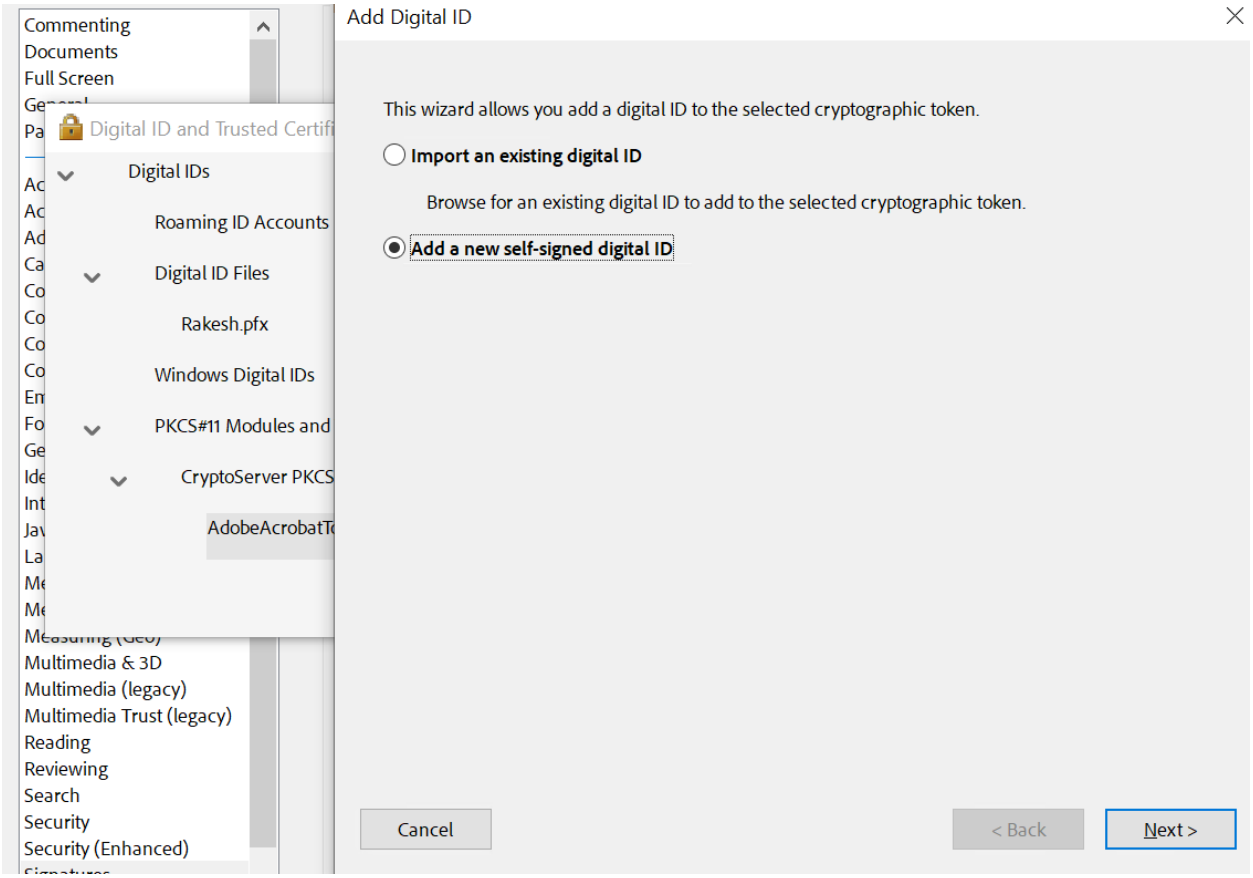

Figure 9 : Add New Digital ID

11. Fill out the **Add Digital ID** form with all information, select 2048-bit RSA from **Key Algorithm,** and select Digital Signatures and Data Encryption from **Use digital ID for:** then click **Finish.**

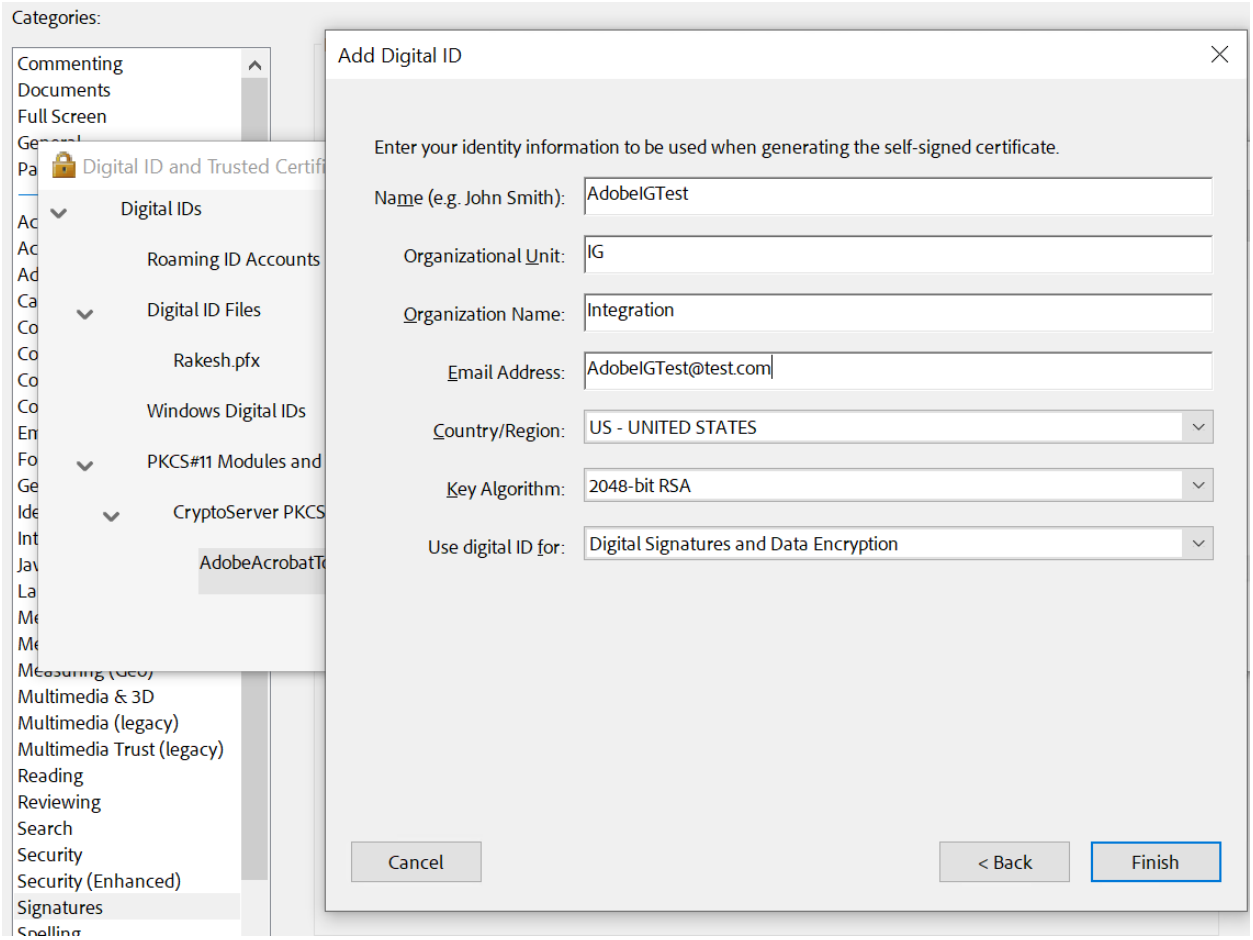

Figure 10 : Add Digital ID

12. Click on the token name and verify created digital ID is now available and stored securely in the token.

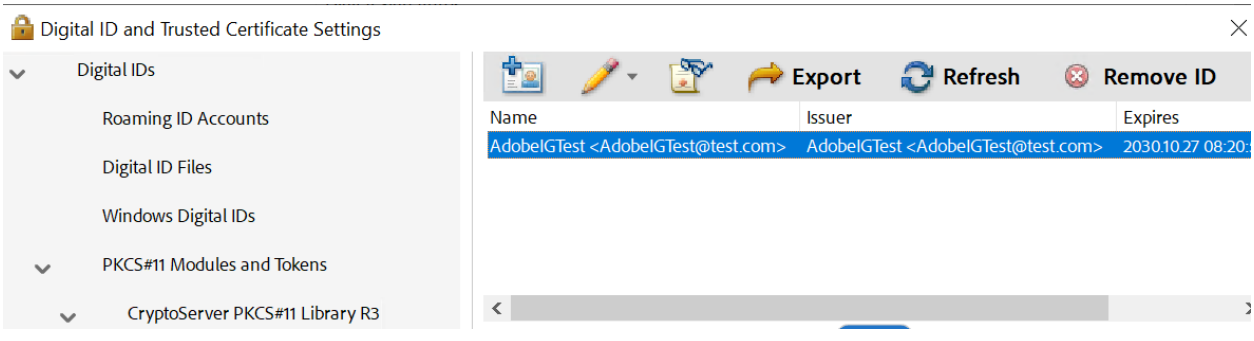

Figure 11 : Digital ID Details

13. Click on **Digital IDs** and check the newly created digital ID in the right section.

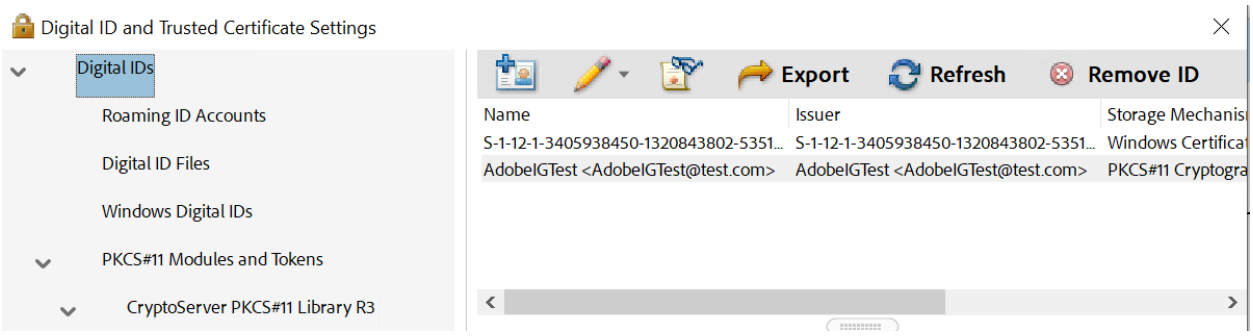

Figure 12 : Newly created digital ID updated in Digital ID's section

14. Close out to return to the Adobe Menu.
15. Log in as a Crypto user to the PKCS11 CryptoServer Administrator Tool.
16. Click the **Object Management** icon.
17. Corresponding Keys and Certificate displayed in the PKCS11 CryptoServer Administrator Tool.

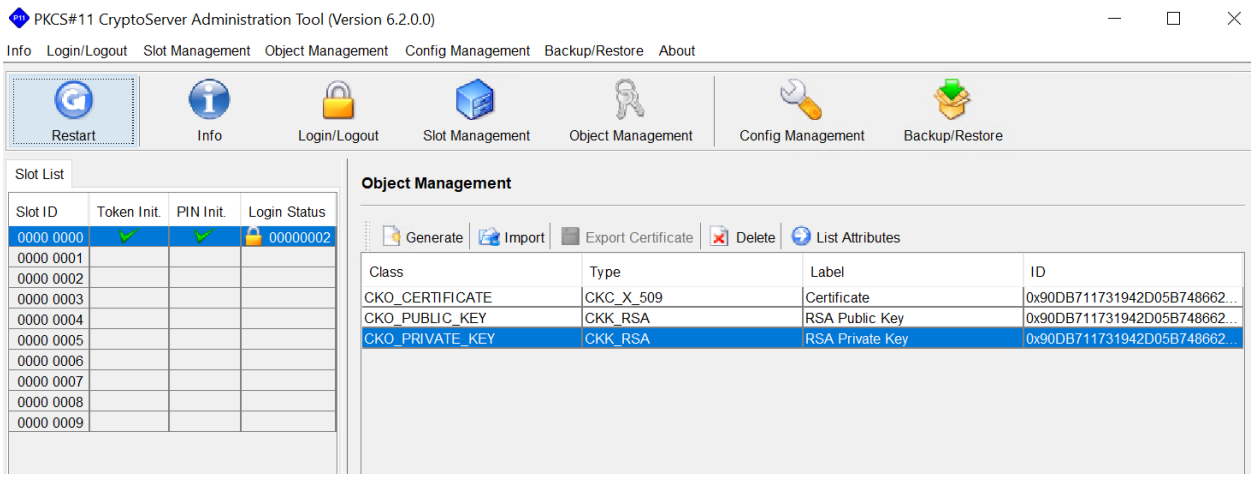

Figure 13 : Key and Certificate Details In PKCS11 Tool

6 Verification and Testing

6.1 Sign PDF Using Digital ID

1. Open a PDF document.
2. Click **All Tools** on the top Menu.
3. Click **Use a certificate** from the left side menu.
4. Click **Digitally sign.**

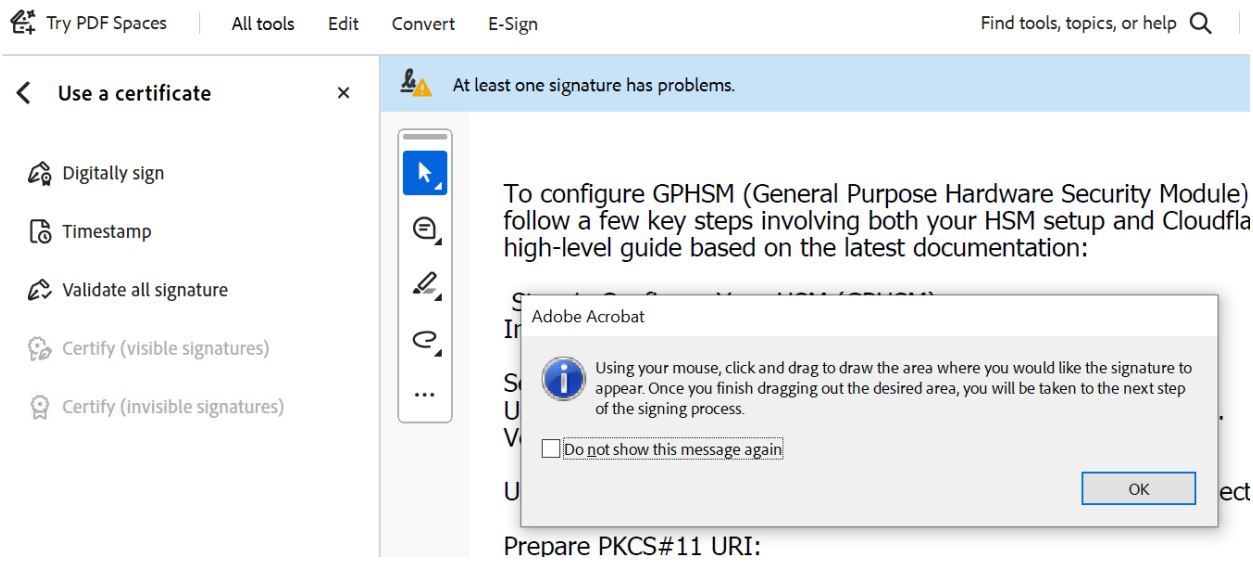

Figure 14 : Select a place to sign

5. Use the cursor to draw a box where the user wants to sign the document.
6. In **Sign with a Digital ID**, choose the Digital ID, then click **Continue.**

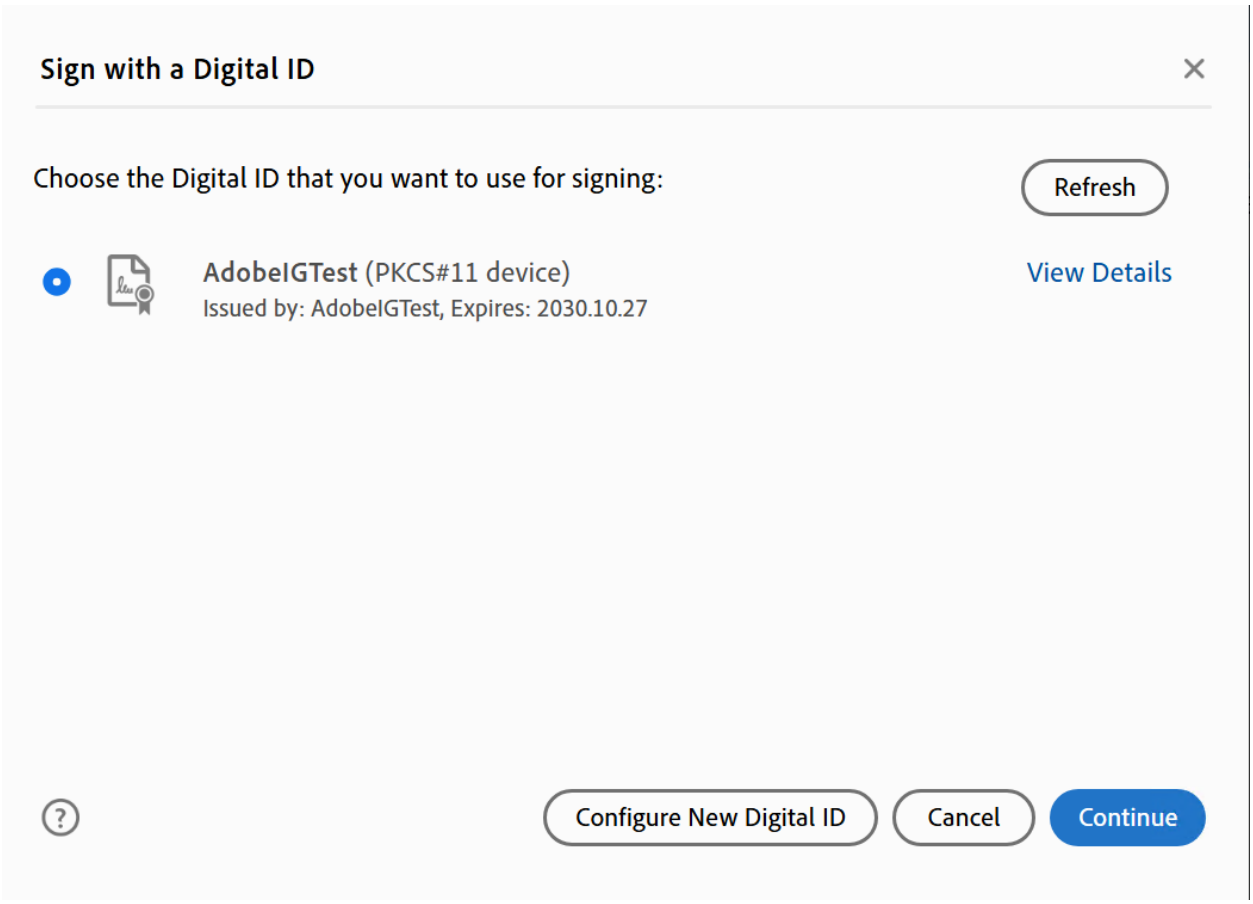

Figure 15 : Select Digital ID

7. Click on the **Sign** button, **Sign as "<Digital ID Name>"** screen
8. Save the file when it prompts to do so.
9. Verify the sign displayed in the document.

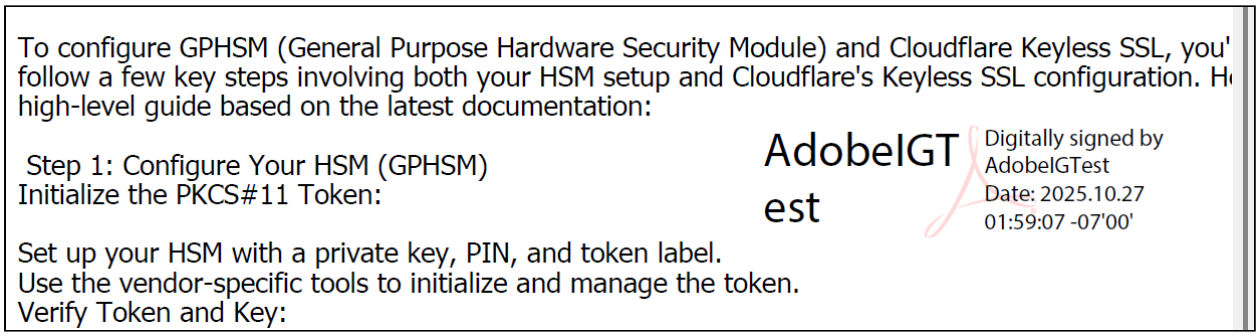

Figure 16 : Digital ID displayed in selected area

6.2 Encrypt and Decrypt PDF Using Digital ID

Encrypt PDF using your Digital ID

1. Open a PDF document in Adobe Acrobat Pro.
2. Click **All Tools**.
3. Click **Protect a PDF**.
4. Click **Encrypt with a Certificate.**
5. Click **Next**.
6. In the Document Security window, select your digital ID, then click **OK.**
7. Click **Next** on the C**ertificate Security Settings** screen.
8. Click **Finish.**

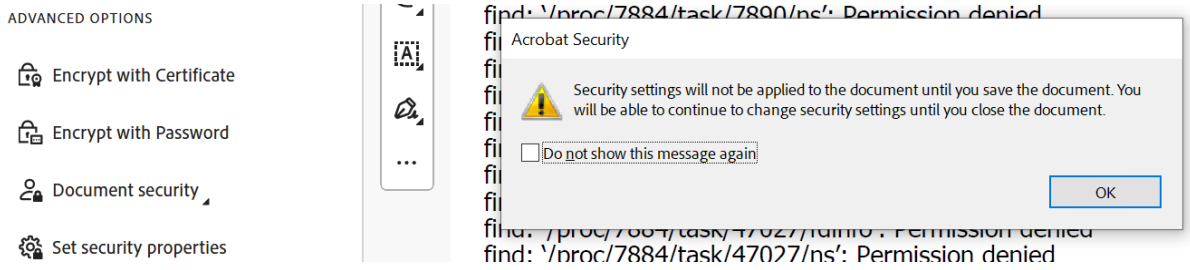

Figure 17 : Warning Message

9. Click **OK** in the **Adobe Security** settings warning.

10. **Close** the document and click **Yes** to save changes.

Decrypt Document using Digital ID

1. Open an encrypted PDF document in Adobe Acrobat Pro.
2. In the Digital ID Authentication window, enter the user PIN in the **Password** box.
3. Click **OK.**

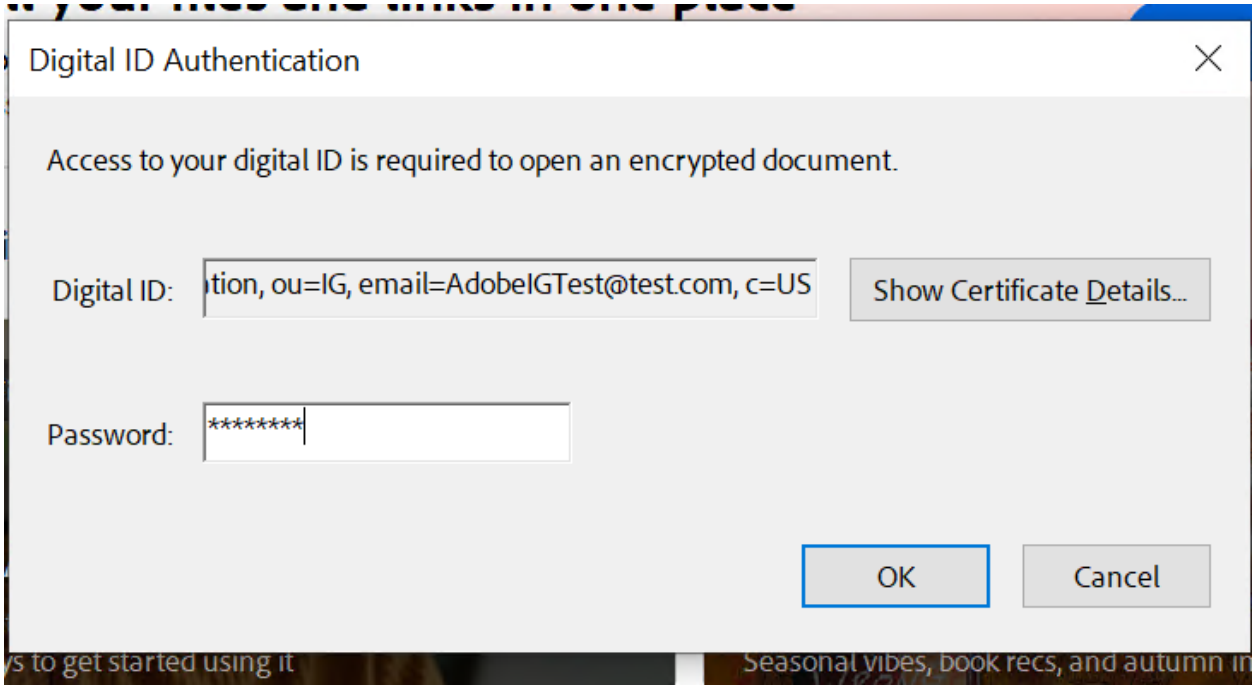

Figure 18 : Authentication Window

4. The PDF file opens with all content.

6.3 Encrypt a Signed PDF

1. Open a signed PDF document in Adobe Acrobat Pro.
2. Click **All Tools**.
3. Click **Protect a PDF**.
4. Click **Encrypt with a Certificate**.

5. Observe an error message.

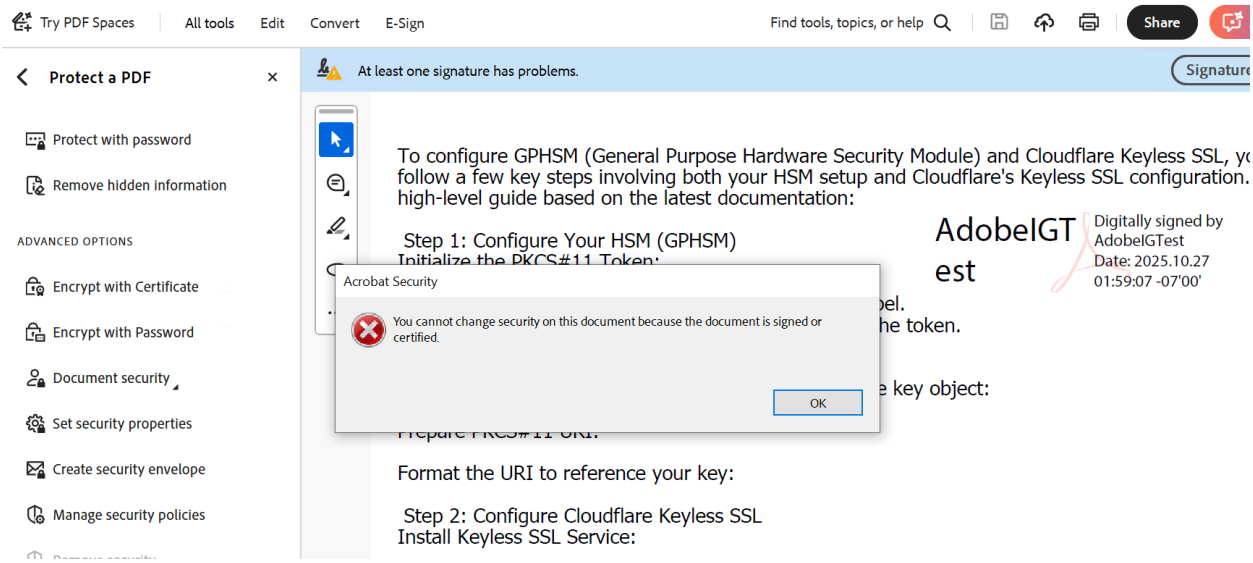

Figure 19 : Error Message

6.4 Logs and Validation Steps

To facilitate easier testing and troubleshooting, it is recommended to enable PKCS#11 logging. 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. Logging Loglevel controls the verbosity of the logs:

- Set it to 1 for basic logging.
- For detailed testing and debugging, increase the level to 4.

The log file generated will be named cs_pkcs11_R3.log and will be located in the directory specified by LogPath. If any issues arise during testing, reviewing this log file can help identify and resolve them.

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

6.5 Upload User's Own Digital ID and Manage Digital ID in HSM

1. Open **Adobe Acrobat Pro**.

2. Go to **Menu > Preferences > Signatures**.
3. Under **Identities & Trusted Certificates**, click **More**.
4. In the **Digital IDs** section, click **Add ID**.
5. Choose **A new digital ID I want to create now**, then click **Next**.

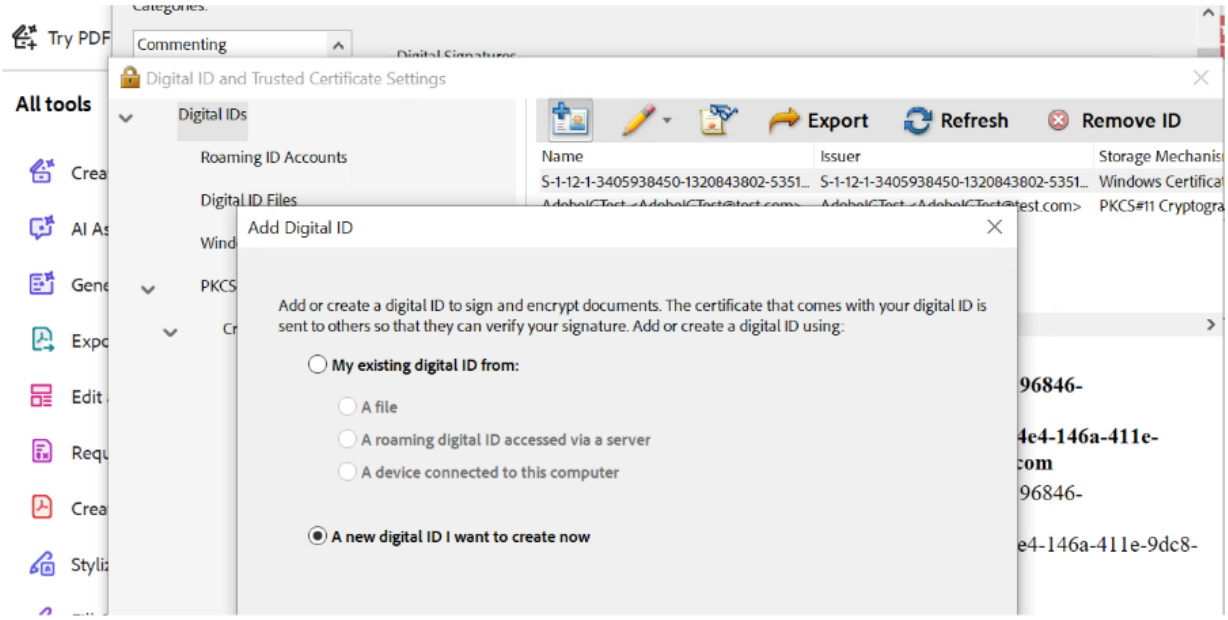

Figure 20 : Select New Digital ID

6. Select **New PKCS#12 Digital ID File** and click **Next**.
7. Fill in all identity details (Name, Email, etc.).
8. Choose **2048-bit RSA** as the key algorithm.

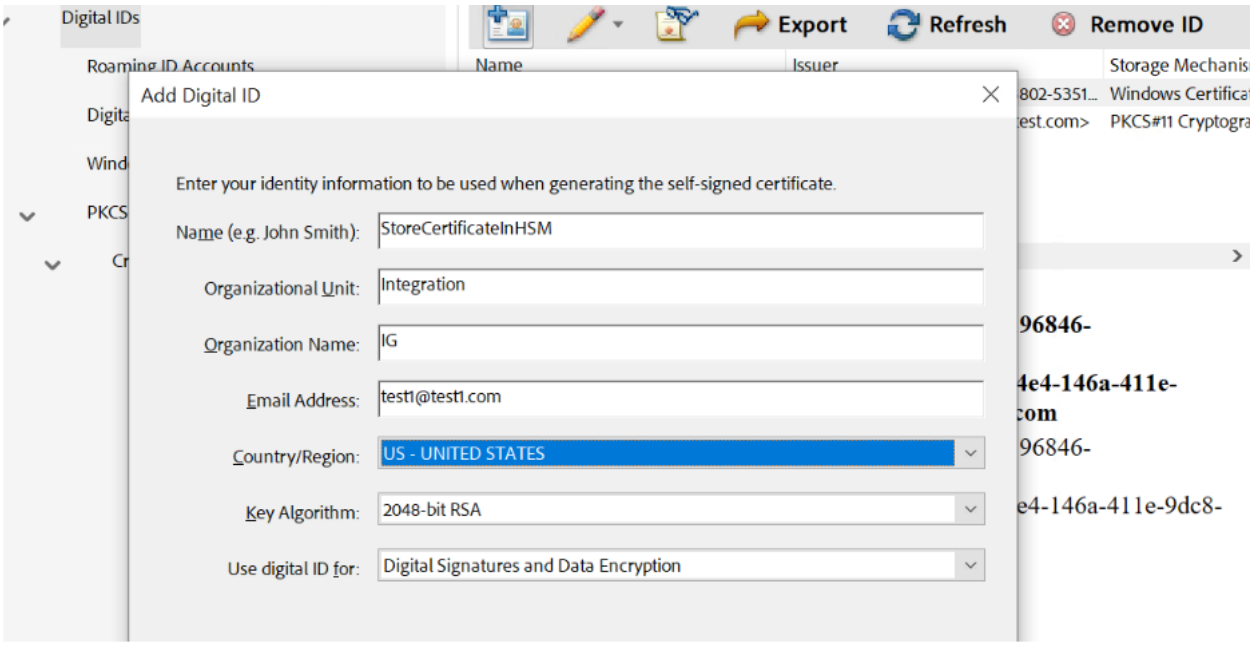

Figure 21 : Add Details

9. Set a password and choose a location to save the `.pfx` or `.p12` file.
10. Click **Finish** to create the Digital ID.

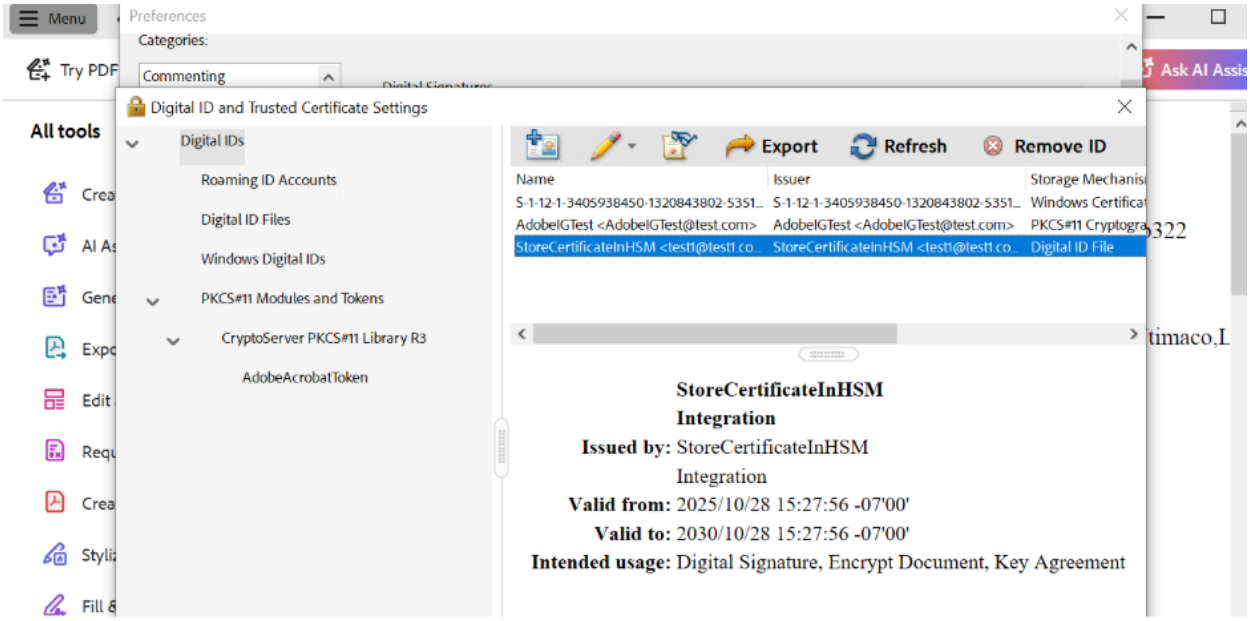

Figure 22 : Digital ID Created

11. Open **PKCS#11 CryptoServer Administration Tool (CAT)**.
12. Log in as Crypto User.
13. Go to the **Object Management** tab.
14. Click On **Import**.
15. Select **Import PKCS#12.**
16. Upload the Digital ID file and enter the **Password**.

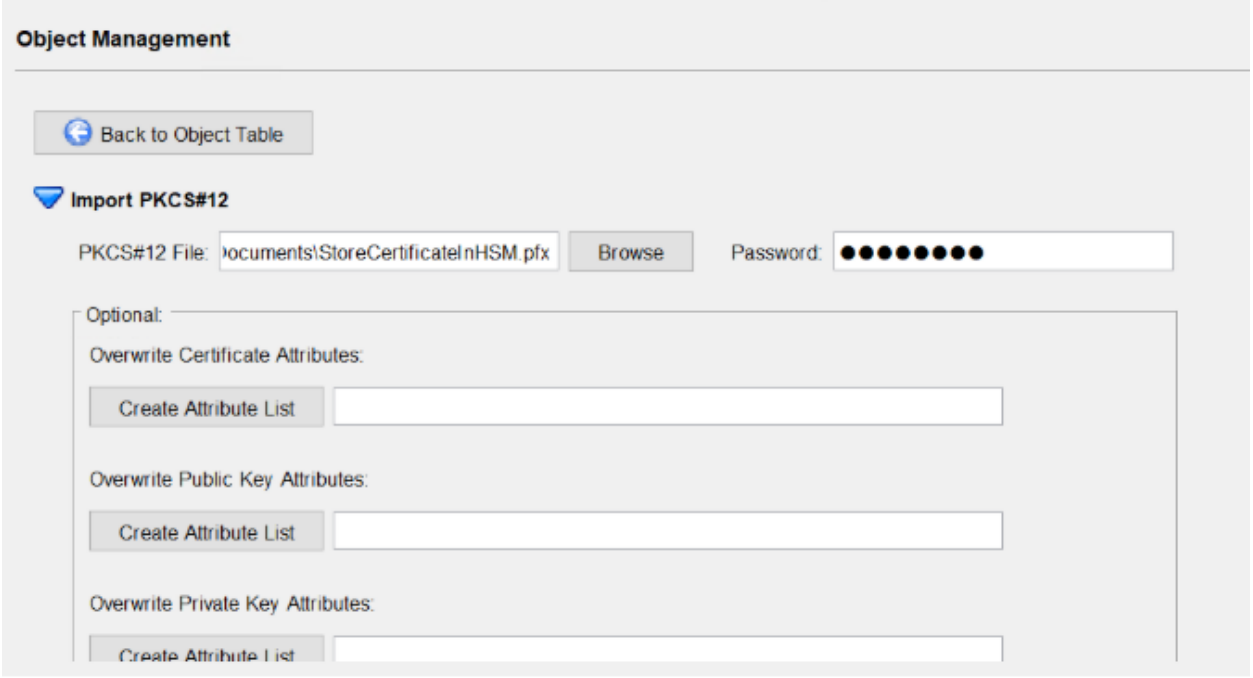

Figure 23 : Import Digital ID file

17. Go to the **Object Management** tab.
18. Key details display in the **Object Management** screen.

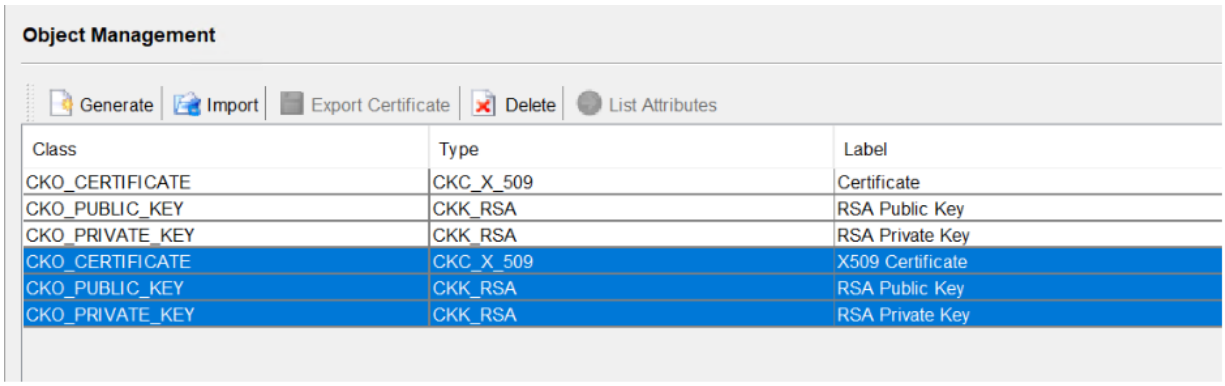

Figure 24 : Imported Key Details

19. Open Acrobat Pro as Administrator.
20. Go to **Edit > Preferences > Signatures**.
21. Click **More** under **Identities & Trusted Certificates**.
22. Navigate to **PKCS#11 Modules and Tokens**.
23. Click **CryptoServer PKCS#11 Library R3** and log in to the token.
24. Select the token displayed below and click the **Refresh** button.
25. Acrobat will detect the token and list available digital IDs.

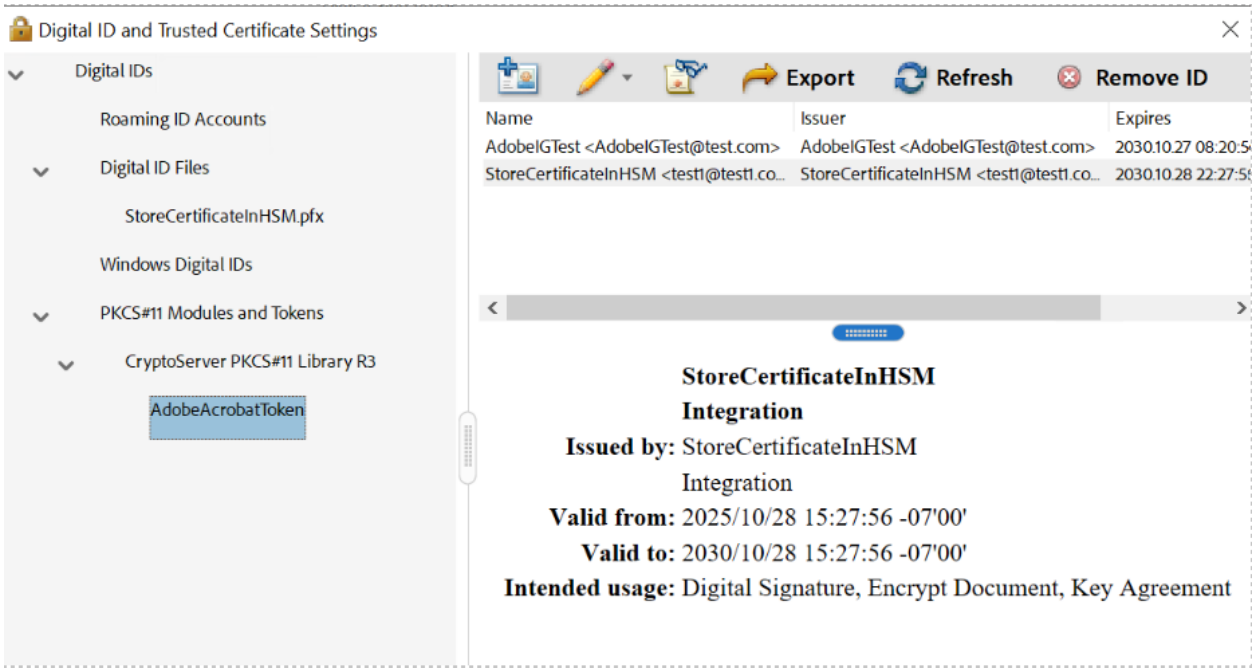

Figure 25 : Digital ID Displayed in Acrobat Pro

26. Open a PDF in Acrobat Pro.
27. Go to **All Tools> Use a certificate**.
28. Click **Digitally sign and select /drag an area to place the sign.**
29. Select the digital ID stored in the HSM.

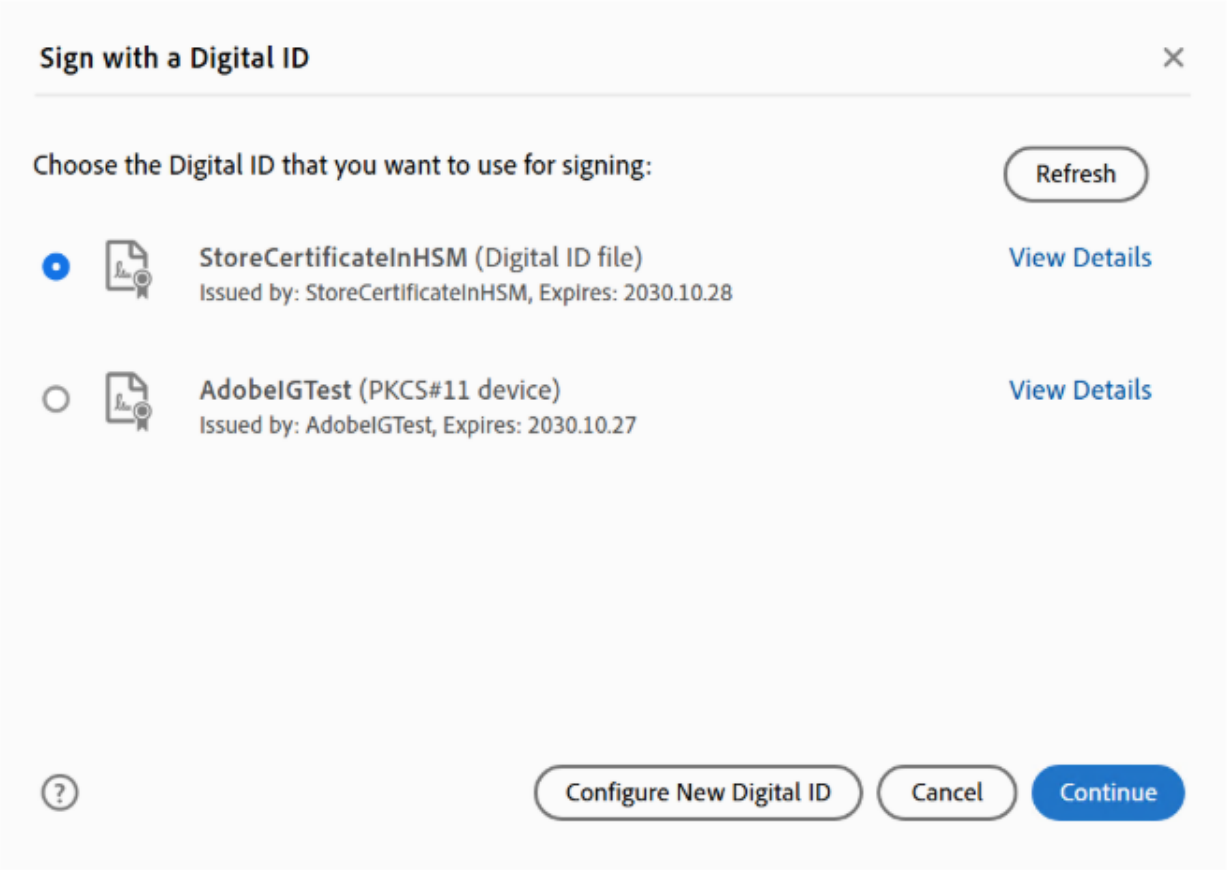

Figure 26 : Digital ID's stored in the HSM.

30. Click **Continue**.
31. Enter the **Password** and click **Sign**.
32. Save the file.

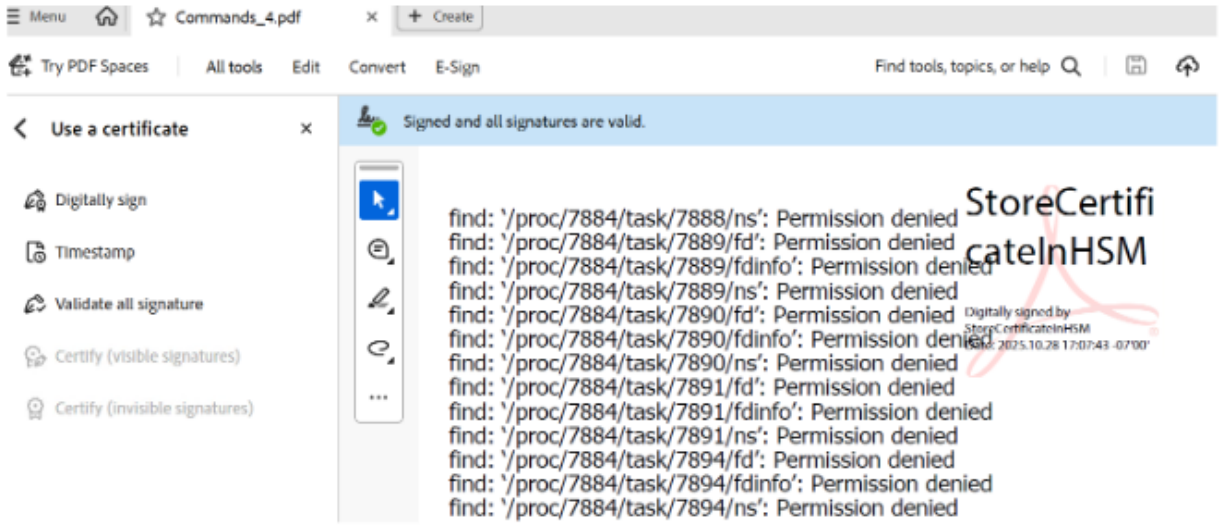

Figure 27 : Digital Signed

7 Troubleshooting

7.1 Log locations and interpretation

Understanding where logs are stored is essential for effective troubleshooting.

7.1.1 PKCS#11 Log File

Log File Name: cs_pkcs11_R3.log

- Location: Defined by the LogPath parameter in the PKCS#11 configuration file. Example: **\tmp** for Linux and **C:\ProgramData\Utimaco\PKCS11_R3** for Windows.
- Details: This log captures detailed information about PKCS#11 operations, including initialization, cryptographic actions, and error messages. The verbosity is controlled by the Logging Loglevel setting.

7.1.2 Adobe Acrobat Log File

Location: For Windows **%temp%/Acrobat_Diagnostics/Output/**

To access: Go to **Help > Troubleshoot Acrobat**

To enable: **Preferences > General > Enable troubleshooting** (select the checkbox)

Details: Acrobat includes a built-in diagnostics tool that helps collect detailed logs and system information. It captures process monitor logs, product logs, and system data, along with optional dumps like registry, plist, and memory. This tool is especially useful for troubleshooting crashes, hangs, and performance-related issues.

8 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.

9 Appendices

9.1 References

This document provides a detailed guide for integrating Utimaco's u.trust GP HSM Se-Series with Adobe Acrobat Pro. For further details on Utimaco's full range of products, solutions, and documentation, please visit the official Utimaco Portal.