Adobe Experience Manager Forms

nShield® HSM Integration Guide

2024-10-21

Table of Contents

1. Introduction . . . 1
    1.1. nShield configurations . . . 1
    1.2. Software configurations . . . 1
    1.3. Requirements . . . 1
2. Install and configure the Entrust nShield HSM . . . 3
    2.1. Select the protection method . . . 3
    2.2. Install the HSM . . . 3
    2.3. Install the nShield Security World Software and create the Security World . . . 3
    2.4. Generate the OSC or Softcard in the CA server . . . 4
3. Procedures . . . 7
    3.1. Prerequisites . . . 7
    3.2. Configure Java . . . 8
    3.3. Generate a signed certificate on the HSM . . . 9
    3.4. Configure the HSM credential alias . . . 10
4. Additional resources and related products . . . 13
    4.1. nShield Connect . . . 13
    4.2. nShield as a Service . . . 13
    4.3. Entrust products . . . 13
    4.4. nShield product documentation . . . 13

Chapter 1. Introduction

Adobe Experience Manager Forms is an end-to-end digital document solution that enables the creation of forms that customers can complete and securely e-sign. Digital signatures in AEM Forms can use credentials stored in an Entrust nShield HSM to apply server-side digital signatures.

1.1. nShield configurations

Entrust has successfully tested the integration of an nShield HSM with Adobe Experience Manager Forms in the following configurations:

Product	Security World Software	Firmware	Netimage	OCS	Softcard	Module
nSaaS	12.80.4	12.72.1 (FIPS 140-2 certified)	12.80.5	✓	✓	✓
Connect XC	12.80.4	12.72.1 (FIPS 140-2 certified)	12.80.5	✓	✓	✓
nShield 5c	13.2.2	13.2.2	13.2.2	✓	✓	✓

1.2. Software configurations

Entrust has successfully tested the integration of an nShield HSM with Adobe Experience Manager Forms using the AEM Forms on JEE deployment using the following versions:

Base OS	Java	AEM Forms	JBoss	MSSQL Server
Windows Server 2019	JDK 1.8.0_321	6.5.15.0	Red Hat JBoss EAP 7.4.0.GA	2019

1.3. Requirements

Before starting the integration process, familiarize yourself with the Adobe Documentation and Software Requirements along with nShield Documentation. The following include links to documentation for Adobe Experience Manager Forms used in this integration:

- Supported Platforms for AEM Forms on JEE
- Installing and Deploying Adobe Experience Manager Forms on JEE for JBoss
- Preparing to install AEM Forms (Single Server)
- Managing HSM credentials
- Adobe Experience Manager 6.5 Latest Service Pack Release Notes

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Install and configure the Entrust nShield HSM

To install and configure the Entrust HSM:

1. Select the protection method
2. Install the HSM
3. Install the nShield Security World Software and create the Security World
4. Generate the OSC or Softcard in the CA server

2.1. Select the protection method

OCS, Softcard, or Module protection can be used to authorize access to the keys protected by the HSM. Follow your organization's security policy to select which one.

2.2. Install the HSM

Install the nShield Connect HSM locally, remotely, or remotely via the serial console. See the following nShield Support articles and the *Installation Guide* for the HSM:

- How to locally set up a new or replacement nShield Connect
- How to remotely set up a new or replacement nShield Connect
- How to remotely set up a new or replacement nShield Connect XC Serial Console model

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

2.3. Install the nShield Security World Software and create the Security World

To install the nShield Security World Software and create the Security World:

1. Install the Security World software as described in *Installation Guide* and the *User Guide* for the HSM. This is supplied on the installation disc.

2. Add the Security World utilities path `/opt/nfast/bin` to the system path.
3. Open the firewall port 9004 for the HSM connections.
4. Open a command window and confirm the HSM is `operational`:

```
# enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        530E-02E0-D947 7724-8509-81E3 09AF-0BE9-53AA 9E10-03E0-D947
 mode                 operational
...
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        530E-02E0-D947
 mode                 operational
 ...
```

5. Create your Security World if one does not already exist, or copy an existing one. Follow your organization's security policy for this. Create extra ACS cards as spares in case of a card failure or a lost card.

ACS cards cannot be duplicated after the Security World is created.

6. Confirm the Security World is `usable`:

```
# nfkminfo
World
 generation  2
 state       0x37270008 Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
```

2.4. Generate the OSC or Softcard in the CA server

The OCS or Softcard and associated passphrase will be used to authorize access to the keys protected by the HSM. Typically, one or the other will be used, but rarely both. Follow your organization's security policy to select which one to use.

2.4.1. Create the OCS

To create the OCS:

1. Ensure file `/opt/nfast/kmdata/config/cardlist` contains the serial number of the card(s) to be presented, or the asterisk wildcard (*).
2. Open a command window as administrator.
3. Run the `createocs` command as described below, entering a passphrase or password at the prompt.

   Follow your organization's security policy for this for the values K/N, where K=1 as mentioned above. Use the same passphrase for all the OCS cards in the set (one for each person with access privilege, plus the spares). Note that `slot 2`, remote via a Trusted Verification Device (TVD), is used to present the card.

   After an OCS card set has been created, the cards cannot be duplicated.

   ```
   # createocs -m1 -s2 -N testOCS -Q 1/1

   FIPS 140-2 level 3 auth obtained.

   Creating Cardset:
    Module 1: 0 cards of 1 written
    Module 1 slot 0: Admin Card #1
    Module 1 slot 2: empty
    Module 1 slot 3: empty
    Module 1 slot 2: blank card
    Module 1 slot 2:- passphrase specified - writing card
   Card writing complete.

   cardset created; hkltu = a165a26f929841fe9ff2acdf4bb6141c1f1a2eed
   ```

   Add the **-p** (persistent) option to the command above to retain authentication after the OCS card has been removed from the HSM front panel slot, or from the TVD. The authentication provided by the OCS as shown in the command line above is non-persistent and only available while the OCS card is inserted in the HSM front panel slot, or the TVD.

4. Verify the OCS was created:

   ```
   # nfkminfo -c
   Cardset list - 1 cardsets:  (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
    Operator logical token hash              k/n timeout  name
    a165a26f929841fe9ff2acdf4bb6141c1f1a2eed  1/1  none-NL testOCS
   ```

   The `rocs` utility also shows the OCS was created:

   ```
   # rocs
   'rocs' key recovery tool
   Useful commands: 'help', 'help intro', 'quit'.
   rocs> list cardset
   No. Name                    Keys (recov) Sharing
     1 testOCS                 0 (0)        1 of 1
   ```

```
rocs> quit
```

2.4.2. Create the Softcard

To create the Softcard:

1. Run the following command and enter a passphrase or password:

```
# ppmk -n EntrustSNSoftcard

Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU d9414ed688c6405aab675471d3722f8c70f5d864
```

2. Verify the Softcard was created:

```
# nfkminfo -s
SoftCard summary - 1 softcards:
 Operator logical token hash               name
 d9414ed688c6405aab675471d3722f8c70f5d864  testSC
```

The `rocs` utility also shows that the OCS and Softcard were created:

```
# rocs
`rocs` key recovery tool
Useful commands: 'help', 'help intro', 'quit'.
rocs> list cards
No. Name                    Keys (recov) Sharing
  1 testOCS                 0 (0)        1 of 1
  2 testSC                  0 (0)        (softcard)
rocs> quit
```

Chapter 3. Procedures

To configure Adobe Experience Manager Forms with the nShield HSM:

1. Prerequisites
2. Configure Java
3. Generate a signed certificate on the HSM
4. Configure the HSM credential alias

3.1. Prerequisites

Before you can use Adobe Experience Manager Forms with the nShield HSM, complete the following steps:

1. Install the Java Development 8 Kit.
2. Set up the HSM client software on the machine where Adobe Experience Manager Forms will be installed.
3. Configure the HSM(s) to have the IP address of your host machine as a client.
4. Create or edit the `cknfastrc` file in `nfast` directory add one of the following two config settings:
   - Module protection:

     ```
     CKNFAST_FAKE_ACCELERATOR_LOGIN=1
     ```

   - OCS or Softcard protection:

     ```
     CKNFAST_LOADSHARING=1
     CKNFAST_NO_ACCELERATOR_SLOTS=1
     ```

   - Optional lines to enable debug:

     ```
     CKNFAST_DEBUG=5
     CKNFAST_DEBUGFILE=C:\pkcs11.log
     ```

5. Install Adobe Experience Manager Forms. To do this, follow the Adobe online documentation and set up AEM forms on a JEE deployment:

   Preparing to install AEM Forms (Single Server)

   When setting up, ensure that the user account has login permissions to the database server.

For more information on configuring and managing nShield HSMs, Security Worlds, and Remote File Systems, see the *User Guide* for your HSM(s).

3.2. Configure Java

You must configure Java for the nShield HSM before you can use the HSM with Adobe Experience Manager Forms Credentials.

1. Add lines to `C:\ProgramData\nCipher\Key Management Data\config\config` about privileged and non-privileged ports:

```
[server_startup]
...
priv_port=9001
nonpriv_port=9000
```

2. Open a command prompt as Administrator.
3. Set the path variables:

```
% setx JAVA_HOME "C:\Program Files\Java\jdk1.8.0_321"
% setx PATH "%PATH%;%JAVA_HOME%\bin";
```

4. Copy the `nCipherKM.jar` file to the `extensions` folder of your local Java Virtual Machine installation from the following directory:

```
%NFAST_HOME%\java\classes
```

5. Paste the file in the following directory:

```
%JAVA_HOME%\jre\lib\ext
```

6. Download the JCE Unlimited Strength Jurisdiction Policy Files from your Java VM vendor's Web site. The downloaded Java 8 file used in this guide was `jce_policy-8`.
7. Extract and copy the extracted files `local_policy.jar` and `US_export_policy.jar` into the security directory:

```
%JAVA_HOME%\jre\lib\security
```

8. Edit the `java.security` file in `%JAVA_HOME%\jre\lib\security`.
9. Add the following line to the top of the list of providers and shift the rest of

the numbers down to keep them in ascending order:

```
security.provider.1=com.ncipher.provider.km.nCipherKM
```

10. Open a command prompt as Administrator and run:

```
% java com.ncipher.provider.InstallationTest
```

The output includes a list of providers and nShield JCE services. Check for the following phrases within the output:

```
Unlimited strength jurisdiction files are installed.
The nCipher provider is correctly installed.
```

3.3. Generate a signed certificate on the HSM

An nShield HSM will be used to generate a Certificate Signing Request to then be signed and imported. This certificate will be later used by AEM Forms Credentials.

If you are using FIPS 140 Level 3, PKCS #11 requires HSM OCS cards for FIPS authentication when you are importing the signed certificate. When you are running the `ckcerttool` command at a later step, you will have to insert the OCS card(s).

1. Open command prompt as administrator and run the required command:
   - Module protection:

     ```
     % generatekey pkcs11 protect=module certreq=yes type=rsa size=2048 pubexp=65537 plainname=<key_name>
     nvram=no
     ```

   - OCS protection:

     ```
     % generatekey pkcs11 cardset=<cardset_name> protect=token certreq=yes type=rsa size=2048 pubexp=65537
     plainname=<key_name> nvram=no
     ```

   - Softcard protection:

     ```
     % generatekey pkcs11 softcard=<cardset_name> protect=softcard certreq=yes type=rsa size=2048
     pubexp=65537 plainname=<key_name> nvram=no
     ```

2. Take note of the path to the key and the CSR.

3. Take the CSR file to a Certificate Authority and have it signed.
4. Take the generated signed certificate file and place it in the same directory where the CSR file was originally generated.
5. Open command prompt as administrator and run one of the following to import the signed certificate:
   - Module protection:

     ```
     % ckcerttool -n -f <signed_cert_filename> -k <identof the key, the part after pkcs11_> -L
     <label_for_the_key>
     ```

   - OCS and Softcard protection:

     ```
     % ckcerttool -c <cardset name> -f <signed_cert_filename> -k <identof the key, the part after pkcs11_>
     -L <label_for_the_key>
     ```

     For example (OCS protection):

     ```
     % ckcerttool -c testOCS -f ocscertificate.cer -k uc6951563523344ac316e14299c7006a8e0aecd377-
     30f2a9379f7f23b6710e14d4f80ed2b1a45e99ee -L aemocskey
     ```

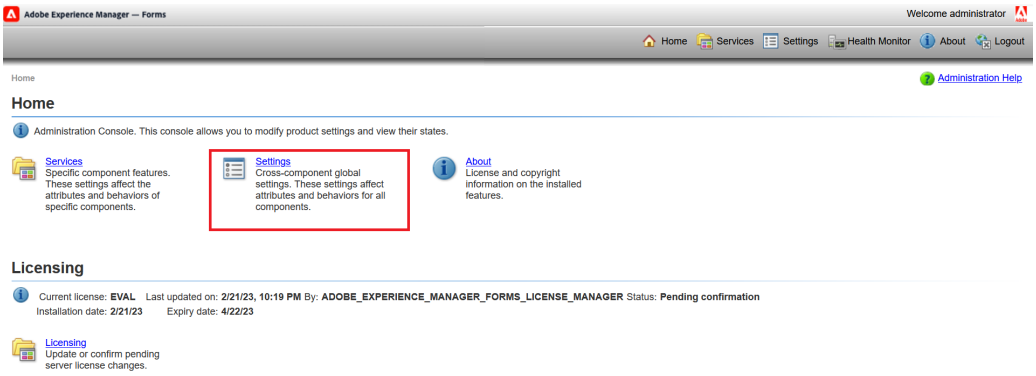
     Check for the following phrases within the output:

     ```
     Certificate found, processing...
     Certificate successfully imported.
     Run cklist to view your certificate object.
     OK
     ```

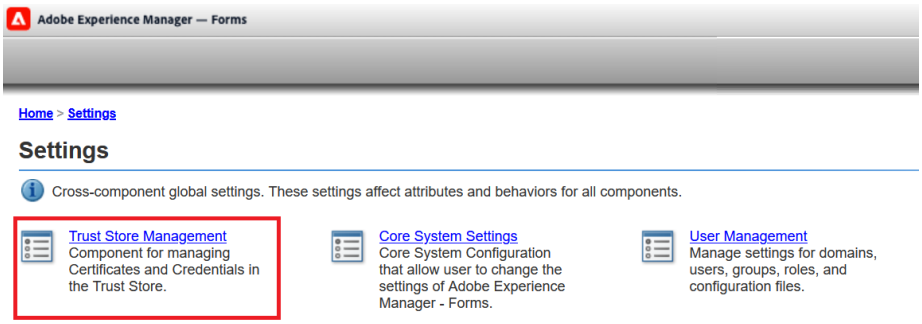
3.4. Configure the HSM credential alias

If you generated the HSM certificate while the Application Server was running, AEM Forms may not immediately recognize the certificate. To resolve this, restart the Application Server before you configure the HSM credential alias.

1. Open the administrative console of AEM Forms in a web browser at `http://localhost:8080/adminui`.
2. Select **Settings**.



3. Select **Trust Store Management**.

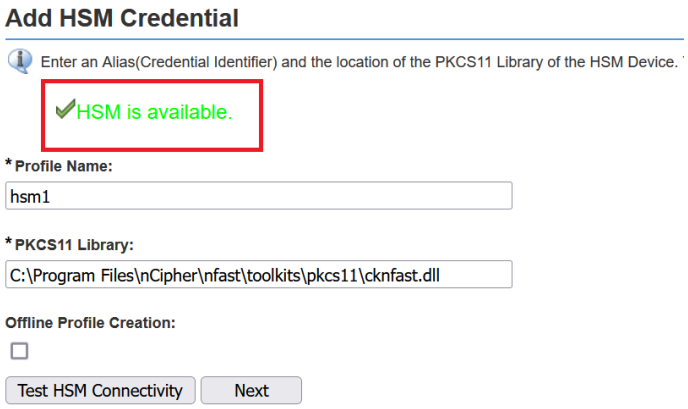


4. Select **HSM Credentials**.
5. Enter a **Profile Name** for the HSM.
6. Enter the path of the pkcs11 library:

```
C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll
```

7. Select **Test HSM Connectivity**.

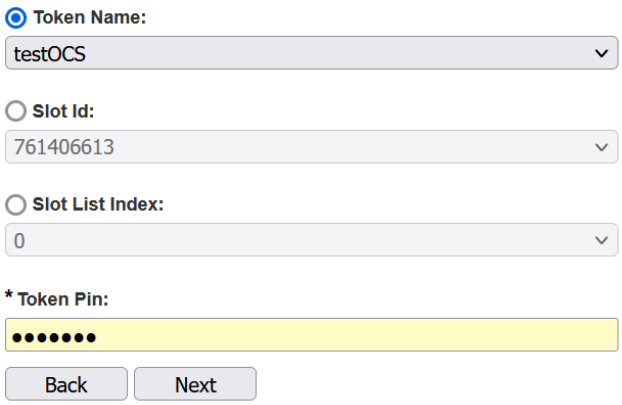
   A success message **HSM is available** appears. For example:



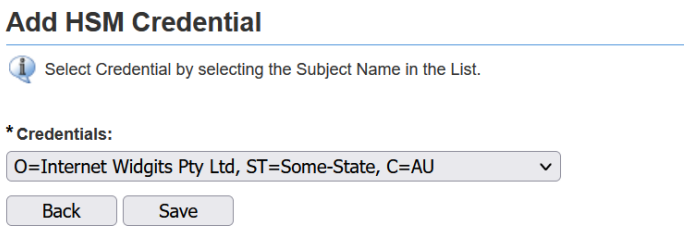
8. For the **Token Name**, select the accelerator for module protection or the card

set name for OCS/Softcard protection.

9. The corresponding **Slot ID** and **Slot List Index** values will be selected automatically.
10. For the **Token Pin**, enter the administrator card passphrase if you are using module protection. If you are using OCS cards or Softcard protection, enter their passphrase. For example:

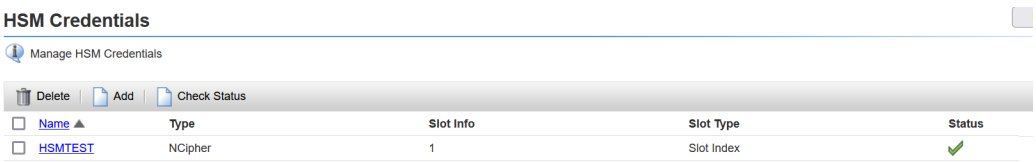


11. Select **Next**.
12. Select the HSM's **Credentials**. This will be the same as the certificate that was made in Generate a signed certificate on the HSM. For example:



13. Select **Save**.
14. Test this credential by selecting the check box next to it and selecting **Check Status**.

    A green check mark appears. For example:



Chapter 4. Additional resources and related products

4.1. nShield Connect

4.2. nShield as a Service

4.3. Entrust products

4.4. nShield product documentation