gemalto
a Thales company

Adobe Experience Manager Forms

INTEGRATION GUIDE

SAFENET LUNA HSM

Document Information	
Document Part Number	007-011210-001
Release Date	May 2019

Revision History

Revision	Date	Reason
D	May 2019	Update

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE

This document guides administrators through the steps for using a SafeNet Luna HSM with Adobe Experience Manager Forms.

Scope

This document outlines the steps to integrate Adobe Experience Manager Forms with a SafeNet Luna HSM to secure credentials for Digital Signatures.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

> **NOTE:** Take note. Notes contain important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

> **CAUTION!** Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury**

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: > Command-line commands and options (Type **dir /p**.) > Button names (Click **Save As**.) > Check box and radio button names (Select the **Print Duplex** check box.) > Window titles (On the **Protect Document** window, click **Yes**.) > Field names (**User Name:** Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) > User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a | b | c] [<a> | <b> | <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

{ a | b | c }
{ <a> | <b> | <c> }
	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1: Introduction

Adobe Experience Manager (AEM) provides an easy-to-use solution to create, manage, publish, and update complex digital forms while integrating with back-end processes, business rules, and data. AEM Forms combine form authoring, management, and publishing along with correspondence management capabilities, document security, and integrated analytics to create engaging end-to-end experiences. AEM Forms integrate with the SafeNet Luna HSM by using HSM stored credentials to apply server-side Digital Signatures.

The benefits of using an HSM with Adobe Experience Manager Forms include:

> Secure generation, storage, and protection of the private keys on FIPS 140-2 level 3 validated hardware.

> Full life cycle management of the keys.

> Access to the HSM audit trail.

Supported Platforms

SafeNet Luna HSM: It is a standalone network-attached appliance that physically and logically secure cryptographic keys and cryptographic processing. The purpose of an HSM is to protect sensitive data from being stolen by providing a highly secure operation structure. HSMs are fully contained and complete solutions for cryptographic processing, key generation, and key storage.

This integration is verified with SafeNet Luna HSM on the following operating systems:

> Windows 2016 Server

Prerequisites

Before you proceed with the integration, configure the SafeNet Luna HSM and install Adobe Experience Manager Forms.

Configure SafeNet Luna HSM

Before you get started ensure the following:

1. Ensure the HSM is setup, initialized, provisioned and ready for deployment.
2. Create a partition on the HSM that will be later used by Adobe Experience Manager Forms.
3. If using a SafeNet Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.

> **NOTE:** Adobe Experience Manager Forms use 32-bit Java. Ensure you configure the 32-bit Luna HSM client for integration.

4. Ensure that the partition is successfully registered and configured. The command to see the registered partition is:

    ```
    C:\Program Files\SafeNet\LunaClient\win32>lunacm.exe
    lunacm.exe (32-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

    Available HSMs:

    Slot Id ->              0
    Label ->                AdobeEM
    Serial Number ->        1280780175907
    Model ->                LunaSA 7.3.0
    Firmware Version ->     7.3.0
    Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
    Slot Description ->     Net Token Slot

    Current Slot Id: 0
    ```

    > **NOTE:** Follow the *SafeNet Network Luna HSM Product Documentation* for detailed steps on creating the NTLS connection, initializing the partition, and initializing the various user roles.

Using SafeNet HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the SafeNet HSM in FIPS mode, you have to make the following change to the configuration file:

```
Misc {

RSAKeyGenMechRemap = 1;

}
```

This setting redirects the older calling mechanism to a new approved mechanism when SafeNet HSM is in FIPS mode.

SafeNet Luna HSM HA (High-Availability) Setup

Refer to the *SafeNet Luna HSM Product Documentation* for steps and details regarding configuring and setting up two or more HSM boxes on host systems.

You must enable the HAOnly setting in HA for failover to work.

Setup Adobe Experience Manager Forms

Install Adobe Experience Manager Forms on the target machine. Refer to the *Adobe Documentation* for detailed installation instructions.

CHAPTER 2: Integrating Adobe Experience Manager Forms with a SafeNet Luna HSM

To integrate Adobe Experience Manager (AEM) Forms with the SafeNet Luna HSM to generate the credentials for Digital Signing, complete the following:

> Creating Credentials on the HSM

> Configuring the java.security file

> Configuring Adobe Experience Manager Forms

Creating Credentials on the HSM

Create a certificate and Certificate Signing Request (CSR) for each HSM credential that Digital Signatures requires. Submit the CSR to a certificate authority and then add the signed certificate to the HSM.

To create credentials on the HSM

1. Create a certificate request using CMU utility provided with HSM client.

```
# cmu generatekeypair -modulusBits=2048 -publicExp=65537 -sign=1 -verify=1 -
labelPublic="Public Verify Key" -labelPrivate="Private Verify Key" -id=101000
```

2. Determine the key handles for the public and private keys.

```
# cmu list
```

3. Generate a PKCS#11 request based on the public and private keys.

```
# cmu requestcertificate -slot=1
```

   Fill out the parameters, including the public and private key handles, it will create a Certificate Signing Request file.

4. Submit the Certificate Signing Request to a Certificate Authority and obtain the signed certificate.

5. Import the signed certificate into the HSM.

```
# cmu import -label=”HSM Credential”
```

   Specify the name of the certificate to be imported when prompted

6. Determine the key handles for the certificate.

```
# cmu list
```

7. Add an ID to the new certificate:

```
# cmu setAttribute -handle=x -id=101000
```

   where x is the handle of the certificate on the HSM

Configuring the java.security file

Configure AEM Forms for use with the SafeNet Luna HSM. Update the **java.security** files and copy the SafeNet Luna cryptographic libraries to the AEM Forms utility.

To configure the java.security file

1. Edit the Java Security Configuration file java.security located in the directory **<Adobe_Experience_Manager_Forms_InstallationDirectory>Java\32bit\jdk1.8.0_74\jre\lib\security**

   Add the Luna Provider to the **java.security** file as shown below:

   ```
   security.provider.1=sun.security.provider.Sun
   security.provider.2=sun.security.rsa.SunRsaSign
   security.provider.3=sun.security.ec.SunEC
   security.provider.4=com.sun.net.ssl.internal.ssl.Provider
   security.provider.5=com.sun.crypto.provider.SunJCE
   security.provider.6=sun.security.jgss.SunProvider
   security.provider.7=com.sun.security.sasl.Provider
   security.provider.8=org.jcp.xml.dsig.internal.dom.XMLDSigRI
   security.provider.9=sun.security.smartcardio.SunPCSC
   security.provider.10=sun.security.mscapi.SunMSCAPI
   security.provider.11=com.safenetinc.luna.provider.LunaProvider
   ```

   Save the changes to the **java.security** file.

2. Copy the **LunaAPI.dll** from the **<HSMClient_InstallationDirectory>\win32\JSP** folder and **LunaProvider.jar** file from the **<HSMClient_InstallationDirectory>\JSP\lib** folder to **<Adobe_Experience_Manager_Forms_InstallationDirectory>Java\32bit\jdk1.8.0_74\jre\lib\ext**.

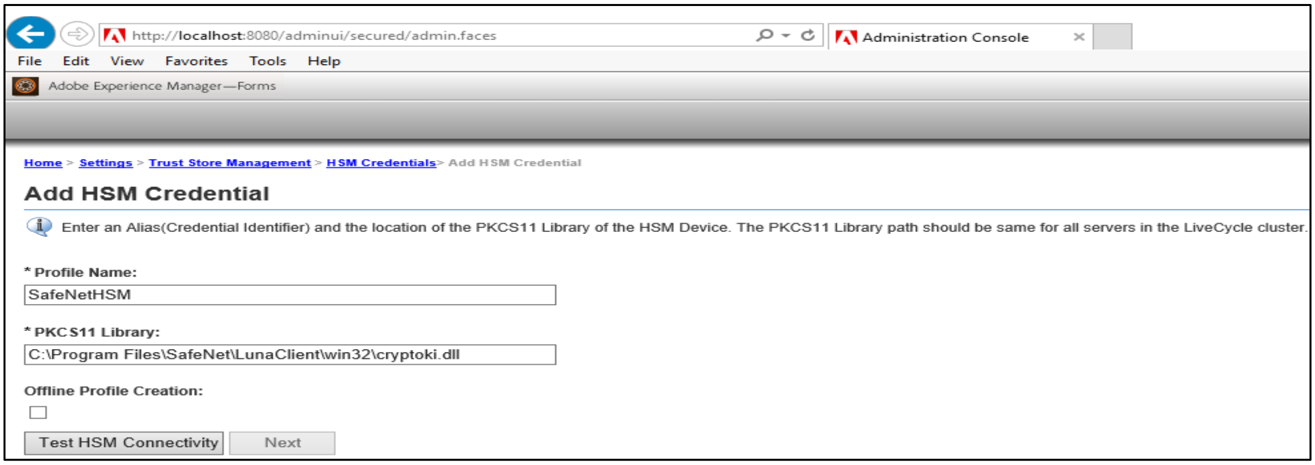
Configure Adobe Experience Manager Forms

Access AEM Forms and add an alias that uses the HSM security library credentials.

To create an alias for an HSM credential

1. Browse `http://localhost:8080/adminui` to access the Administrative console.
2. Click **Settings → Trust Store Management → HSM Credentials**.
3. Click **Add**.
4. In the **Profile Name** field, type a string used to identify the alias. This value is used as a property of Digital Signatures operations.

5. In the **PKCS11 Library** field, enter the path of 32bit HSM client library **cryptoki.dll** on the server.


http://localhost:8080/adminui/secured/admin.faces
Administration Console
File Edit View Favorites Tools Help
Adobe Experience Manager—Forms

Home > Settings > Trust Store Management > HSM Credentials> Add HSM Credential

Add HSM Credential

Enter an Alias(Credential Identifier) and the location of the PKCS11 Library of the HSM Device. The PKCS11 Library path should be same for all servers in the LiveCycle cluster.

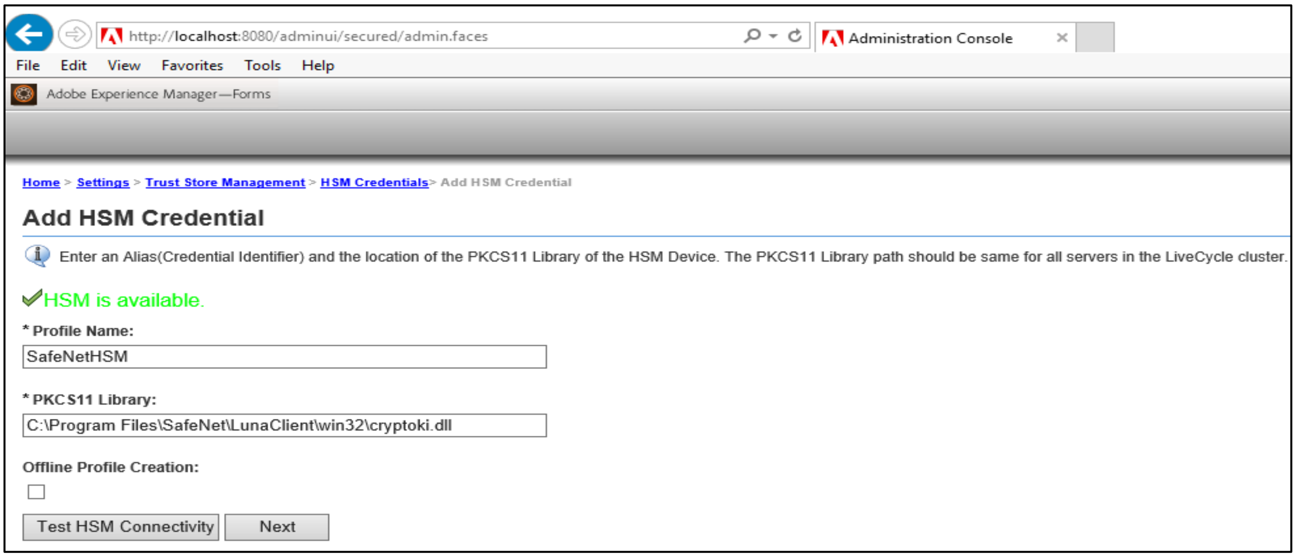
* Profile Name: SafeNetHSM

* PKCS11 Library: C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll

Offline Profile Creation: □

6. Click **Test HSM Connectivity**.

   If AEM Forms is able to connect to the HSM, a message displays stating that the HSM is available.


http://localhost:8080/adminui/secured/admin.faces
Administration Console
File Edit View Favorites Tools Help
Adobe Experience Manager—Forms

Home > Settings > Trust Store Management > HSM Credentials> Add HSM Credential

Add HSM Credential

Enter an Alias(Credential Identifier) and the location of the PKCS11 Library of the HSM Device. The PKCS11 Library path should be same for all servers in the LiveCycle cluster.

✓HSM is available.

* Profile Name: SafeNetHSM

* PKCS11 Library: C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll

Offline Profile Creation: □

7. Click **Next.**

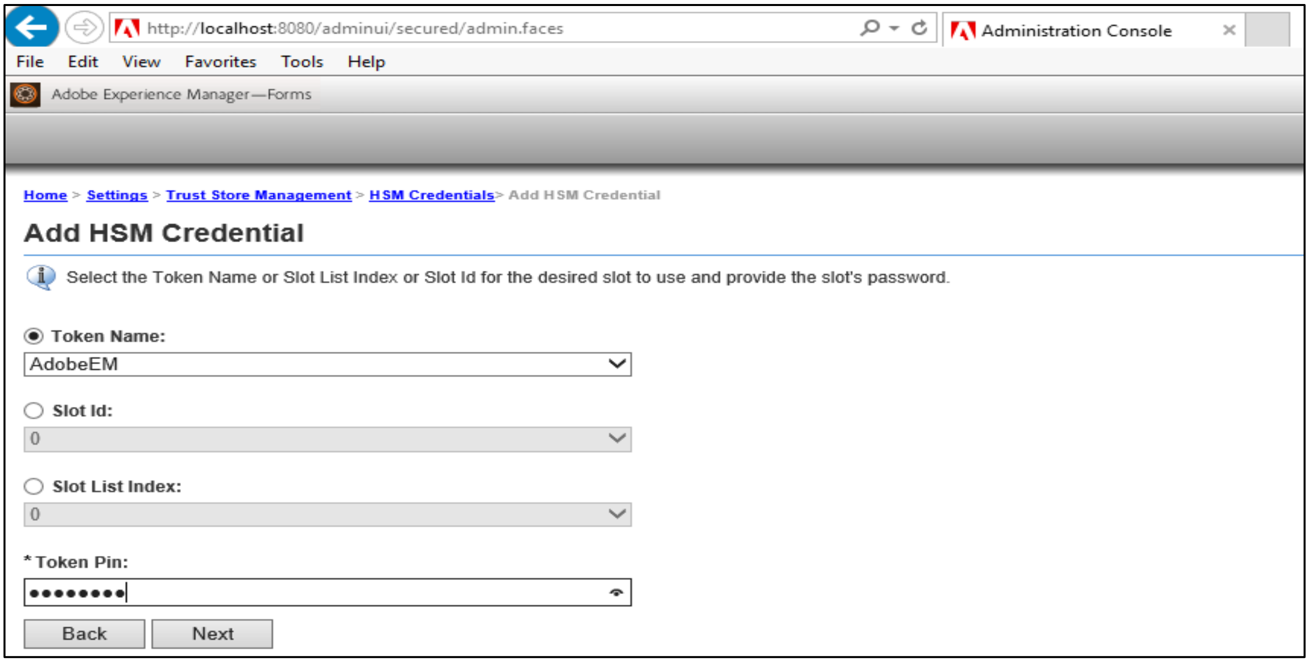
8. Use either the **Token Name**, **Slot ID**, or **Slot List Index** to identify where the credentials are stored on the HSM where:

   Token Name corresponds to the name of the HSM partition to be used.

   Slot ID is a slot identifier of type data type long.

   Slot List Index is a 0-based index. Set the Slot List Index to an integer that corresponds to the slot.

9. In the **Token Pin** field, type the partition password required to access the HSM key.


http://localhost:8080/adminui/secured/admin.faces
Administration Console
File
Edit
View
Favorites
Tools
Help
Adobe Experience Manager—Forms
Back
Next

Home > Settings > Trust Store Management > HSM Credentials> Add HSM Credential

Add HSM Credential

Select the Token Name or Slot List Index or Slot Id for the desired slot to use and provide the slot's password.

● Token Name: AdobeEM

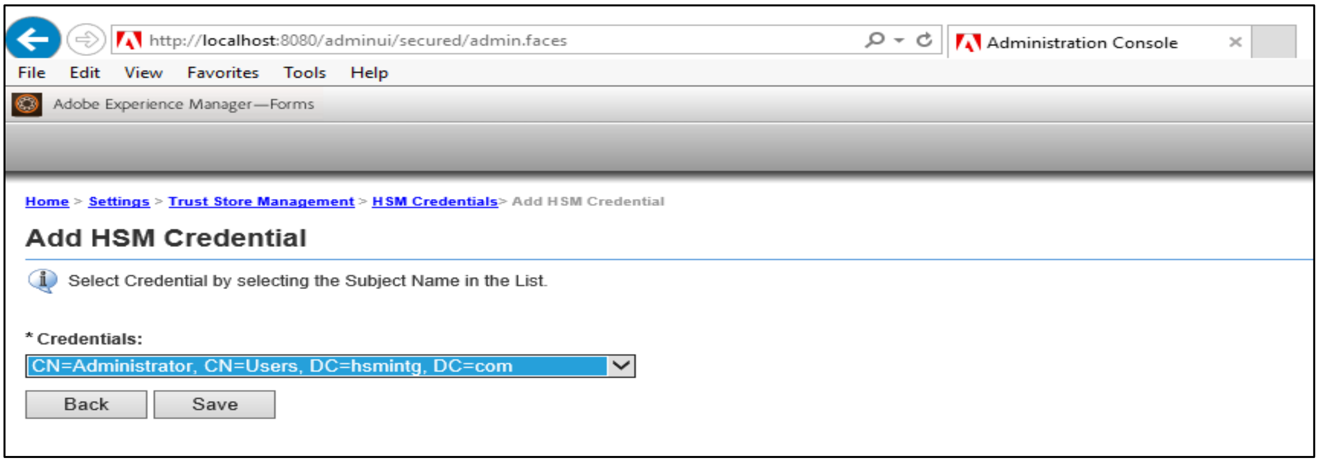
○ Slot Id: 0

○ Slot List Index: 0

* Token Pin: ●●●●●●●●

10. Click **Next**.

11. In the **Credentials** drop-down, select the credentials.


http://localhost:8080/adminui/secured/admin.faces
Administration Console
File
Edit
View
Favorites
Tools
Help
Adobe Experience Manager—Forms
Back
Save

Home > Settings > Trust Store Management > HSM Credentials> Add HSM Credential

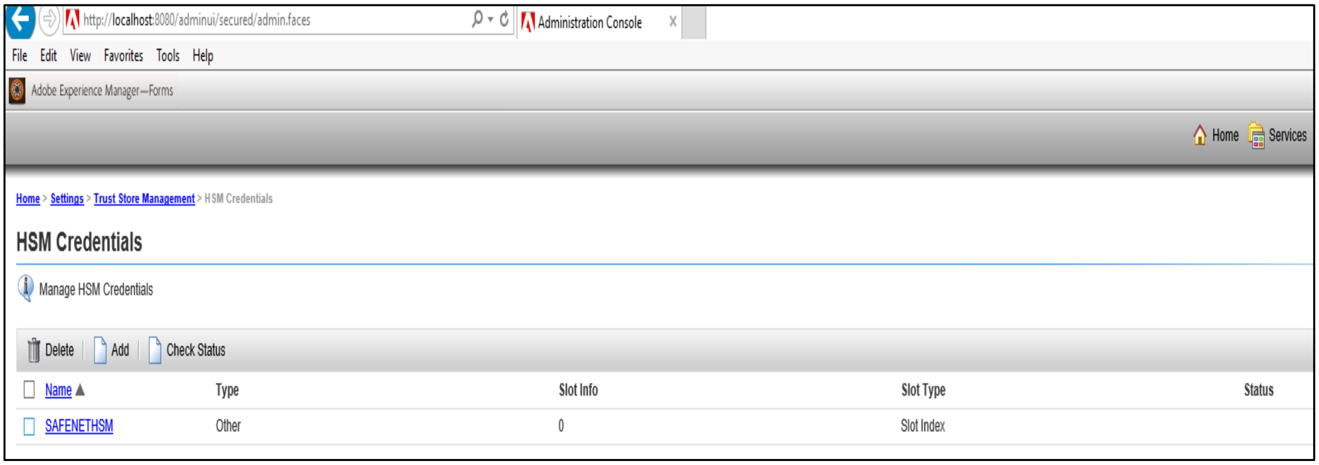
Add HSM Credential

Select Credential by selecting the Subject Name in the List.

* Credentials: CN=Administrator, CN=Users, DC=hsmintg, DC=com

12. Click **Save**.

    HSM Credentials generate in Trust Store Management.

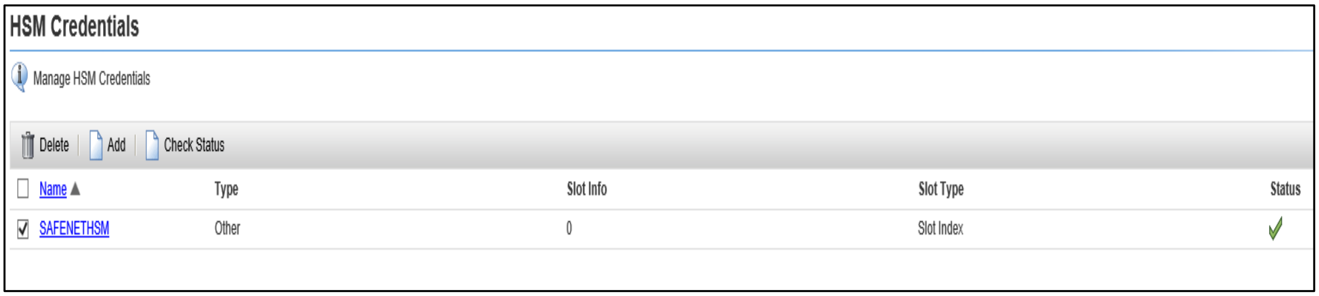

http://localhost:8080/adminui/secured/admin.faces
Administration Console
File Edit View Favorites Tools Help
Adobe Experience Manager—Forms
Home
Services
Home > Settings > Trust Store Management > HSM Credentials
HSM Credentials
Manage HSM Credentials
Delete
Add
Check Status

	Name ▲	Type	Slot Info	Slot Type	Status
□	SAFENETHSM	Other	0	Slot Index	

To check the status of an HSM credential

1. Browse http://localhost:8080/adminui to access the Administrative console.
2. Click **Settings → Trust Store Management → HSM Credentials**.
3. Select the Check box next to credential that you want to check.
4. Click **Check Status**.

    The Status column reflects the current status of the credential. A green tick will ensure the HSM availability.



	Name ▲	Type	Slot Info	Slot Type	Status
☑	SAFENETHSM	Other	0	Slot Index	✓

This completes the integration of Adobe Experience Manager Forms with SafeNet Luna HSM securing credentials on HSM partition.