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.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Part Number:** 007-012087-001, Rev. E

**Release Date:** March 2016
Contents

Preface .................................................................................................................................................. 5
Scope ................................................................................................................................................ 5
Document Conventions ...................................................................................................................... 5
Command Syntax and Typeface Conventions ................................................................................... 6

1 Introduction .................................................................................................................................... 7
Overview.......................................................................................................................................... 7
Understanding the Active Directory Federation Services ............................................................ 7
  3rd Party Application Details ......................................................................................................... 8
Supported Platforms ......................................................................................................................... 8
  Windows Server 2008 R2 ............................................................................................................. 8
  Windows Server 2012 R2 ............................................................................................................. 8
Prerequisites .................................................................................................................................... 9
  SafeNet Network HSM Setup ...................................................................................................... 9
  Microsoft ADFS Setup ................................................................................................................ 9

2 Integrating Microsoft Active Directory Federation Services ................................................... 10
Configuring Active Directory Certificate Services with SafeNet Luna HSM ................................... 10
  Configuring SafeNet Luna HSM Key Storage Provider ............................................................... 10
  Installing Microsoft Active Directory Certificate Services on Windows Server 2008 R2 Enterprise Full using SafeNet Luna Key Storage Provider ......................................................................................................................... 16
  Configuring the CA to issue ADFS Web Server Certificates ...................................................... 30
SafeNet Luna HSM for Active Directory Federation Services .......................................................... 32
  Register CSP .............................................................................................................................. 32
Generate Token Signing Certificate to use with Active Directory Federation Services ................... 33
  Create a Token Signing/Decrypting Certificate using Luna CSP ................................................ 33
  Setting permission for Private Key of Certificate ......................................................................... 34
Configure ADFS to use SafeNet Luna HSM ...................................................................................... 34
  Install AD FS 2.0 and apply the patch for HSM support ............................................................... 34
  Create and configure a server authentication certificate in IIS .................................................... 34
  Configure the system as a federation server .............................................................................. 35
  Install the token signing/decrypting certificate generated by Luna CSP ...................................... 35

3 Install and Configure WIF and Sample Application ................................................................ 37
Install and configure WIF SDK ....................................................................................................... 37
Create the WIF Sample Application ............................................................................................ 37
Create and configure the WifSamples application pool ................................................................. 38
Configure the WIF sample application to trust incoming claims .................................................. 38
Configure AD FS 2.0 to send claims to the application ................................................................. 38
Configure the claim rule for the sample application .................................................................... 39
Test the access to sample application ........................................................................................... 39

4 Integrating Microsoft Active Directory Federation Services 3.0 with SafeNet Luna HSM40
Configuring Active Directory Certificate Services with SafeNet Luna HSM .................................. 40
SafeNet Luna HSM for Active Directory Federation Services ......................................................... 41
Contents

Register CSP ................................................................................................................................................ 41
Generating the Token Signing Certificate to use with Active Directory Federation Services (ADFS)........... 42
Configure ADFS to use SafeNet Luna HSM .................................................................................................. 43

5  Configure Multiple ADFS Instances Using Same Key Pair on HSM................................................. 48
Setting up Two Instances of ADFS Sharing Same Keys on HSM ................................................................. 48
   Microsoft ADFS Setup .................................................................................................................................. 48
   SafeNet Luna HSM Setup ................................................................................................................................ 48
Setting up SafeNet Luna HSM for Active Directory Federation Services ...................................................... 49
   Register CSP ................................................................................................................................................ 49
Generate Token Signing Certificate to use with ADFS1 ..................................................................................... 49
   Create a Token Signing/Decrypting Certificate using Luna CSP ................................................................. 49
Create Token Signing Certificate to use with ADFS2 ..................................................................................... 51
   Export the existing Token Signing certificate from ADFS1 ....................................................................... 51
Import the ADFS1 Token Signing certificate to ADFS2 .................................................................................. 52
This document guides security administrators on obtaining the necessary information to install, configure, and integrate Microsoft ADFS with SafeNet Luna HSM. This document outlines the steps to integrate Microsoft ADFS with SafeNet Luna HSM.

Scope

This guide provides instructions for setting up a small test lab with Active Directory Federation Services (ADFS) 2.0 with Windows Identity Foundation (WIF) on a server running the Windows Server 2008 R2 operating system and using SafeNet Luna HSM for securing the Token Signing/Decrypting certificate private keys. It explains how to install and configure software that is required for setting up a federation server (running ADFS 2.0 software) and a Web server (running WIF software) while storing certificate keys on SafeNet Luna HSM.

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. Contains 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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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.) |
| **Consolas** | Denotes syntax, prompts, and code examples. |
Introduction

Overview

SafeNet Luna HSM integrates with Microsoft ADFS to provide significant performance improvements by off-loading cryptographic operations from the ADFS Server to the SafeNet Luna HSM. In addition, SafeNet Luna HSM provides extra security by protecting and managing the server’s high value SSL private key within a FIPS 140-2 certified hardware security module.

Active Directory Federation Services (ADFS) is a software component developed by Microsoft that can be installed on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and implement federated identity.

Claims-based authentication is the process of authenticating a user based on a set of claims about its identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means, and that is trusted by the entity doing the claims based authentication.

In ADFS, identity federation is established between two organizations by establishing trust between two security realms. A federation server on one side (the Accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity. On the other side, the Resources side, another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords.

Understanding the Active Directory Federation Services

Active Directory Federation Services (ADFS) is a software component developed by Microsoft that can be installed on Windows Server operating systems to provide users with Single Sign-On access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and implement federated identity.

Claims based authentication is the process of authenticating a user based on a set of claims about its identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means, and that is trusted by the entity doing the claims based authentication.

In ADFS, identity federation is established between two organizations by establishing trust between two security realms. A federation server on one side (the Accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity. On the other side, the Resources side, another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide
controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords.

3rd Party Application Details

- Microsoft Active Directory Federation Services (ADFS2.0)
- Microsoft Active Directory Federation Services (ADFS3.0)
- WindowsIdentityFoundation-SDK-3.5.msi

Supported Platforms

Windows Server 2008 R2

<table>
<thead>
<tr>
<th>Third Party Application</th>
<th>Luna Client Software Version</th>
<th>SafeNet Luna HSM Appliance Software &amp; Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft ADFS 2.0 with patch KB2790338 – Update Rollup 3</td>
<td>Luna Client v6.1.0-5</td>
<td>Luna SA v6.2 F/w 6.24.0</td>
</tr>
<tr>
<td>Microsoft ADFS 2.0 with patch KB2790338 – Update Rollup 3</td>
<td>Luna Client v5.3.0</td>
<td>Luna SA v5.3 F/w 6.10.1</td>
</tr>
<tr>
<td>Microsoft ADFS 2.0 with patch KB2607496 – Update Rollup 1</td>
<td>Luna Client v5.0</td>
<td>Luna SA v5.0 F/w 6.0.8</td>
</tr>
</tbody>
</table>

Windows Server 2012 R2

<table>
<thead>
<tr>
<th>Third Party Application</th>
<th>Luna Client Software Version</th>
<th>SafeNet Luna HSM Appliance Software &amp; Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft ADFS 3.0</td>
<td>Luna Client v5.4.1</td>
<td>Luna SA v5.4.7 (F/w 6.2.1)</td>
</tr>
</tbody>
</table>
Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started, ensure the following:

1. SafeNet Network HSM appliance and a secure admin password
2. SafeNet Network HSM, and a hostname, suitable for your network
3. SafeNet Network HSM network parameters are set to work with your network
4. Initialize SafeNet Network HSM.
5. Create and exchange certificates between SafeNet Network HSM and Client system.
6. Create a partition on SafeNet Network HSM. Remember the partition password that will be later used by Microsoft ADFS. Register the client with the partition. Run the ”vtl verify” command on the client system to display a registered partition. The general form of command for Windows is C:\Program Files\SafeNet\LunaClient > vtl verify.
7. Enable partition policies 22 and 23: Activation and Auto Activation respectively.

Microsoft ADFS Setup

Microsoft ADFS must be installed on the target machine to continue with the integration process. The following setup is required to proceed with the integration process:

1. Windows Server 2008 R2 Enterprise Edition machine, which will become a Domain Controller and Certificate Authority.
3. Domain Administrator privileges.

The machines utilized are denoted in the setup as follows:


It is assumed that you have joined the ADFSWEB computer to the INTEGRATION domain.
Integrating Microsoft Active Directory Federation Services

Configuring Active Directory Certificate Services with SafeNet Luna HSM

Configuring SafeNet Luna HSM Key Storage Provider

1. KSP must be installed in a separate step following completion of the main SafeNet Luna HSM Client software installation.
2. Traverse to the KSP installation directory.
3. Run KspConfig.exe (KSP configuration wizard).
4. Double-click **Register Or View Security Library** on the left side of the pane.
5. Browse the library cryptoki.dll from the SafeNet Luna HSM client installation directory and click **Register**.
6. On successful registration, a message ‘*Success registering the security library*’ displays.
7. Double-click **Register HSM Slots** on the left side of the pane.

![Safelinet Key Storage Provider, Config Wizard]

8. Enter slot (partition) password in the **Slot Password** field.
9. Click **Register Slot** to register the slot for Domain\User. On successful registration, a message *'The slot was successfully and securely registered'* displays.
10. You need to register the slot for NT AUTHORITY\SYSTEM.

Installing Microsoft Active Directory Certificate Services on Windows Server 2008 R2 Enterprise Full using SafeNet Luna Key Storage Provider

To install the Microsoft Active Directory Certificate Services software:

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Refer to the Before you install section at the beginning to configure SafeNet KSP.
3. Click Start, point to Administrative tools, and then click Server Manager. The Server Manager snap-in appears.
4. Select **Roles** in the console tree.

5. Right-click **Roles** and then click, **Add Roles**. The **Add Roles wizard** displays.

6. Click **Next**.
7. Select the **Active Directory Certificate Services** check box from **Server Roles** to install on this server.
8. Click **Next**.

9. Click **Next** to continue.
10. Select the **Certification Authority** check box from the **Role services** list to install **Active Directory Certificate Services**.

11. Click **Next** to continue.
12. Select the type of setup on the **Specify Setup Type** page.

13. Click **Next** to continue.
14. Select the type of CA on the **Specify CA Type** page.

15. Click **Next** to continue.
16. Proceed to setup the **Private Key** for CA to generate and issue certificates to clients. Select **Create a new private key**.

![Set Up Private Key](image)

17. Click **Next** to continue.
18. To create a new private key, you must select a cryptographic service provider and key length. Select algorithm for SafeNet Key Storage Provider from the select a cryptographic service provider (CSP) drop-down menu.

19. Select the Hash Algorithm for signing certificates issued by the Certificate Authority and key length settings for your installation.
20. Select the ‘Allow administrator interaction when the private key is accessed by the CA’ check box.

![Configure Cryptography for CA]

To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

- **Select a cryptographic service provider (CSP):**
  - ECDSA_P256
  - SafeNet Key Storage Provider

- **Key character length:**
  - 512

To select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1

21. Click **Next** to continue.
22. Configure a common name to identify this CA.

![Configure CA Name](image)

23. Click **Next** to continue.
24. Select the certificate validity period.

25. Click **Next** to continue.
26. Configure the **Certificate Database**. It records all certificate requests, issued certificates, and revoked or expired certificates.

27. Click **Next** to continue.

28. Proceed to confirm the installation selections.
29. Click **Install** to install the selected roles, role services, or features.
30. Click **Close** to exit the **Add Roles** wizard after viewing the installation results.

![Add Roles Wizard](image)

A private key for the CA will be generated and stored on HSM.

31. Verify the CA service has been successfully started. To verify that service is running, run the following command on the command prompt:

```bash
sc query certsvc
```

32. Verify the CA key. Run the following command on the command prompt:

```bash
certutil –verifykeys
```

The result of the command shows the CA keys have successfully been verified.

### Configuring the CA to issue ADFS Web Server Certificates

Follow below steps to configure a CA to create a certificate template and issuing properties for ADFS server certificate.

#### Configuring certificate templates for your test environment

1. Log on to ADFSCA as a domain administrator.
2. From the **Start** menu, select **Run**. The **Run** dialog box displays.
3. Type `mmc` and click **OK**.
4. The MMC console displays. In this console, select **File > Add/Remove Snap-in...**
5. In the **Add or Remove Snap-Ins** dialog box, select the **Certificates Templates** snap-in under the **Available snap-ins** menu.

6. Click **Add**, and then click **OK**.

7. Under Console Root, expand the **Certificate Templates** snap-in. Listed in the middle section will be all the available certificate templates that you can make your CA issue.

8. Scroll down the list until you locate the **Web Server** template, right-click and click **Duplicate Template**.

9. Select **Windows Server 2003 Enterprise** and click **OK**.

10. A pop-up dialog box displays. Click the **General** tab.

11. Enter the **Template Display Name** for example ADFS.

12. Click the **Request Handling** tab.

13. Click on **CSPs** and select **Request can use any CSP available on subject’s computer**.

14. Click **OK** to close the window.

15. Click the **Security** tab and click **Add**.

16. Type **NETWORK SERVICE** and click **OK**.

17. Click **NETWORK SERVICE** in the **Group or user names** area.

18. In the **Permissions** area, Ensure that the **Read** and **Enroll** check boxes are ticked.

19. Add and provide the Read and Enroll permissions to the following members:
   - Domain Computers
   - Domain Controllers
   - NETWORK SERVICE
   - IIS_IUSRS

20. For **Domain Admins** and **Enterprise Admins**, ensure that the **Read**, **Write**, and **Enroll** check boxes are ticked.

21. Click **Apply** and then **OK**.

**Configuring the CA to support the ADFS certificate template**

1. Log on to ADFSCA as a domain administrator.

2. From the **Start** menu select **Control Panel > Administrative Tools > Certification Authority**.

3. In the console tree (left-hand section), expand the CA (It has a computer icon and a green tick next to it).

4. In console tree of the Certification Authority snap-in, right-click **Certificate Templates**, and then click **New Certificate Templates to Issue**.

5. In **Enable Certificates Templates**, select the **ADFS** template and any other certificate templates you configured previously, and then click **OK**.

6. Open **Certificate Templates** in the **Certification Authority** and verify that the modified certificate templates appear in the list.
SafeNet Luna HSM for Active Directory Federation Services

To set up SafeNet Luna HSM for Active Directory Federation Services, perform the following steps:

Register CSP

1. CSP must be installed on the Federation Services (ADFSWEB).

   **NOTE:** For Luna Client s/w v5.0, execute 630-010268-001_Alpha2.exe. It will create a zip file, extract the zip file and copy the contents of 630-010268-001_Alpha2 into the C:\Program Files\LunaSA\CSP.

2. Open the command prompt and navigate to <SafeNet Luna HSM installation directory>\CSP.

3. Run the register.exe and provide the SafeNet Luna HSM partition password to register the partition with CSP.

```
C:\Program Files\LunaSA\CSP>register.exe
register v1.0.0-alpha

Safenet Inc. LunaCSP, Partition Registration

* Protect the HSM's challenge for the selected partitions.
* This is a WEAK protection of the challenge!!
* After you have configured all applications that will use
  the LunaCSP, and run them once, you MUST run:
  register /partition /strongprotect
  to strongly protect the registered challenges!!

This procedure is a destructive procedure and will completely replace any previous settings!
Do you wish to continue? [y/n] y
Do you want to register the partition named 'part6'? [y/n]: y
Enter challenge for partition 'part6': ********
Success registering the ENCRYPTED challenge for partition 'part6:1'.
Only the LunaCSP will be able to use this data!
Registered 1 partition(s) for use by the LunaCSP
```

G:\Program Files\LunaSA\CSP>
4. Now execute the following command:

```
C:\Program Files\LunaSA\CSP>register.exe /l
```

Generate Token Signing Certificate to use with Active Directory Federation Services

Create a Token Signing/Decrypting Certificate using Luna CSP

1. Log on to ADFSWEB as a domain administrator.
2. From the Start menu, select Run.
3. In the Run dialog box, type mmc and click OK.
4. The mmc console displays. Select File > Add/Remove Snap-in...
5. In the Add or Remove Snap-Ins dialog box, find the Certificates snap-in (under the Available snap-ins section) and select it.
6. Click Add, Select Computer Account and Click Next.
7. Select Local Computer, and click Finish.
8. Click OK and expand the Certificates under Console Root.
9. Right-click on the Personal folder and select All Tasks -> Request New Certificate...
10. Click Next, Select Active Directory Enrollment Policy and then click Next. It will display the certificate template you have configured, i.e. ADFS
11. Click on More information is required to enroll for this certificate. Click here for configure settings link.
13. Select Common Name under Subject Name and provide the fully qualified domain name for the computer on which you are installing the certificate in the Value field and click Add. Repeat the same step for adding more values.
14. Click the General tab and provide the Friendly Name. For example: ADFS Token Signing.
15. Click the Private Key tab, and verify that Luna enhanced RSA and AES provider for Microsoft Windows must be selected under the Cryptographic Service Provider.
16. Click the Certificate Authority tab, and ensure that Enterprise Root CA is selected.
17. Click Apply and then OK.
18. Select ADFS certificate template or the certificate template you have configured, and click Enroll.
19. It will take some time to enroll, when enrollment succeeded, click Finish.
Setting permission for Private Key of Certificate

1. Open the certificate snap under the console root, Certificates (Local Computer) > Personal > Certificate.
2. Right-click on the certificate generated by Luna CSP and select All Tasks > Manage Private Keys.
3. Click Add, type Administrator in the Enter the object name to select text box.
4. Click OK. Ensure that Domain Administrator is added in the Group or User Name list.
5. Select the domain administrator and select the Full Permission check box.
6. Click Apply and then OK to close the window.

Configure ADFS to use SafeNet Luna HSM

Install AD FS 2.0 and apply the patch for HSM support

To use AD FS 2.0 in conjunction with SafeNet Luna HSM, the AD FS 2.0 must be updated with the patch mentioned in supported platform table so that HSM can be used to protect the ADFS server certificate keys.

1. Log on to ADFSWEB as a domain administrator.
2. Locate the AdfsSetup.exe installation package that you downloaded, and then double-click it.
3. On the Welcome to the AD FS 2.0 Setup Wizard page, click Next.
4. On the End-User License Agreement page, read the license term. If you agree to the terms, select the I accept the terms in the License Agreement check box, and then click Next.
5. On the Server Role page, click Federation Server and click Next.
6. On the Completed the Microsoft AD FS 2.0 Setup Wizard page, uncheck the Start the AD FS 2.0 Management snap-in when this wizard closes check box and then click Finish.
7. Double-click the Windows6.1-KB2607496-v3-x64.msu (Update rollup 1) or Windows6.1-KB2790338-v2-x64 (Update rollup 3) and follow the corresponding steps to install it.
8. After the installation is completed, restart the server.

Create and configure a server authentication certificate in IIS

1. Log on to ADFSWEB as a domain administrator.
2. From the Start menu, select All Programs > Administrative Tools > Internet Information Services (IIS) Manager.
3. In the console tree, click the root node that contains the name of the computer, and then, in the details pane, double-click the icon named Server Certificates in the IIS grouping.
4. In the Actions pane, click Create Certificate Request.
5. Enter the details in the Create Certificate window.
6. Common Name must be fully qualified domain name.
7. After providing all the details, Click Next.
8. Select Microsoft RSA SChannel Cryptographic Provider and 2048 as Bit Length.
9. Click Next, select the location to save the certificate request as C:request.txt.
10. Click **Finish**, it will generate the certificate request. Submit certificate request to CA and save the signed certificate.

11. In the IIS **Action** pane, click **Complete Certificate Request**.

12. Browse and select the CA signed certificate and enter the **Friendly Name** as ADFS Server Certificate.

13. Click **OK** to complete the certificate request and close the window.

14. In the console tree, click the root node that contains the name of the computer, click **Default** website.

15. In the **Actions** pane, click **Bindings**.

16. In the **Site Bindings** dialog box, click **Add**.

17. In the **Add Site Binding** dialog box, select **https** in the **Type** drop-down list, select the certificate that you have generated through IIS in the SSL certificate drop-down list, click **OK**, and then click **Close**.

18. Close the Internet Information Services (IIS) Manager console.

### Configure the system as a federation server

1. Log on to ADFSWEB as a domain administrator.

2. From the **Start** menu, select **All Programs > Administrative Tools > AD FS 2.0 Management**.

3. Click the **AD FS 2.0 Federation Server Configuration Wizard** in the **Actions** pane.

4. On the **Welcome** page, click **Create a new Federation Service**, and then click **Next**.

5. On the **Select Stand-Alone or Farm Deployment** page, click **Stand-alone federation server**, and then click **Next**.

6. On the **Specify the Federation Service Name** page, verify that the ADFS Server Certificate is selected that you have bind with IIS, and then click **Next**.

7. On the **Ready to Apply Settings** page, review the settings, and then click **Next**.

8. On the **Configuration Results** page, when completed, click **Close**.

9. Leave the AD FS 2.0 Management console open, and then proceed to the next step.

### Install the token signing/decrypting certificate generated by Luna CSP

1. From the **Start** menu, select **All Programs > Administrative Tools > Windows PowerShell Modules**.

2. Type `get-ADFSProperties` and press the Enter key. See that **AutoCertificateRollover** is set to be **True**.

3. Type `Set-ADFSProperties -AutoCertificateRollover $False` and press the **Enter** key.

4. Type `get-ADFSProperties` and press the Enter key. Verify that **AutoCertificateRollover** is set to be **False**.

5. Close the **PowerShell** window.

6. Open the **AD FS 2.0 Management**.

7. Expand the **Service** and click **Certificates**.

8. In the **Actions** pane, click **Add Token-Signing Certificate**.

9. Select the ADFS Token Signing certificate that you have generated using Luna CSP.

10. Click **OK**. It will add the certificate in the Certificate pane.

11. Right-click on the certificate and select **Set as Primary**.
12. A confirmation message will pop up. Click Yes.
13. Delete the other certificate, i.e., ADFS Signing Secondary Certificate.
14. In the Actions pane, click on Add Token-Decrypting Certificate.
15. Select the ADFS Token Signing certificate that you have generated using Luna CSP.
16. Click OK. It will add the certificate in the Certificate pane.
17. Right-click on the certificate and select Set as Primary.
18. A confirmation message will pop up. Click Yes.
19. Delete the other certificate, i.e., ADFS Signing Secondary Certificate.
20. Open the command prompt and run the following commands to stop and start the ADFS 2.0 service.
   ```
   Net stop adfssrv
   Net start adfssrv
   ```
21. Verify that the ADFS Service successfully started.
Install and Configure WIF and Sample Application

This chapter lists down the steps to install and configure WIF and a sample application (provided by the WIF SDK) to trust the claims that are issued by the federation server role that you created in the previous chapter. After this step is complete, the ADFSSRV computer is set up in both the federation server role and the claims-aware Web server role.

You can refer the following Microsoft Documentation for setting up Windows Identity Foundation SDK to verify the claim based application:


Install and configure WIF SDK

1. Locate the WindowsIdentityFoundation-SDK.msi installable package that you downloaded, and then double-click it.
2. On the Welcome to the Windows Identity Foundation SDK Setup Wizard page, click Next.
3. On the End-User License Agreement page, read the license terms. If you agree to the terms, select the I accept the terms in the License Agreement check box, and then click Next.
4. On the Destination Folder page, specify the desired installation folder, and then click Next.
5. On the Ready to install Windows Identity Foundation SDK page, click Install.
6. On the Completed the Windows Identity Foundation SDK Setup Wizard page, clear the Open Readme check box, and then click Finish.

Create the WIF Sample Application

1. Open Windows Explorer, and navigate to C:\Program Files\Windows Identity Foundation SDK\v3.5\Samples\Quick Start\Using Managed STS. If you are using a 64-bit version of Windows, change Program Files in this path to Program Files (x86).
2. Right-click setup.bat, and then click Run as administrator.
3. After the command-line script stops running, close the Command Prompt window.
Create and configure the WifSamples application pool

1. Open the Internet Information Services (IIS) Manager console.
2. In the root node under console tree that contains the name of the computer, right-click Application Pools, and then click Add Application Pool.
3. In the Add Application Pool dialog box, in Name type WifSamples, and then click OK.
4. In IIS Manager, in the center pane, right-click the newly created WifSamples application pool, and then click Advanced Settings.
5. In the Advanced Settings dialog box, in the Process Model section, change the value for Load User Profile to True, and then click OK.
6. Close the IIS Manager console.

Configure the WIF sample application to trust incoming claims

1. From the Start menu, select All Programs > Administrative Tools > Windows Identity Foundation Federation Utility.
2. On the Welcome page, click Browse and navigate to the C:\Program Files (x86)\Windows Identity Foundation SDK\v3.5\Samples\Quick Start\Using Managed STS\ClaimsAwareWebAppWithManagedSTS.
3. Select web.config file and click Open.
4. In Application URI, type https://<fully qualified domain name>/ClaimsAwareWebAppWithManagedSTS/ to indicate the path to the sample application that will trust the incoming claims from the federation server. Click Next.
   
   NOTE: Verify that the Uniform Resource Identifier (URI) starts with https and that it does not specify a port number. For example: https://ADFSWEB.integration.com/ClaimsAwareWebAppWithManagedSTS/

7. Click Select an existing certificate from store and then click Select Certificate.
8. Click and select ADFS Token Signing certificate generated by Luna CSP, click OK and then click Next.
9. On the Offered claims page, review the claims that will be offered by the federation server, and then click Next.
10. On the Summary page, review the changes that will be made to the sample application by the Federation Utility Wizard, and then click Finish.
11. A message You have successfully configured your application displays. Click OK.

Configure ADFS 2.0 to send claims to the application

1. In the AD FS 2.0 Management console, click AD FS 2.0, and then, in the details pane, click Required: Add a trusted relying party to start the Add Relying Party Wizard.
2. On the Welcome page, click Start.
3. On the **Select Data Source** page, click Import data about the relying party published online or on a local network, type https://<fully qualified domain name>/ClaimsAwareWebAppWithManagedSTS/, and then click **Next**. This action prompts the wizard to check for the metadata of the application that the Web server role hosts.

4. On the **Specify Display Name** page, in **Display name** type **WIF Sample App**, and then click **Next**.

5. On the **Choose Issuance Authorization Rules** page, click ** Permit all users to access this Relying Party**, and then click **Next**.

6. On the **Ready to Add Trust** page, review the relying party trust settings, and then click **Next** to save the configuration.

7. Click **Close** to exit. The **Edit Claim Rule** window displays.

**Configure the claim rule for the sample application**

1. On the **Edit Claim Rules for WIF Sample App properties** page, on the **Issuance Transform Rules** tab, click **Add Rule** to start the **Add Transform Claim Rule Wizard**.

2. On the **Select Rule Template** page, under **Claim rule template**, click and select **Pass Through or Filter an Incoming Claim**.

3. Click **Next**. This action passes an incoming claim through to the user by means of Windows Integrated Authentication.

4. On the **Configure Rule** page, in **Claim rule name** type **Pass through Windows Account Name Rule**.

5. In the **Incoming claim type** drop-down list, click **Windows account name**, and then click **Finish**.

6. Click **OK** to close the property page and save the changes to the relying party trust.

**Test the access to sample application**

1. Log on to the computer using the domain administrator account.

2. Open a browser window, and then go to https://<fully qualified domain name>/ClaimsAwareWebAppWithManagedSTS/default.aspx.

3. Enter the username and password for the domain administrator and click **OK**

4. This action automatically redirects the request to the federation server role and then back to the sample application with claims. Notice that the claims that AD FS 2.0 issues appear in the page.
Integrating Microsoft Active Directory Federation Services 3.0 with SafeNet Luna HSM

Configuring Active Directory Certificate Services with SafeNet Luna HSM

To set up SafeNet Luna HSM for Active Directory Certificate Services, kindly refer the Configuring SafeNet Luna HSM Key Storage Provider Section of chapter 2.

Configuring the CA to issue ADFS Web Server Certificates

Follow below steps to configure a CA to create a certificate template and issuing properties for ADFS server certificate.

Configuring certificate templates for your test environment

1. Log on to ADFSCA as a domain administrator.
2. From the Start menu, select Run. The Run dialog box displays.
3. Type mmc and click OK.
4. The MMC console displays. In this console, select File > Add/Remove Snap-in…
5. In the Add or Remove Snap-Ins dialog box, select the Certificates Templates snap-in under the Available snap-ins menu.
6. Click Add, and then click OK.
7. Under Console Root, expand the Certificate Templates snap-in. Listed in the middle section will be all the available certificate templates that you can make your CA issue.
8. Scroll down the list until you locate the Web Server template, right-click and click Duplicate Template.
10. In the pop-up dialog that appears click Yes and then click the General tab.
11. Enter the Template Display Name for example ADFSWEB.
12. Select Publish certificate in Active Directory.
13. Click the Cryptography tab.
14. Click on CSPs and select Request can use any CSP available on subject’s computer.
15. Click **OK** to close the window.
16. Click the **Security** tab and click **Add**.
17. Type **NETWORK SERVICE** and click **OK**.
18. Click on **NETWORK SERVICE** in the **Group or user names** area.
19. In the **Permissions** area, make sure that the **Read** and **Enroll** check boxes are ticked.
20. Add and provide the Read and Enroll permissions to the following:
   - Domain Computers
   - Domain Controllers
   - NETWORK SERVICE
   - IIS_IUSRS
21. For Administrator, **Domain Admins** and **Enterprise Admins**, make sure that **Read**, **Write**, and **Enroll** check boxes are ticked.
22. Click **Apply** and then **OK**.

### Configuring the CA to support the ADFS certificate template

1. Log on to ADFSCA as a domain administrator.
2. From the **Start** menu select **Control Panel > Administrative Tools > Certification Authority**.
3. In the console tree (left-hand section), expand the CA (It has a computer icon and a green tick next to it).
4. In console tree of the Certification Authority snap-in, right-click **Certificate Templates**, and then click **New Certificate Templates to Issue**.
5. In **Enable Certificates Templates**, select the **ADFSWEB** template and any other certificate templates you configured previously, and then click **OK**.
6. Open **Certificate Templates** in the **Certification Authority** and verify that the modified certificate templates appear in the list.

### SafeNet Luna HSM for Active Directory Federation Services

To set up Luna HSM for Active Directory Federation Services, perform the following:

#### Register CSP

1. CSP must be installed on the Federation Services (ADFSWEB) in a separate step following completion of the main Luna Client software installation.

   **NOTE**: For Luna Client s/w v5.0, execute 630-010268-001_Alpha2.exe. It will create a zip file, extract the zip file and copy the contents of 630-010268-001_Alpha2 into the C:\Program Files\LunaSA\CSP.

2. Open the command prompt and navigate to `<SafeNet Luna HSM installation directory>\CSP`. 
3. Run the register.exe and provide the SafeNet Luna HSM partition password to register the partition with CSP.

4. Now execute the following command:
   ```
   <SafeNet Luna HSM installation directory>CSP >register.exe /l
   ```

**Generating the Token Signing Certificate to use with Active Directory Federation Services (ADFS)**

**Create a Token Signing/Decrypting Certificate using Luna CSP**

1. Log on to ADFSWEB as a domain administrator.
2. From the **Start** menu, select **Run**.
3. In the **Run** dialog box, type **mmc** and click **OK**.
4. The **mmc** console displays. Select **File > Add/Remove Snap-in...**
5. In the **Add or Remove Snap-Ins** dialog box, find the **Certificates** snap-in (under the Available snap-ins section) and select it.
6. Click **Add**, Select **Computer Account** and Click **Next**.
7. Select **Local Computer**, and click **Finish**.
8. Click **OK** and expand the **Certificates** under **Console Root**.
9. Right-click on the **Personal** folder and select **All Tasks -> Request New Certificate...**
10. Click **Next**, Select **Active Directory Enrollment Policy** and then click **Next**. It will display the certificate template you have configured, i.e. ADFSWEB
11. Click on **More information is required to enroll for this certificate.** Click here for configure settings link.
12. The **Certificate Properties** window displays. Select the **Subject** tab.
13. Select **Common Name** under **Subject Name** and provide the fully qualified domain name for the computer on which you are installing the certificate in the **Value** field and click **Add**. Repeat the same step for adding more values.
14. Click the **General** tab and provide the **Friendly Name**. For example: ADFS Token Cert.
15. Click the **Private Key** tab, and verify that Luna enhanced RSA and AES provider for Microsoft Windows must be selected under the **Cryptographic Service Provider**.
16. Click the **Certificate Authority** tab, and ensure that **Enterprise Root CA** is selected.
17. Click **Apply** and then **OK**.
18. Select ADFSWEB certificate template or the certificate template you have configured, and click **Enroll**.
19. It will take some time to enroll, when enrollment succeeded, click **Finish**.

**Setting permission for Private Key of Certificate**

1. Open the certificate snap under the **console root, Certificates** (Local Computer) > **Personal > Certificate**.
2. Right-click on the certificate generated by Luna CSP and select **All Tasks > Manage Private Keys**.
3. Click **Add**, type **Administrator** in the **Enter the object name to select** text box.
4. Click OK. Ensure that Domain Administrator is added in the Group or User Name list.
5. Select the domain administrator and select the Full Permission check box.
6. Click Apply and then OK to close the window.

Configure ADFS to use SafeNet Luna HSM

Install ADFS 3.0 Using Server Manager

1. Log on to ADFSWEB as a domain administrator.
2. Open Server Manager. To open Server Manager, click Server Manager on the Start screen or Server Manager in the taskbar on the desktop. In the Quick Start tab of the Welcome tile on the Dashboard page, click Add roles and features. Alternatively, you can click Add Roles and Features on the Manage menu.
3. On the Before you begin page, click Next.
4. On the Select installation type page, click Role-based or Feature-based installation, and then click Next.
5. On the Select destination server page, click Select a server from the server pool, verify that the target computer is selected, and then click Next.
6. On the Select server roles page, click Active Directory Federation Services, and then click Next.
7. On the Select features page, click Next. The required prerequisites are preselected for you. You do not have to select any other features.
8. On the Active Directory Federation Service (AD FS) page, click Next.
9. After you verify the information on the Confirm installation selections page, click Install.
10. On the Installation progress page, verify that everything installed correctly, and then click Close.

Create and configure a server authentication certificate in IIS

1. Log on to ADFSWEB as a domain administrator.
2. From the Start menu, select All Programs > Administrative Tools > Internet Information Services (IIS) Manager.
3. In the console tree, click the root node that contains the name of the computer, and then, in the details pane, double-click the icon named Server Certificates in the IIS grouping.
4. In the Actions pane, click Create Certificate Request.
5. Enter the details in the Create Certificate window.
6. Common Name must be fully qualified domain name.
7. After providing all the details, Click Next.
8. Select Microsoft RSA SChannel Cryptographic Provider and 2048 as Bit Length.
9. Click Next, select the location to save the certificate request as C:\request.txt.
10. Click Finish, it will generate the certificate request. Submit certificate request to CA and save the signed certificate.
11. In the IIS Action pane, click Complete Certificate Request.
12. Browse and select the CA signed certificate and enter the Friendly Name as ADFS Server Certificate.
13. Click **OK** to complete the certificate request and close the window.

14. In the console tree, click the root node that contains the name of the computer, click **Default** website.

15. In the **Actions** pane, click **Bindings**.

16. In the **Site Bindings** dialog box, click **Add**.

17. In the **Add Site Binding** dialog box, select **https** in the **Type** drop-down list, select the certificate that you have generated through IIS in the SSL certificate drop-down list, click **OK**, and then click **Close**.

18. Close the Internet Information Services (IIS) Manager console.

### Configure the computer as a first federation server

1. Log on to ADFSWEB as a domain administrator.

2. Open the **Server Manager**. On the **Server Manager Dashboard** page, click the **Notifications** flag, and then click **Configure the federation service on the server**.

3. The **Active Directory Federation Service Configuration Wizard** opens.

4. On the **Welcome** page, select **Create the first federation server in a federation server farm**, and then click **Next**.

5. On the **Connect to AD DS page**, specify an account by using domain administrator permissions for the Active Directory (AD) domain to which this computer is joined, and then click **Next**.

6. On the **Specify Service Properties page**, do the following, and then click Next:
   - Select the certificate that you have configured and bind in the IIS.
   - Provide a name for your federation service. For example, fsweb.contoso.com. This name must match one of the subject or subject alternative names in the certificate.
   - Provide a display name for your federation service. For example, Contoso Corporation. Users see this name on the Active Directory Federation Services (AD FS) sign-in page.

7. On the **Specify Service Account** page, select the option to use an existing gMSA or domain account, click **Select** to select an account. Add **Contoso\Administrator** and provide the password.

8. On the **Specify Configuration Database** page, specify an AD FS configuration database, and then click **Next**. You can select **create a database on this computer by using Windows Internal Database (WID)**, also you can specify the location and the instance name of Microsoft SQL Server.

9. On the **Review Options** page, verify your configuration selections, and then click **Next**.

10. On the **Pre-requisite Checks** page, verify that all prerequisite checks are successfully completed, and then click **Configure**.

11. On the **Results** page, review the results and check whether the configuration is completed successfully, and then click **Next** steps required for completing your federation service deployment. Click **Close** to close the configuration wizard.

### Configure Corporate DNS for the Federation Service and DRS

1. On your domain controller, log on as domain administrator.

2. In **Server Manager**, on the **Tools** menu, click **DNS** to open the DNS snap-in.

3. In the console tree, expand the domain_controller_name node, expand **Forward Lookup Zones**, right-click **domain_name**, and then click **New Host (A or AAAA)**.
4. In the Name box, type the name to use for your AD FS farm. i.e. ADFSWEB
5. In the IP address box, type the IP address of your federation server. Click Add Host.
6. Right-click the domain_name node, and then click New Alias (CNAME).
7. In the New Resource Record dialog box, type enterpriseregistration in the Alias name box.
8. In the fully qualified domain name (FQDN) of the target host box, type federation_service_farm_name.domain_name.com, i.e. ADFSWEB.contoso.com and then click OK.
9. Open the command prompt and then run ipconfig /flushdns on domain controller and also the AD FS Server.

Install the token signing/decrypting certificate generated by Luna CSP

1. Log on to ADFSWEB as domain administrator.
2. From the Start menu, select All Programs > Administrative Tools > Windows PowerShell Modules.
3. Type get-ADFSProperties and press the Enter key. See that AutoCertificateRollover is set to be True.
4. Type Set-ADFSProperties -AutoCertificateRollover $False and press the Enter key.
5. Type get-ADFSProperties and press the Enter key. Verify that AutoCertificateRollover is set to be False.
6. Close the PowerShell window.
7. Open the ADFS Management.
8. Expand the Service and click Certificates.
9. In the Actions pane, click Add Token-Signing Certificate.
10. Select the ADFS Token Signing certificate that you have generated using Luna CSP.
11. Click OK. It will add the certificate in the Certificate pane.
12. Right-click on the certificate and select Set as Primary.
13. A confirmation message will pop up. Click Yes.
14. Delete the other certificate, i.e., ADFS Signing Secondary Certificate.
15. In the Actions pane, click on Add Token-Decrypting Certificate.
16. Select the ADFS Token Signing certificate that you have generated using Luna CSP.
17. Click OK. It will add the certificate in the Certificate pane.
18. Right-click on the certificate and select Set as Primary.
19. A confirmation message will pop up. Click Yes.
20. Delete the other certificate, i.e., ADFS Signing Secondary Certificate.
22. Open the command prompt and run the following commands to stop and start the ADFS service.
   ```
   Net stop adfssrv
   Net start adfssrv
   ```
23. Verify that ADFS Service successfully started.
Verify that Federation Server is Operational

1. Open a browser window and in the address bar, type the federation server name, and then append it with federationmetadata/2007-06/federationmetadata.xml to browse to the federation service metadata endpoint. For example, https://adfsweb.contoso.com/federationmetadata/2007-06/federationmetadata.xml.

In your browser window, if you can see the federation server metadata without any Secure Socket Layer (SSL) errors or warnings, your federation server is operational.
2. You can also browse to the AD FS sign-in page where your federation service name is appended with adfs/ls/idpinitiatedsignon.htm, for example, https://adfsweb.contoso.com/adfs/ls/idpinitiatedsignon.htm.

This entry displays the AD FS sign-in page where you can sign in by using domain administrator credentials.

**NOTE:** Ensure to configure your browser settings to trust the federation server role by adding your federation service name, for example, https://adfsweb.contoso.com, to the browser’s local intranet zone.
Configure Multiple ADFS Instances Using Same Key Pair on HSM

This chapter describes how to set up small test lab for multiple ADFS instances which will use the same keys on the HSM for encryption\decryption of tokens issued by ADFS.

Setting up Two Instances of ADFS Sharing Same Keys on HSM

Microsoft ADFS Setup

Microsoft ADFS must be installed on the target machines to carry on with the integration process.

The following setup is required:

- TESTDC: Windows Server 2008 R2 Enterprise Edition machine, which will become a Domain Controller.
- Domain Administrator privileges

It is assumed that you have joined the ADFS1 and ADFS2 computer to the CONTOSO domain.

SafeNet Luna HSM Setup

Luna Client should be installed on the target machines to carry out the integration. Refer the Prerequisite section of this guide to install the SafeNet Luna HSM Client and establishing the NTLS connection with the registered partition on the SafeNet Luna HSM.

To use the same key pair on SafeNet Luna HSM, you have to register the same SafeNet Luna HSM partition on both ADFS1 and ADFS2 computers. Run the \texttt{vtl verify} command to ensure that you have registered the same partition with both instances.
Setting up SafeNet Luna HSM for Active Directory Federation Services

To set up SafeNet Luna HSM for Active Directory Federation Services, perform the following steps:

Register CSP

CSP must be installed on the Federation Servers (ADFS1 and ADFS2) in a separate step following completion of the main SafeNet Luna HSM Client software installation.

Refer to Chapter two for installation steps of Luna CSP.

Generate Token Signing Certificate to use with ADFS1

Create a Token Signing/ Decrypting Certificate using Luna CSP

1. Log on to ADFS1 as a domain administrator.
2. From the Start menu, select Run.
3. In the Run dialog box, type mmc and click OK.
4. The mmc console displays. Select File > Add/Remove Snap-in...
5. In the Add or Remove Snap-Ins dialog box, find the Certificates snap-in (under the Available snap-ins section) and select it.
6. Click Add, Select Computer Account and Click Next.
7. Select Local Computer, and click Finish.
8. Click OK and expand the Certificates under Console Root.
9. Right-click on the Personal folder and select All Tasks > Advanced Operations > Create Custom Request...
10. Click Next, Select Proceed without enrollment policy and then click Next.
11. On Custom request page, select (No template) Legacy Key from the drop-down list and Request format as PKCS #10. Click Next.
12. Click Details and then Properties.
14. Select Common Name under Subject Name and enter the “ADFS_TOKEN_SIGNING” in Value field and click Add. Repeat the same step for adding more values.
15. Click the General tab and provide the Friendly Name. For example ADFS Token.
16. Click the Private Key tab, and verify that Luna enhanced RSA and AES provider for Microsoft Windows must be selected under the Cryptographic Service Provider.
17. Click Key and select Key size as 2048 from the drop-down list.
18. Click Key type and select Exchange.
19. Click Key permissions and select Use custom permissions check box.
20. Click **Set permissions**... and then **Add**.

21. Type **NETWORK SERVICE** in the text box and click **OK**. It will add the **NETWORK SERVICE** in the **Group or user name** area. Provide it read permission by selecting **Read** check box under the **Permission** area.

22. Click **Add** again and add the Domain Administrator (CONTOSO\Administrator) and provide **Full Control** and **Read** permissions to the Administrator by clicking respective check boxes and click **OK**.

23. Click **Next** and then Browse to save the certificate request.

24. Select **Base 64 File** format, and click **Finish**.

25. Check the SafeNet Luna HSM registered partition to see the container and keys generated. The snapshot given below shows the keys and container generated on the SafeNet Luna HSM partition.

```
[local_host] lunash:>partition showContents -partition part2 -password userpin2

Partition Name: part2
Partition SN: 152037009
Storage (Bytes): Total=102701, Used=2144, Free=100557
Number objects: 3

Object Label: X-le-aa48606f-252d-4753-9e7c-26cbcb11baa9
Object Type: Public Key

Object Label: X-le-aa48606f-252d-4753-9e7c-26cbcb11baa9
Object Type: Private Key

Object Label: le-aa48606f-252d-4753-9e7c-26cbcb11baa9
Object Type: Data

Command Result: 0 (Success)
```

**NOTE:** The Object Type: Data is the key container for the ADFS keys; copy the Object Label of the container i.e. “le-aa48606f-252d-4753-9e7c-26cbcb11baa9”. This container will be used to associate the certificate with the same key pair on ADFS2.
26. Submit the certificate request and obtain signed certificate from the Certificate Authority such as, VeriSign, GlobalSign, etc. You can also use local CA to sign the certificate request.

   a. In the Certificate Console, right-click on the Personal folder and select All Tasks > Import and follow the instruction to import the Token Signing Certificate signed by CA.

   b. You will get a message 'Certificate imported successfully'. Double-click on the certificate and verify that “You have a private key that corresponds to this certificate.”

Now follow the steps of Chapter two from section “Configure ADFS to use SafeNet Luna HSM” to complete the integration on ADFS1.

Create Token Signing Certificate to use with ADFS2

Export the existing Token Signing certificate from ADFS1

It is assumed that you have followed the Integration Guide and successfully completed the integration on first node i.e., ADFS1.
The process is as follows:

1. Log on to the ADFS1 server with the administrator account.
2. Click Start > Run > type MMC and press the Enter key.
3. In the console click File > Add/Remove Snap-in… > Certificates > Add.
4. Select Computer Account and click Next.
5. Select Local computer and click Finish.
6. Click OK and expand Personal, and then click Certificates.
7. Right-click the ADFSTokenSigning certificate, point to All Tasks, and then click Export.
9. On the Export Private Key page, click No, do not export the private key, and then click Next.
10. On the Export File Format page, click DER encoded binary X.509, and then click Next.
11. On the File to Export page, in the File Name box, type C:\export.cer and then click Next.
13. In the Certificate Export Wizard message box, click OK.
14. Close the certificate management console.
15. Copy and paste the exported certificate on the ADFS2 server.

Import the ADFS1 Token Signing certificate to ADFS2

Before you import the certificate on ADFS2 server you must install Luna CSP first and then register it with the same partition as you registered for ADFS1.

1. Log on to the ADFS2 server with the administrator account.
2. Click Start->Run->type MMC and press Enter.
3. In the console click File-> Add/Remove Snap-in…-> Certificates-> Add.
4. Select Computer Account and click Next.
5. Select Local computer and click Finish.
6. Click OK and expand Personal, and then click Certificates.
7. Right-click the Certificate, point to All Tasks, and then click Import.
8. On the Welcome to the Certificate Import Wizard page, click Next.
9. On the File to Import page, click Browse and select the certificate you have copied from ADFS1.
11. Right-click on the certificate and click Open.
12. In the Certificate dialog box, on the Details tab, select the Thumbprint attribute then press the Control-C on the keyboard to copy the Thumbprint to the Windows clipboard.
13. Open the command prompt.
14. At the command prompt, type
   ```
   certutil -repairstore -v -csp "Luna enhanced RSA and AES provider for Microsoft Windows" My "Thumbprint" repaircsp.inf
   ```
NOTE: here is a sample file "repaircsp.inf":

```
[Properties]
11 = ""; Add friendly name property
2 = "{text}"; Add Key Provider Information property
   _continue_="Container=le-aa48606f-252d-4753-9e7c-26cbb11baa9&"
   _continue_="Provider=Luna enhanced RSA and AES provider for Microsoft Windows&"
   _continue_="ProviderType=24&"
   _continue_="Flags=32&"
   _continue_="KeySpec=1"
```

**NOTE:** Replace the container "le-aa48606f-252d-4753-9e7c-26cbb11baa9" with Object label that is generated on your SafeNet Luna HSM partition when you generated the keys on ADFS1.

15. The output of the command is similar to the following:

```
My
================ Certificate 0 ================
X509 Certificate:
Version: 3
Serial Number: 616470f3000000000007
Signature Algorithm:
   Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
   Algorithm Parameters:
      05 00
Issuer:
   CN=contosoCA
   DC=contoso
   DC=com
NotBefore: 1/16/2014 1:07 PM
NotAfter: 1/16/2014 1:07 PM
Subject:
   CN=ADFSWithToken
   OU=TestToken
   O=ADFSWithHSM
   L=MYCity
   S=MYState
   C=IN
Public Key Algorithm:
   Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA (RSA_SIGN)
   Algorithm Parameters:
      05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
   0000 30 82 01 0a 02 82 01 01 00 e8 75 9b 10 71 7b 0c
   0010 6e 6f 2e 15 23 84 6c 05 9f 3e 29 d0 c6 dc 09 2c
   0020 ac e5 07 97 fe c5 03 f0 30 1e 9a a9 b9 95 dd 0d
   0030 a6 54 f4 df 59 a8 47 0b f3 7f db 04 59 92 97 b2
   0040 42 2a 3b cd ec b4 f2 2c 64 2b 13 60 83 bd 25 4a
   0050 d2 a6 f1 9e c7 e7 fe 04 ac cc b6 b1 39 54 52 c3
   0060 2c 67 62 60 8f 4f ad 37 d5 93 91 f9 24 9c ca 33
```
5 – Configure Multiple ADFS Instances Using Same Key Pair on HSM

Certificate Extensions: 7

2.5.29.14: Flags = 0, Length = 16
Subject Key Identifier
7b 75 de c6 26 9e a2 1f e9 18 04 60 24 2f 31 36 ff da 19 e9

2.5.29.15: Flags = 1(Critical), Length = 4
Key Usage
Digital Signature, Key Encipherment (a0)

2.5.29.35: Flags = 0, Length = 18
Authority Key Identifier
KeyID=cd bd 53 10 dd 8e 67 3d 4b e4 80 d5 68 8e 0f d4 22 90 e5 01

2.5.29.31: Flags = 0, Length = ba
CRL Distribution Points
[1]CRL Distribution Point
Distribution Point Name:
  Full Name:
  URL=ldap:///CN=contosoCA,CN=CA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint

1.3.6.1.5.5.7.1.1: Flags = 0, Length = ae
Authority Information Access
[1]Authority Info Access
  Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
  Alternative Name:
  URL=ldap:///CN=contosoCA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=com?cACertificate?base?objectClass=certificationAuthority

1.3.6.1.4.1.311.20.2: Flags = 0, Length = 14
Certificate Template Name (Certificate Type)
  WebServer

2.5.29.37: Flags = 0, Length = c
Enhanced Key Usage
  Server Authentication (1.3.6.1.5.5.7.3.1)

Signature Algorithm:
  Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
  Algorithm Parameters:
  05 00

Signature: UnusedBits=0
0000  76 a1 7d 4d 13 6c fd e3 13 e2 0d e4 ea 5d 85 ff
0010  1e a8 81 68 5c d9 7b ad e5 69 d9 b3 82 0a cf 3b
0020  7d bf e2 52 22 ce 38 ef e8 57 fc eb 3e ca af e4
0030  09 6b d1 22 2a e3 9f b6 e1 d6 33 55 9a 93 d9 2e
0040  df f6 33 d9 ae 06 63 b3 f9 0c a9 2e e8 34 e4 14
0050  d8 51 b8 6b 6e 62 13 85 a5 d7 f6 81 98 42 11 b3
16. After completing the command, right-click on certificate in the console and click Properties.

17. In the General tab, type ADFS Token in the Friendly name text box. Click OK to close the Properties window.

18. Right-Click on the certificate and click Open.

19. Ensure that the certificate displays the text “You have a private key that corresponds to this certificate”.

20. Click OK to close the certificate window.
21. At the command prompt, type `certutil -verifystore My "Thumbprint"` and press the Enter key.

```
C:\>certutil -verifystore My "da 9e 7e 9b 0f 7f 42 1b 46 b3 53 bb 22 63 48 ed 38 ce d5 c3"
---------- Certificate 0 ----------
Serial Number: 616470f3000000000007
Issuer: CN=contosoCA, DC=contoso, DC=con
NotBefore: 1/16/2016 1:07 PM
NotAfter: 1/16/2016 1:07 PM
Subject: CN=ADFSsTokenSigning, OU=TestToken, O=ADFSwithHSM, L=MYCity, S=MYState,
G=IN
Certificate Template Name (Certificate Type): WebServer
Non-root Certificate
Template: WebServer, Web Server
Cert Hash<sha1>: da 9e 7e 0b 0f 7f 42 1b 46 b3 53 bb 22 63 48 ed 38 ce d5 c3
- Key Container = 1e-aa48606f-252d-4753-9c7c-26c86b11bae
- Provider = Luna enhanced RSA and AES provider for Microsoft Windows
- Private key is NOT exportable
- Encryption test passed
- Verbose Issue Policies: None
- Verified Application Policies:
- 1.3.6.1.5.5.7.3.1 Server Authentication
- Certificate is valid
- Certutil -verifystore command completed successfully.
```

22. Ensure that the command result states that the Certificate is Valid and shows Encryption test passed. Now the certificate is ready to use as a Token Signing Certificate for ADFS2.

23. Close the **Command Prompt** window

24. Close all the open windows and restart the server.

After successful restart, log on to the ADFS2 server as a domain administrator and follow the steps of Chapter two from section “**Configure ADFS to use SafeNet Luna HSM**” to complete the integration on ADFS2.

You can configure more ADFS instances like ADFS2 node to use the same key pair on HSM using the steps provided above.