### Document Information

<table>
<thead>
<tr>
<th>Product Version</th>
<th>1.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Part Number</td>
<td>007-013897-001</td>
</tr>
<tr>
<td>Release Date</td>
<td>21 November 2018</td>
</tr>
</tbody>
</table>

### Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rev. A</td>
<td>17 August 2017</td>
<td>For initial release 1.1.0</td>
</tr>
<tr>
<td>Rev. B</td>
<td>19 September 2017</td>
<td>For release 1.1.1</td>
</tr>
<tr>
<td>Rev. C</td>
<td>14 November 2017</td>
<td>For release 1.2</td>
</tr>
<tr>
<td>Rev. D</td>
<td>05 February 2018</td>
<td>For release 1.3</td>
</tr>
<tr>
<td>Rev. E</td>
<td>02 March 2018</td>
<td>For HSM on Demand release 1.3</td>
</tr>
<tr>
<td>Rev. F</td>
<td>05 April 2018</td>
<td>For release 1.4</td>
</tr>
<tr>
<td>Rev. G</td>
<td>07 May 2018</td>
<td>For HSM on Demand release 1.4</td>
</tr>
<tr>
<td>Rev. H</td>
<td>10 June 2018</td>
<td>For release 1.5</td>
</tr>
<tr>
<td></td>
<td>12 September 2018</td>
<td>For release 1.6</td>
</tr>
<tr>
<td></td>
<td>21 November 2018</td>
<td>For release 1.7</td>
</tr>
</tbody>
</table>

### Trademarks and Copyrights

Copyright 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto 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.

### Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto 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, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible 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.

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Gemalto.
Contents

Overview .................................................................................................................. 5
  Third Party Application Details ........................................................................... 5
  Supported Platforms ......................................................................................... 5

Preparing for the Integration ................................................................................. 6
  Provision HSMoD Service .................................................................................. 6
  Adding a Service ............................................................................................... 6
  Adding a Service Client ..................................................................................... 6
  Initializing the HSM ......................................................................................... 8
  Constraints on HSMoD services ........................................................................ 9
  Preparing Environment in Windows Integrations ............................................. 9

Integrating Microsoft Active Directory Certificate Services with an HSM on Demand Service on Windows Server 2012 R2 or Windows Server 2016 ................................................................. 10
  Configuring the SafeNet Key Storage Provider (KSP) ...................................... 10
  Installing Microsoft ADCS .............................................................................. 11
  Enrolling the CA certificate ............................................................................ 14
  Archiving Keys ............................................................................................... 15
  Performing a Key Recovery ............................................................................. 17
  Preparing the Active Directory Certificate Services Cluster Environment .... 18
    Setting up the CA server role on the secondary cluster node .................... 19
    Installing the Failover Cluster feature ......................................................... 21
    Configuring the Failover Cluster feature ..................................................... 21
    Configuring the Active Directory Certificate Services Failover Cluster ....... 22
    Creating CRL objects in the Active Directory ............................................ 22
  Modifying the CA configuration in Active Directory ....................................... 22
  Backing up the Certification Authority ............................................................ 23
  Restoring the Certification Authority .............................................................. 24
  Migrating a MS CA onto a HSM on Demand service using ms2Luna ............ 24
Overview

This document covers the necessary information to install, configure, and integrate Microsoft Active Directory Certificate Services (ADCS) on Windows with an HSM on Demand (HSMoD) service. It demonstrates how to secure your Microsoft Root Certificate Authority (CA) signing keys in an HSMoD service.

The Microsoft ADCS on Windows provides customizable services for creating and managing public key certificates used in software security systems employing public key infrastructure.

A server configured as a certification authority (CA) provides the management features needed to regulate certificate distribution and use. ADCS is the Windows Server service that provides the core functionality for Windows Server CAs. ADCS provides customizable services for managing certificates for a particular CA and for the enterprise.

The root of trust in a public key infrastructure is the CA. Fundamental to this trust is the CA’s root cryptographic signing key, which is used to sign the public keys of certificate holders and more importantly, its own public key. The compromise of a CA's root key by malicious intent, inadvertent errors, or system failures can be of catastrophic proportions. Hence, this root-signing key must be diligently protected by the best technologies and practices within the cryptographic community such as using an HSM on Demand Service.

Using an HSMoD service to secure the Microsoft ADCS root key provides the following benefits:

- full life cycle management of the keys
- load-balancing and failover by clustering

This document contains the following sections:

- "Preparing for the Integration" on page 6
- "Integrating Microsoft Active Directory Certificate Services with an HSM on Demand Service on Windows Server 2012 R2 or Windows Server 2016" on page 10

This overview contains the following topics:

- "Third Party Application Details" below
- "Supported Platforms" below

Third Party Application Details

This integration guides uses the following third party applications:

- Microsoft Active Directory Certificate Services

Supported Platforms

The following platforms are tested with HSMoD Service:

- Windows Server 2016
- Windows Server 2012R2
Preparing for the Integration

Before you proceed with the integration, ensure you have completed the following:

> "Provision HSMoD Service" below
> "Preparing Environment in Windows Integrations" on page 9

Provision HSMoD Service

The HSM on Demand Service provides your client machine with access to an HSM application partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share, a single application partition.

You must provision your HSM on Demand service by adding the service, downloading the service client package and initializing the HSM. Provisioning your HSM on Demand service entails:

> "Adding a Service" below
> "Adding a Service Client" below
> "Initializing the HSM" on page 8

Adding a Service

1. Under the Services tab, select the Add New Service page. Click Deploy on the service tile for the service you wish to add.

   **NOTE** Click Deploy on the HSM on Demand Service tile for your integration.

2. Review the "Terms of Services DPoD." Enable the I have read and accept the Terms of Service above check box and then click Next.

3. On the Add <service_type> Service page, enter a name for the Service in the Service Name field. You can optionally allow non-FIPS approved algorithms by selecting the Allow non-FIPS approved algorithms check box. Click Next.

   **CAUTION!** You cannot alter the FIPS setting after creating the service. You must decide if the service should allow or disallow non-FIPS approved algorithms before clicking Finish in the next step.

4. Review the configuration summary page. If acceptable, click Finish. If you would like to make changes to the configuration, click Go Back.

   When completed, the new service is listed under My Services and a Create Service Client? window displays.

5. Click Create Service Client.

Adding a Service Client

1. In the Create Service Client window enter a name for the service client in the Service Client Name field.
Preparing for the Integration

2. Select **Create Service Client**.

   A new HSM service client package is created and provided for downloading on your client system.

   **NOTE** The HSM service client package is a zip file that contains system information needed to connect your client system to an existing HSM on Demand service. The HSM service client package should download immediately on creation. If it does not, or you lose access to your HSM service client package it can be accessed or reacquired through the **My Services** table.

3. Transfer the service client package to your client system. You can use SCP, PSCP, WinSCP, FTPS, or any other secure file transfer tool.

4. Unzip the service client package.

   For Linux, enter:
   
   ```
   unzip <service_client_package>.zip
   ```

   For Windows, using the Windows GUI or an unzip tool unzip the file:
   
   ```<service_client_package>.zip```

   **NOTE** For more information about the service client package contents see.

5. Extract the cvclient-min file.

   **NOTE** Extract the cvclient-min file in the directory where you extracted the `<service_client_package>.zip`. Do not extract to a new cvclient-min directory.

   For Linux, untar the cvclient-min.tar
   
   ```
   tar xvf cvclient-min.tar
   ```

   For Windows, unzip the cvclient-min.zip.

6. Set the environment variable.

   For Linux, execute:
   
   ```
   source ./setenv
   ```

   For Windows, right click setenv.cmd and select **Run as Administrator**.

   **NOTE** If you encounter the error dll load failed with GetLastError() 126 move the contents of the cvclient_min folder up one directory and execute setenv.

7. Start LunaCM.
Preparing for the Integration

For Linux, execute the following from the directory where you extracted the cvclient-min.tar file.

```
./bin/64/lunacm
```

For Windows, execute the following from the directory where you unzipped the cvclient-min.zip file.

`lunacm`

### Initializing the HSM

1. Set the active slot to the service partition.

   `lunacm:> slot set -slot <slot_number>`

   **NOTE** Execute slot list in LunaCM to identify the slot number associated with your service.

2. Initialize the application partition. During this process you will create the partition’s Security Officer (SO), set the SO password, and specify the cloning domain.

   `lunacm:> partition init -label <service_label>`

3. Optional: If you wish to transfer key material to or from a PED-authenticated Luna partition, you initialize the SafeNet Data Protection On Demand partition using the red PED domain key.
   
   a. For DPoD deployments, contact customer support to obtain the necessary PED drivers so that your HSM client can communicate with the PED.
   
   b. Attach the PED locally to the client computer, insert the red cloning domain PED key, and initialize the partition, including the option to set the cloning domain from the red PED key. Execute:

      ```
lunacm:> partition init -label <cryptovisor_partition_label> -importpeddomain
```

4. Log in as the partition’s Security Officer:

   `lunacm:> role login -name Partition SO`

5. Initialize the Crypto Officer role:

   `lunacm:> role init -name Crypto Officer`

6. Log out of the partition Security Officer role and log in as the Crypto Officer.

   `lunacm:> role logout
   lunacm:> role login -name Crypto Officer`

7. You must change the Crypto Officer password immediately on the initial log in. Failure to due so will result in a password error on subsequent logins.

   `lunacm:> role changepw -name Crypto Officer`

8. Initialize the Crypto User role:

   `lunacm:> role init -name Crypto User`

9. Log out of the partition Crypto Officer role and log in as the Crypto User.

   `lunacm:> role logout
   lunacm:> role login -name Crypto User`

10. You must change the Crypto User password immediately on the initial log in. Failure to do so will result in a password error on subsequent logins.

    `lunacm:> role changepw -name Crypto User`
This completes initializing the HSM on Demand Service. The Crypto Officer and Crypto User roles can now be used to integrate applications with the HSMoD service to perform cryptographic operations.

**Constraints on HSMoD services**

Please take the following limitations into consideration when integrating your application software with an HSM on Demand Service.

**HSM on Demand Service in FIPS mode**

HSMoD services operate in a FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand service. The FIPS mode is enabled by default.

Refer to the *Mechanism List* in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

**Verify HSM on Demand <slot> value**

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send commands to. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use **slot list** to determine which slot numbers are in use by which HSMoD service.

**Preparing Environment in Windows Integrations**

Your system requires access to the SafeNet Key Storage Provider (KSP). Copy the **SafeNetKSP.dll** file from your downloaded service client package to C:\Windows\System32.

Failure to copy the **SafeNetKSP.dll** file will result in no access to the SafeNet Key Storage Provider's during the integration. For example, if configuring Microsoft Active Directory Certificate Services, the SafeNet Key Storage Providers will not be available options when setting up the Cryptography for CA.
Integrating Microsoft Active Directory Certificate Services with an HSM on Demand Service on Windows Server 2012 R2 or Windows Server 2016

This document provides detailed instructions and procedures to install and integrate Microsoft ADCS on Windows Server 2012 R2/2016 with an HSM on Demand Service. Microsoft ADCS uses the SafeNet Luna Key Storage Provider (KSP) for integration.

We recommend that you familiarize yourself with Microsoft ADCS before beginning the integration. Refer to the Windows Server 2012 R2 or Windows Server 2016 documentation for more information.

This integration contains the following topics:

> "Configuring the SafeNet Key Storage Provider (KSP) " below
> "Installing Microsoft ADCS" on the next page
> "Enrolling the CA certificate" on page 14
> "Archiving Keys" on page 15
> "Performing a Key Recovery" on page 17
> "Preparing the Active Directory Certificate Services Cluster Environment" on page 18
> "Modifying the CA configuration in Active Directory" on page 22
> "Backing up the Certification Authority " on page 23
> "Restoring the Certification Authority" on page 24
> "Migrating a MS CA onto a HSM on Demand service using ms2Luna" on page 24

Configuring the SafeNet Key Storage Provider (KSP)

You need to configure the SafeNet Key Storage Provider (KSP) so that the system can access the HSM on Demand Service as a user.

To configure the SafeNet Key Storage Provider

1. Navigate to the KSP installation directory. Run KspConfig.exe.

   ![Tip] The KSP client is available in the HSM on Demand service client package in the /KSP folder.

2. Double-click Register or View Security Library.
3. Click Browse. Select the cryptoki.dll file from the HSM on Demand service client package. Click Register.
4. On successful registration, a Success! message displays. Click OK.
5. Double-click Register HSM Slots.
6. Register the HSM for the Administrator user.
Integrating Microsoft Active Directory Certificate Services with an HSM on Demand Service on Windows

7. Register the HSM for the System user.

   a. Open the Register For User drop-down menu and select **Administrator**.
   b. Open the Domain drop-down menu and select your domain.
   c. Open the Available Slots drop-down menu and select the service label.
   d. Enter the Slot Password.
   e. Click Register Slot.
   f. On successful registration, a Success! message displays. Click OK.

NOTE The HSMoD service has been registered for both users, despite only one entry appearing for the <slot_label> in the Registered Slots section of the KSP interface.

Installing Microsoft ADCS

You need to install Microsoft ADCS to configure the Certificate Authority role for the system. You must configure the Microsoft ADCS to use the HSMoD service when you install and configure the Microsoft Certificate Authority (CA) user role.

To install Microsoft ADCS on Windows Server 2012/2016 Enterprise Full

1. Log in as an Enterprise Admin or Domain Admin with administrative privileges.
2. Click Start, Administrative Tools, and open the Server Manager.
3. Install the Certification Authority user role.

   a. Select Add roles and features.
   b. On the Before You Begin page click Next.
   c. On the Select installation type page enable the **Role-based or feature-based installation** radio button. Click Next.
   d. On the Select destination server page enable the Select a server from the server pool radio button. Select your server from the Server Pool menu. Click Next.
   e. On the Select Server Roles page select the Active Directory Certificate Services check box. Click Next.
f. A window will display asking you to **Add features that are required for Active Directory Certificate Services**. Click **Add Features**. Click **Next**.

   ![Select server roles](image)

   **NOTE** These are additional features that must be installed for the Active Directory Certificate Services to function.

   g. On the Active Directory Certificate Services page click **Next**.

   h. On the Select Role Services page select the **Certification Authority** check box. Click **Next**.

   **NOTE** The Certificate Authority is the only CA service supported by a cluster environment.

   i. Click Install.

4. When the installation completes click **Configure Active Directory Certificate Services** on the destination server. The AD CS configuration wizard will display.

   a. On the Credentials page click **Next**.

   b. On the Role Services page enable the **Certification Authority** check box. Click **Next**.

   c. On the Setup Type page enable the **Enterprise CA** check box. Click **Next**.

   d. On the CA Type page enable the **Root CA** check box. Click **Next**.

   e. On the Private Key page select the option that is most appropriate for your organization. Follow the relative procedural set below:
Create a New Private Key

1. Enable the **Create a new private key** check box.
2. On the Cryptography for CA page open the **Select a cryptographic service provider (CSP)** drop-down menu and select a SafeNet Key Storage Provider algorithm from the list.
3. Open the **Key character length** drop-down menu and select an appropriate length. Select the **Hash algorithm** that the CA will use for signing certificates.
4. Enable the **Allow administrator interaction when the private key is accessed by the CA** check box.
5. Click **Next**.

Use Existing Private Key

1. Enable the **Use existing private key** and the **Select an existing private key on this computer** check box. The Change Cryptographic Provider dialog will display.
2. Click **Change** and select the SafeNet KSP algorithm that you used to generate the private key.
3. Clear the **CA common name** field. Click **Search**.
4. Select the existing key. Click **Next**.
5. Select the **Hash algorithm** that the CA will use for signing certificates.
6. Enable the **Allow administrator interaction when the private key is accessed by the CA** check box.
7. Click **Next**.

f. On the CA name page enter a **Common name** for this CA. Click **Next**

g. On the Validity Period page set the validity period for the CA certificate. Click **Next**.

h. On the Configure Certificate Database page set the location where the CA will store its logs. Click **Next**.
i. On the Confirm Installation Selections page verify that the CA you are about to configure is appropriate.

j. Click **Configure**.

8. Click **Close** to exit the AD CS Configuration after viewing the installation results.

9. Verify that the CA service is running.

   `sc query certsvc`

10. Verify the CA key.

    `certutil -verifykeys`

    The MS ADCS integration with the HSM on Demand Service is complete. If you are configuring RAC you need to continue. If you are not configuring RAC, proceed to "Enrolling the CA certificate" on the next page.

11. Export the CA certificate

    a. Open a command prompt and execute `certsrv.msc`. Click **OK**.

    b. Select the CA node. Open the **Action** menu, click **All Tasks** and select **Backup CA**.

    c. On the Welcome to the Certification Authority Backup Wizard page click **Next**.
d. Enable the **Private key and CA certificate** check box. Enter a directory location to store the certificate and key. Click **Next**.

e. Enter a password in the **Password** field, and confirm the password in the **Confirm Password** field. Click **Next**.

f. Click **Finish**.

**NOTE** You will receive a warning message stating that the private key cannot be exported. This is expected behaviour. The private key will never leave the SafeNet HSM.

g. Click **OK**.

h. Use the `ksputil.exe` so that the keys will be visible to the second node in the cluster.

   ```
   ksputil clusterKey /s <slot_number> /n <CA_name> /t <Target_host_name>
   ```

12. Halt the CA service to unlock the shared disk resources.

   a. Click **Action**, select **All Tasks**, and then click **Stop Service**.

   b. Close the CA management utility.

13. Detach the shared storage from the cluster node.

   a. Access the Server Manager MMC utility. Click the **File and Storage Services**.

   b. Open **Disks** and right-click the shared disk resource, select **Take Offline**.

14. Release the HSM from the cluster node.

   a. Disable the network connection to the HSM.

   b. Log off from the cluster node.

**Enrolling the CA certificate**

You need to set the certificate that will be used by the Certification Authority on the system.

**To enroll a CA certificate using SafeNet Key Storage Provider**

1. Verify that the CA service is running.

   ```
   sc query certsvc
   ```

2. Create a CA template that uses SafeNet KSP.

   a. Open a command prompt and execute `certtmpl.msc`.

   b. Right-click the Administrator template and click **Duplicate Template**.

   c. On the **Compatibility** tab open the **Certification Authority** drop-down menu and select Windows Server 2008. Open the **Certificate Recipient** drop-down menu and select Windows Server 2008. Click **OK**.

   d. Select the **General** tab and enter a name for the template in the **Template display name** field.

   e. Select the **Cryptography** tab and open the **Provider Category** drop-down menu. Select **Key Storage Provider**. Enable the **Requests must use one of the following providers** check box.
In the Providers field, select the SafeNet Key Storage Provider check box.

Open the Algorithm name drop-down menu and select an algorithm.

Open the Request hash drop-down menu and select a hash signature.

Select the Subject Name tab and uncheck the Include e-mail name in subject name check box and the E-mail name check box.

Click Apply to save the template and click OK.

3. Open a command prompt and execute certsrv.msc.


5. Select the template that was recently created. Click OK.

6. Request a certificate based on the template.
   a. Open a command prompt and execute certmgr.msc.
   b. Right-click Personal, select All Tasks, and click Request New Certificate….
   c. Click Next.
   d. Click Next.
   e. Enable the checkbox next to the recently created template.
   f. Click Enroll.
   g. Verify the certificate was enrolled successfully.

Archiving Keys

This section will demonstrate that the various configurations with the SafeNet Luna HSM do not interfere with the CA key archival functionality.

To add a Key Recovery Agent Template to the CA

1. Add Key Recovery Agent (KRA) template to the CA.
2. Open a command prompt and execute certsrv.msc.
4. Select the Key Recovery Agent template. Click OK.

To request a KRA certificate

1. Open a command prompt and execute certmgr.msc.
2. Right-click Personal, select All Tasks, and click Request New Certificate….
3. Click Next.
4. Click Next.
5. Enable the Key Recovery Agent check box.
6. Click Enroll.
7. Verify that enrollment is pending. Click Finish.

**To issue the KRA certificate**

1. Open a command prompt and execute `certsrv.msc`.
2. Open Pending Requests. Right-click on the latest request for the KRA template, select All Tasks, and click Issue.
3. Select Issued Certificates... and verify that a new certificate has been issued.

**To retrieve the issued certificate from CA.**

1. Open a command prompt and execute `certmgr.msc`.
2. Right-click Certificates – Current User, select All Tasks, and click Automatically enroll and retrieve certificates. Click Next.
3. Select the recently issued KRA certificate. Click Finish.

**To configure the CA to support Key Archival.**

1. Open a command prompt and execute `certsrv.msc`.
2. Right-click the CA name and select Properties.
3. Select the Recovery Agents tab and enable the Archive the key radio button. Click Add.
4. Select the recently created KRA certificate. Click OK.
5. A dialog window displays stating you must restart the Active Directory Certificate Services for the changes to take effect. Click Yes.

**To create a template with key archival enabled**

1. Open a command prompt and execute `certtmpl.msc`.
2. Right-click the User template and select Duplicate Template.
4. Select the General tab and enter a name for the template in the Template display name field. Enable the Publish certificate in Active Directory check box.
5. Select the Request Handling tab and enable the Archive subject’s encryption private key check box.
6. Select the Subject Name tab and uncheck the Include e-mail name in subject name check box and the E-mail name check box.
7. Click Apply and then click OK.

**To add a new template to CA for issuing**

1. Open a command prompt and execute `certsrv.msc`.
2. Right-click Certificate Templates, click New, and select Certificate Template to Issue.
3. Select UserKeyArchival and click OK.
To issue the key archival template.

1. Open a command prompt and execute `certmgr.msc`.
2. Right-click Personal, select All Tasks, and click Request New Certificate…
3. Click Next.
4. Click Next.
5. Enable the UserKAarchival check box.
6. Click Enroll. Verify that the enrolment was successful.
7. Click Finish.

Performing a Key Recovery

You can recover archived keys.

To perform a key recovery

1. Log on to the system as Domain Administrator and ensure that the private key is still recoverable by viewing the Archived Key column in the Certification Authority console.
   a. Log on as Domain Administrator.
   b. From Administrative Tools, open Certification Authority.
   c. In the console tree, double-click CA, and then click Issued Certificates.
   d. From the View menu, click Add/Remove Columns.
   e. In Add/Remove Columns, in Available Column, select Archived Key, and then click Add. The Archived Key should now appear in Displayed Columns.
   f. Click OK and then, in the details pane, scroll to the right and confirm that the last issued certificate to UserKeyArchival has a Yes value in the Archived Key column.

   **NOTE** A certificate template must be modified so that the Archive bit and Mark Private Key as Exportable attributes are enabled. The private key is only recoverable if there is data in the Archived Key column.

   g. Double-click the Archive User certificate.
   h. Click Details. Write down the serial number of the certificate.

   **NOTE** The serial number is required for recovery. Do not include spaces between the values.

   i. Click OK, and close the Certification Authority.

2. Import the private key into an output file.
   a. Open a command prompt and execute `cd\`. Ensure that you are in the c:\ directory.
b. Execute `certutil -getkey <serial_number> <output_blob>`

c. Execute `dir <output_blob>`

**NOTE** If the file `<output_blob>` does not exist, verify the serial number that you used.

3. Recover the original private/public key.
   a. Open a command prompt and execute `certutil -recoverkey <output_blob> user.pfx`.
   b. When prompted, enter a new password.
   c. Execute `exit`. Close all windows and log off as the current user.

4. Find the recovered certificate.
   a. Open a command prompt and execute `certmgr.msc`.
   b. Right-click `Certificates (Current User)`, and select `Find Certificates`.
   c. Enter the CA name into the `Contains` field and click `Find Now`.
   d. Click `Select All` on the `Edit` menu.
   e. Click `Delete` on the `File` menu.
   f. Click `Yes`.
   g. Close Find Certificates.

5. Import the certificate.
   a. Right-click `Personal`, click `All Tasks`, and select `Import`.
   b. Click `Next`.
   c. On the Files to Import page enter `c:\user.pfx` in the `File Name` field. Click `Next`.
   d. Enter the password for the `.pfx` file. Click `Next`.
   e. On the Certificate Store page enable the `Automatically select the certificate store based on the type of certificate` check box. Click `Next`.
   f. Click `Finish`.

6. Verify the serial number of the imported certificate.
   a. Double-click `Personal` and select `Certificates`.
   b. Double-click the certificate.
   c. Click the `Details` tab. Verify that the serial number matches the original.

### Preparing the Active Directory Certificate Services Cluster Environment

If you are configuring RAC you must prepare the ADCS cluster environment for configuration. Before you proceed with the following procedures, ensure you have completed the following:
You must configure the SafeNet KSP before preparing the ADCS cluster environment. See "Configuring the SafeNet Key Storage Provider (KSP)" on page 10 for more information.

You must complete "Installing Microsoft ADCS" on page 11 on the primary cluster node.

Setting up the CA server role on the secondary cluster node.
This section provides detailed procedures on setting up the secondary cluster node.

To configure the secondary cluster node

1. Log in to the cluster node with permissions to install the secondary cluster node. To install an enterprise CA log in to an account with enterprise permissions in the Active Directory domain.
2. Click Start, select Run, and enter servermanager.msc in the field. Click OK.
3. Click File and Storage Services and select Disks. Ensure that the shared disk used by the CA is online.
4. Click Start, select Run, and enter MMC in the field. Click OK.
5. Open the File menu and select Add/Remove Snap-in....
6. Select Certificates from the Available snap-ins menu and click Add.
7. Enable the Computer account radio button and click Next.
8. Enable the Local computer: (the computer this console is running on) radio button. Click Finish.
9. Click OK.

To import an existing certificate

1. Right-click Certificates (Local Computer) and select Personal.
2. In the Action menu click All Tasks and select Import....
3. The Certificate Import Wizard will open. Click Next.
4. Enter the filename of the CA certificate for import. Click Next.

NOTE If you use the Browse... utility to find the certificate you must change the file type extension to Personal Information Exchange - *.pfx

5. Enter the password that was previously used to secure the private key. Click Next.

NOTE The private key password is required even if there is no private key in the *.pfx file.

6. Enable the Place all certificates in the following store radio button. Enter Personal in the Certificate Store field. Click Next.
7. Click Finish to import the certificate. Click OK to confirm the import.
8. Repair the association between the certificate and private key.
   a. In the Certificate Manager expand Personal and select Certificates.
   b. Select the imported certificate. Open the Action menu and select Open.
c. On the Details tab select the **Serial number** field. Copy the serial number value to the clipboard. Click OK.

d. Open a command prompt and execute `certutil –repairstore MY “<serial_number>”`.

**To add the AD CS role**

1. Open the Server Manager and select **Add Roles and Features**.
2. The Add Roles and Features wizard displays. On the Before You Begin page click **Next**.
3. On the Select installation type page enable the **Role-based or feature-based installation** radio button. Click **Next**.
4. On the Select Destination server page enable the **Select a server from the server pool** radio button. Select your server in the Server Pool menu. Click **Next**.
5. On the Select Server Roles page select the **Active Directory Certificate Services** check box. Click **Next**.
6. A window displays asking you to **Add features that are required for Active Directory Certificate Services**. Click **Add Features**. Click **Next**.

![NOTE] These are additional features that must be installed for the Active Directory Certificate Services to function.

7. On the Features page click **Next**.
8. On the Active Directory Certificate Services page click **Next**.
9. On the Select Role Services page select the **Certification Authority** check box. Click **Next**.

![NOTE] The Certificate Authority is the only CA service supported by a cluster environment.

e. Click **Install**.

10. When the installation completes click **Configure Active Directory Certificate Services on the destination server**. The AD CS configuration wizard displays.

**To configure the AD CS role**

1. On the Credentials page click **Next**.
2. On the Role Services page enable the **Certification Authority** check box. Click **Next**.
3. On the Setup Type page enable the **Enterprise CA** check box. Click **Next**.
4. On the CA Type page enable the **Root CA** check box. Click **Next**.
5. On the Private Key page enable the **Use existing private key** and the **Select a certificate and use its associated private key** radio buttons. Click Next.
6. On the Existing Certificate page select the CA certificate that was generated on the primary node. Click **Next**.
7. On the Configure Certificate Database page set the location where the CA will store its logs. Click **Next**.
8. A dialog box will display stating an existing database was found. Click Yes to proceed.

9. Click Configure.

10. Click Close to finish the role installation.

11. Log off from the secondary cluster node.

Installing the Failover Cluster feature

The following procedure must be repeated for each node in the cluster.

To install the failover cluster feature

1. Log in to the cluster node with local Administrator permissions.

2. Open Server Manager. Click Add roles and features.

3. On the Before you begin page click Next.

4. Select the Role-based or feature-based installation radio button. Click Next.

5. On the Select destination server page enable the Select a server from the server pool radio button. Select your server in the Server Pool menu. Click Next.

6. Click Next.

7. On the Select Features page enable the Failover Clustering check box. Click Next.

8. A window will display asking you to Add features that are required for Failover Clustering. Click Add Features. Click Next.

   NOTE These are additional features that must be installed for the Active Directory Certificate Services to function.

9. Click Install. When the installation is complete click Close.

Configuring the Failover Cluster feature

You need to install and enable the failover cluster feature.

To configure the failover cluster feature

1. Log on to the cluster node.

2. Open Server Manager. Open the Tools menu and select Failover Cluster Manager.

3. Open the Action menu and select Create a cluster.


5. On the Select Servers page enter the cluster node name of the first cluster node in the Enter Server Name field. Click Add.

6. On the Select Servers page enter the cluster node name of any remaining nodes. Click Add.

7. Click Next to continue.
8. On the Access Point for Administering the Cluster page enter a name to identify the cluster configuration. Click Next.

9. On the Confirmation page verify that you have properly configured the cluster name with the failover cluster. Click Next.


Configuring the Active Directory Certificate Services Failover Cluster

You need to configure the failover cluster feature to recognize the primary and activate the standby databases on failure.

To configure the Active Directory Certificate Services Failover Cluster

1. Open the Failover Cluster Management snap-in. Right-click Role and select Configure Role.
2. On the Before You Begin page click Next.
3. On the Select role page select Generic Service. Click Next.
5. On the Client Access Point page enter a name for the service in the Name field. Click Next.
6. On the Select Storage page enable the check box next to the disk storage that is mounted to the node. Click Next.
7. On the Replicate Registry Settings page click Add. Enter SYSTEM\CurrentControlSet\Services\CertSvc and click OK. Click Next.
8. On the Confirmation page verify the service you are configuring. Click Next.
10. Use the ksputil.exe to migrate the keys to the cluster.

   ksputil c /s <slot_number> /t <CA_cluster_service_name> /n <CA_name>

Creating CRL objects in the Active Directory

You can create a Certificate Revocation List object for your active directory.

To create CRL objects in the active directory

1. Log on to the cluster node.
2. Open a command prompt and execute cd %WINDIR%\System32\Certsrv\CertEnroll
3. Publish the CRL into the active directory.

   certutil -f dpublish "<CRL_file>"

Modifying the CA configuration in Active Directory

You can perform the following procedural set from any computer in your Active Directory configuration. The AIA object in the Active Directory stores the CA certificate. To enable both cluster nodes to update the CA certificate, complete the following.
To modify the CA configuration in active directory

1. Log on to the system with enterprise permissions.
2. Click Start, select Run, and enter dssite.msc in the field. Click OK.
3. Select the top node in the left pane. Open the View menu and select Show Services.
4. Expand Services and Public Key Services.
5. Select AIA. Select the CA name. Open the Action menu and select Properties.
   a. Select the Security tab and click Add….
   b. Click Object Types and enable the Computers check box. Click OK.
   c. Enter the name of the secondary cluster node in the Enter the object names to select field. Click OK.
   d. Select the Full Control check box for each cluster in the configuration. Click OK.
6. Select Enrollment Services. Select the CA name. Open the Action menu and select Properties.
   a. Select the Security tab and click Add….
   b. Click Object Types and enable the Computers check box. Click OK.
   c. Enter the name of the secondary cluster node in the Enter the object names to select field. Click OK.
   d. Select the Full Control check box for each cluster in the configuration. Click OK.
7. Select KRA. Select the CA name. Open the Action menu and select Properties.
   a. Select the Security tab and click Add….
   b. Click Object Types and enable the Computers check box. Click OK.
   c. Enter the name of the secondary cluster node in the Enter the object names to select field. Click OK.
   d. Select the Full Control check box for each cluster in the configuration. Click OK.
8. Close the Sites and Services snap-in.

Backing up the Certification Authority

You can enable and configure the location where the CA backup files will be stored using the Active Directory certificate services management console.

To backup the CA

1. Click Start, select Run, and enter certsrv.msc in the field. Click OK.
2. Select the CA node. Open the Action menu, click All Tasks and select Backup CA.
3. On the Welcome to the Certification Authority Backup Wizard page click Next.
4. Enable the Private key and CA certificate check box. Enter a directory location to store the certificate and key. Click Next.
5. Enter a password in the Password field, and confirm the password in the Confirm Password field. Click Next.
6. Click Finish.
Restoring the Certification Authority

You can restore CA certificates from the Active Directory certificate services management console.

To restore the CA

1. Click Start, select Run, and enter certsrv.msc in the field. Click OK.
2. Select the CA node. Open the Action menu, click All Tasks and select Restore CA.
3. On the Welcome to the Certification Authority Backup Wizard page click Next.
4. Enable the Private key and CA certificate check box. Enter a directory location to temporarily store the certificate and key. Click Next.
5. Enter a password in the Password field, and confirm the password in the Confirm Password field. Click Next.
6. Click Finish.
7. A dialog will display. It asks “Do you want to start Active Directory Certificate Services?” Click Yes.
8. Verify the Active Directory Certificate Services have successfully restarted in certsrv.

Migrating a MS CA onto a HSM on Demand service using ms2Luna

Storing keys on the software is not a secure practice. We recommend migrating the security key onto the HSM on Demand service. Refer to the SDK Reference Guide for more information about using the ms2luna.exe command.

To migrate a MS CA onto a SafeNet HSM using ms2Luna

1. Copy the CA certificate thumbprint.
2. Open a command prompt and run ms2Luna.exe from the HSMoD service client package

   NOTE: You need to register the service using KSP before migrating MSCA to SafeNet HSM. See "Configuring the SafeNet Key Storage Provider (KSP)" on page 10 for more information about registering the service with the SafeNet KSP.

3. Enter the Thumbprint of CA certificate and press Enter.
4. Verify that CA provider changes to SafeNet Key Storage Provider.
5. Uninstall the existing CA that the key was removed from.