Microsoft OCSP

Integration Guide

security to be free

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 below, 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.

Document Number: 007-011100-001, Rev. R

Release Date: August 2018

Contents

Preface

This document is intended to guide the security administrators through the procedure for integrating Microsoft Online Certificate Status Protocol (OCSP) with a SafeNet Luna HSM or HSM on Demand (HSMoD) service. This guide provides the necessary information to install, configure, and integrate Microsoft OCSP with a SafeNet Luna HSM or an HSMoD service. Microsoft OCSP uses the SafeNet Luna HSM or HSMoD service to secure signing keys for OCSP operations.

Scope

This guide demonstrates integrating Microsoft OCSP with a SafeNet Luna HSM or HSMoD service. The Microsoft online responder service implements the OCSP for decoding revocation status requests for specific certificates. The service evaluates the status request for these certificates and sends back a signed response containing the requested certificate status information.

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

Convention	Description
• bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type dir /p.) • Button names (Click Save As.) • Check box and radio button names (Select the Print Duplex check box.) • Window titles (On the Protect Document window, click Yes.) • Field names (User Name: Enter the name of the user.) • Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) • User input (In the Date box, type April 1.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1 Introduction

Overview

Microsoft Online Certificate Status Protocol (OCSP) is a protocol which provides real-time validation of a certificate's status. An OCSP responder is used to respond to certificate status requests. The OCSP responder can issue one of the following three responses:

- Valid
- Invalid
- Unknown

The OCSP responder implements the Online Certificate Status Protocol (OCSP) by decoding revocation status requests for specific certificates. The service evaluates the status requests for these certificates and sends back a signed response containing the requested certificate status information.

The integration between SafeNet Luna HSMs or HSMoD service and OCSP uses the industry standard PKCS#11 interface to generate the identity keys and provide security by protecting the Identity private keys within a hardware security module.

The benefits of using SafeNet HSMs to generate the signing keys for OCSP are:

- Secure generation, storage and protection of the Identity signing private key on FIPS 140-2 level 3 validated hardware*
- Full life cycle management of the keys.
- HSM audit trail.

NOTE: HSM on Demand services do not have access to the secure audit trail.

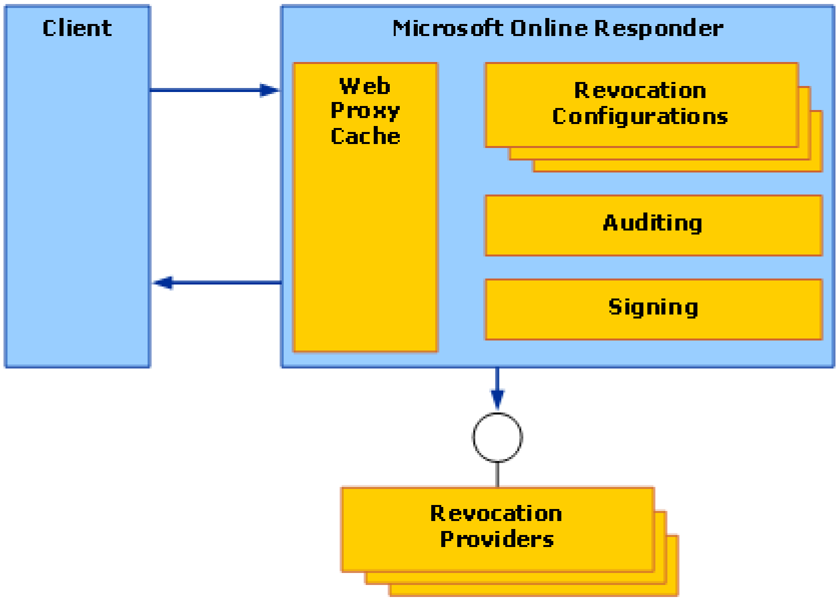
- Take advantage of cloud services with confidence.
- Significant performance improvements by off-loading cryptographic operations from application servers

*FIPS 140-2 validation in progress for HSMoD services.

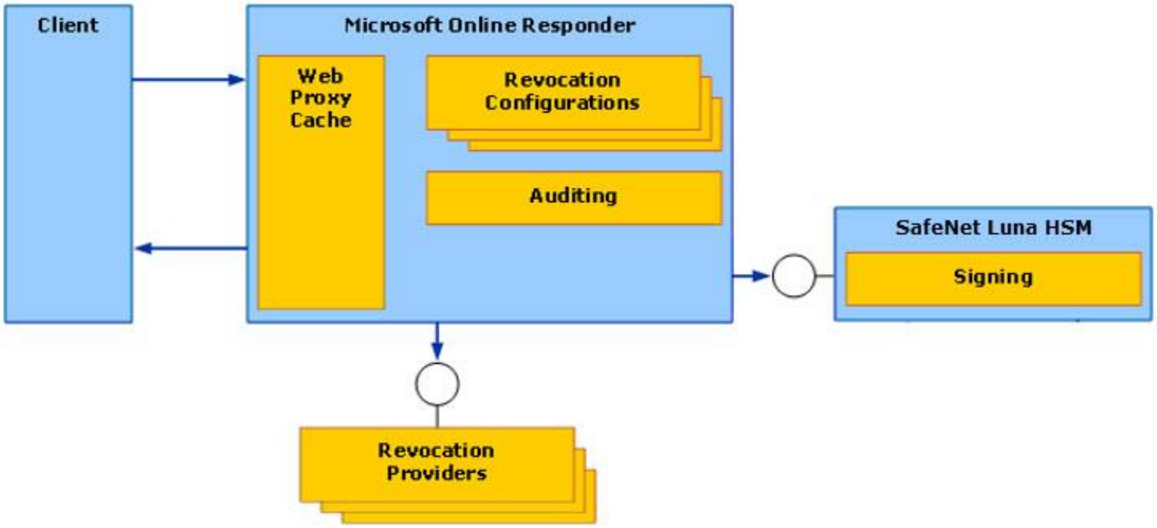
About the Microsoft Online Responder

The Microsoft OCSP implementation is separated into client and server components.

The client component is built into the Crypto API 2.0 library:



Microsoft Online Responder Components after integration with SafeNet Luna HSM:



Online Certificate Status Protocol Client

The Microsoft Online Certificate Status Protocol (OCSP) client is integrated into the CryptoAPI 2.0 certificate revocation infrastructure. OCSP implements the recommendation specified in the draft Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) "Lightweight OCSP Profile for High Volume Environment" and is optimized for high-volume scenarios.

Online Responder Service

The Online Responder service is a Microsoft Windows NT service (ocspsvc.exe) that is running with Network Service privileges. It performs the following operations:

- **Manages the Online Responder configuration**- The Online Responder provides a responder-wide set of attributes that can be configured. These attributes include public interfaces, access control settings, audit settings, and Web proxy cache settings. All the configuration information is stored in the registry under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OCSPSvc\Responder`.
- **Retrieves and caches revocation information based on configuration**- Based on the revocation configuration, the Online Responder service can retrieve and cache revocation information such as CRLs and delta CRLs for future use.
- **Signs responses**- For each successful request, the Online Responder signs the response with a pre-acquired signing key. SafeNet Luna HSM are used here for secure and fast signing of the response.
- **Audits configuration changes**-To conform to the Common Criteria requirements, all configuration changes of the Online Responder can be audited.

Microsoft Online Certificate Status Protocol Revocation Configuration

A revocation configuration is a set of definitions that configure the Online Responder service to respond to a certificate status request for a specific CA. Each Online Responder service can have one or more revocation configuration. Revocation configurations include the following objects:

- CA certificate
- Signing certificate for OCSP responses
- Revocation provider specific configuration

Third Party Application Details

This integration guide uses the following third party applications:

- Microsoft Online Certificate Service Provider (OCSP)

Supported Platforms

List of the platforms which are tested with the following HSMs.

SafeNet Luna HSM: SafeNet Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. SafeNet Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.
The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

This Integration is supported with following operating systems:

- Window Server 2016
- Window Server 2012 R2

NOTE: This integration is tested with SafeNet Luna Clients in both HA and FIPS Mode.

SafeNet Data Protection on Demand (DPoD): is a cloud-based platform that provides on-demand HSM and Key Management services through a simple graphical user interface. With DPoD, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain only the services that you need.

This integration is supported/verified with SafeNet DPoD on the following operating systems:

- Windows 2016 Server

Prerequisites

Before starting the integration of Microsoft OCSP with SafeNet Luna HSM or HSM on Demand Service ensure you have completed configuring the SafeNet Luna Network HSM or provisioning HSM on Demand service as per the requirement.

Configuring SafeNet Luna HSM

Before you get started ensure the following

1. Ensure the HSM is setup, initialized, provisioned and ready for deployment. Refer to the HSM product documentation for help.
2. Create a partition on the HSM that will be later used by Microsoft OCSP.
3. If using a SafeNet Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
 # /usr/safenet/lunaclient/bin/lunacm

 LunaCM v7.1.0-379. Copyright (c) 2006-2017 SafeNet.


Available HSMs:

 Slot Id ->               0

Label ->                 OCSP

Serial Number ->         1238712343066

Model ->                 LunaSA 7.1.0

Firmware Version ->      7.1.0

Configuration ->         Luna User Partition With SO (PED) Key Export With Cloning Mode

Slot Description ->      Net Token Slot
```

NOTE: Follow the SafeNet Network Luna HSM Product Documentation for detailed steps for creating NTLS connection, initializing the partitions, and initializing the necessary user roles.

Provision your HSM on Demand Service

This 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.

To use the HSM on Demand Service you need to provision you application partition, starting by initializing the following roles:

- **Security Officer (SO)** - responsible for setting the partition policies and for initialize the Crypto Officer.
- **Crypto Officer (CO)** - responsible for creating, modifying and deleting crypto objects within the partition. The CO can use the crypto objects and initialize an optional, limited-capability role called Crypto User that can use the crypto objects but cannot modify them.
- **Crypto User (CU)** - optional role that can use crypto objects while performing cryptographic operations.

NOTE: Refer to the “SafeNet Data Protection on Demand Application Owner Quick Start Guide” for procedural information on configuring the HSM on Demand service and create a service client.

The HSM on Demand Service client package is a zip file that contains system information needed to connect your client machine to an existing HSM on Demand service.

Constraints on HSM on Demand Services

Please consider the following limitations into consideration when integrating your application software with an HSMoD 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.

zVerify 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 the 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.

Using SafeNet HSM in FIPS Mode

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

```
[Misc]
```

```
RSAKeyGenMechRemap=1
```

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

Setup Microsoft OCSP

NOTE: All machines in the OCSP setup require Domain Administrator privileges.

Microsoft OCSP must be installed on the target machine to complete the integration process. The following setup is required:

- Windows Server machine that will be used as a Domain Controller.
- Windows Server machine that will be used as CA and OCSP Server.
- Windows machine, which will become a client to submit enrolment requests to the CA.

The three machines utilized are denoted in the setup as follows:

- **OCSPDC**: Windows Server Domain Controller machine.
- **OCSPSERV**: Windows Server CA and OCSP Server machine.
- **OCSPCL**: Windows Server client machine.

You can install Microsoft OCSP and CA on separate machines. If you are configuring your OCSP on separate machines, we recommend the following setup:

- **OCSPCA:** Windows Server machine, which will become a Domain Controller and CA.
- **OCSPSERV:** Windows Server machine, which will become an OCSP Server.
- **OCSPCL:** Windows machine, which will become a client to submit enrolment requests to the CA.

Register Security Library

Install the KSP for generating the CA certificate keys on the SafeNet Luna HSM or HSM on Demand service. See To register the SafeNet Key Storage provider for more information about configuring the SafeNet KSP. The tool **KspConfig.exe** is included in the Luna Client installation directory or is available in the HSMoD service client package. If you are registering with KSP see To register the SafeNet Key Storage provider. Alternatively, you can use the CSP to generate the OCSP signing keys. To use CSP for OCSP signing keys, you also need to register the CSP.

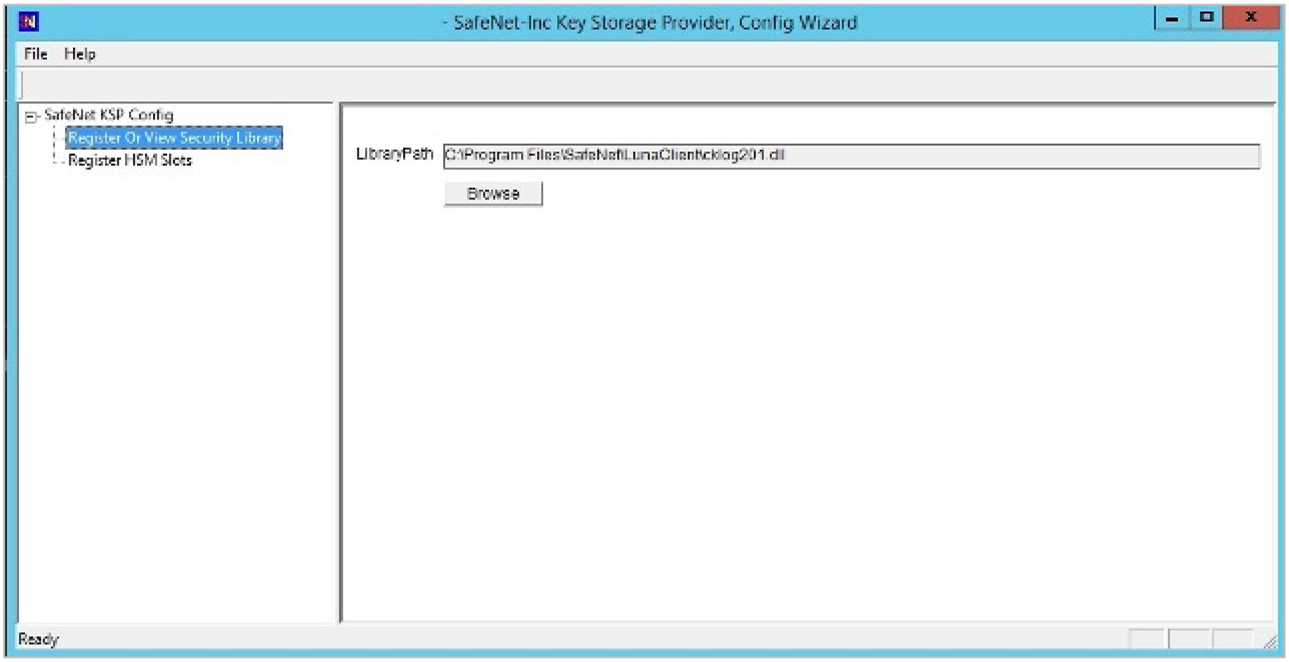
See To register the SafeNet CSP for more information about configuring the SafeNet CSP. If you are registering with CSP see To register the SafeNet CSP.

NOTE: If you are configuring the Microsoft OCSP on multiple systems, the SafeNet Key Storage Provider must be configured on the Certificate Authority and OCSP server systems.

To register the SafeNet Key Storage provider

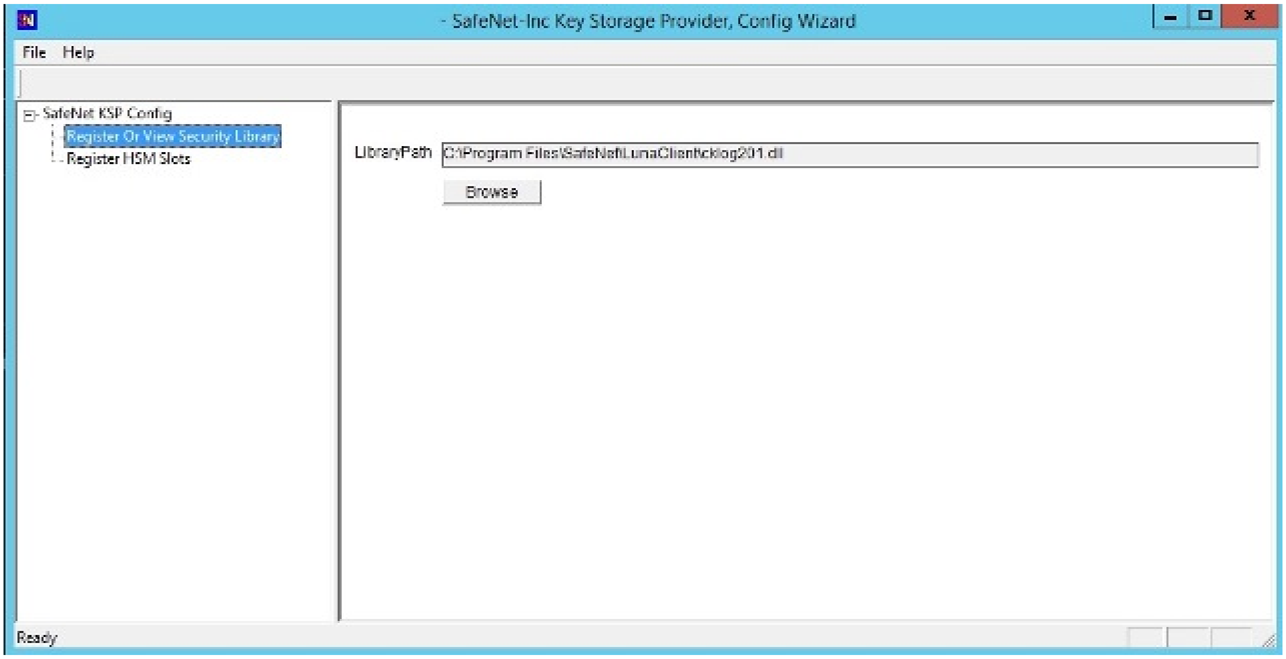
1. Navigate to the KSP installation directory. Execute **KspConfig.exe**.

2. Double-click **Register Or View Security Library** on the left side of the pane.


- SafeNet-Inc Key Storage Provider, Config Wizard
File Help
SafeNet KSP Config
Register Or View Security Library
Register HSM Slots
Browse
Ready

LibraryPath C:\Program Files\SafeNet\LunaClient\cklog201.dll

3. Click **Browse.** Select the cryptoki.dll file, available in the SafeNet Luna Client installation folder or HSMoD service client package. Click **Register.**

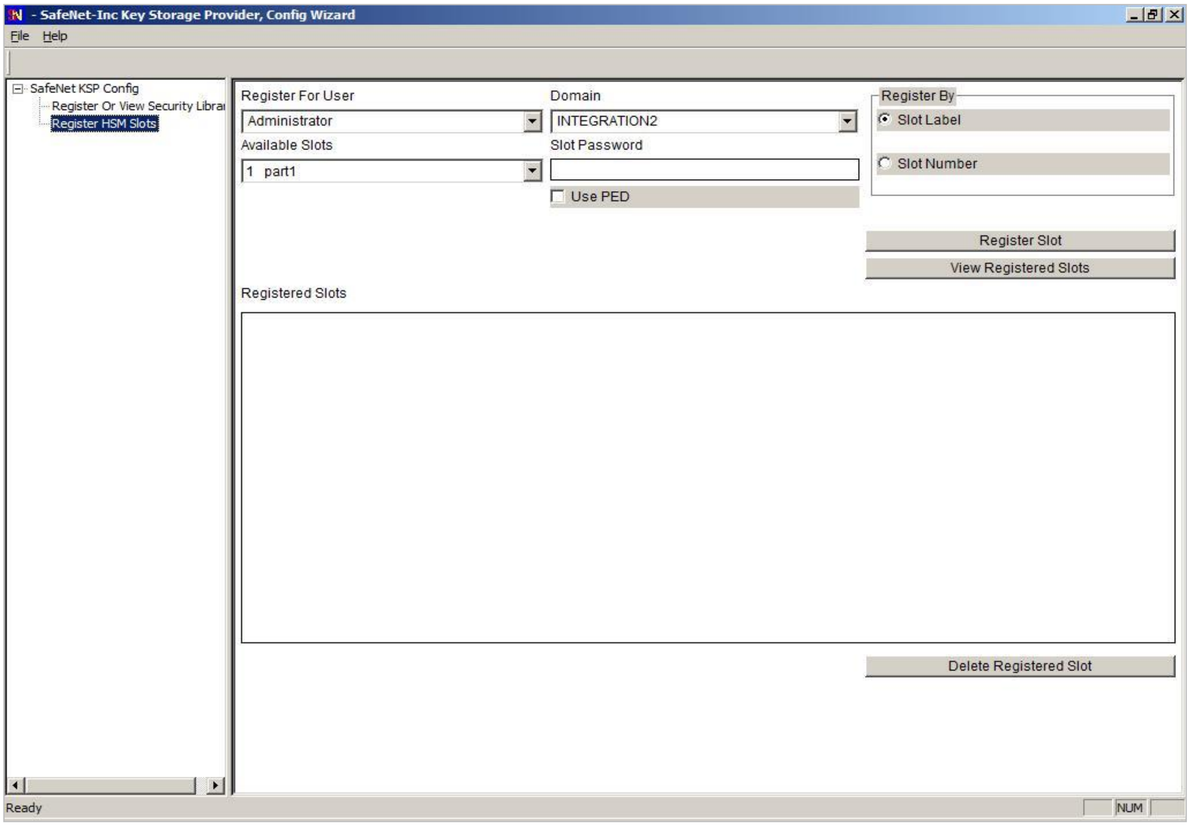

- SafeNet-Inc Key Storage Provider, Config Wizard
File Help
SafeNet KSP Config
Register Or View Security Library
Register HSM Slots
Browse
Ready

LibraryPath C:\Program Files\SafeNet\LunaClient\cklog201.dll

4. On successful registration a **Success!** message displays. Click **OK**.

5. Double-click **Register HSM Slots** on the left side of the pane.

6. Register the slot for the Administrator 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 relevant service or partition.
   d. Enter the **Slot Password**
   e. Click **Register Slot**.
   f. On successful registration, a **Success!** message displays. Click **OK**.



- SafeNet-Inc Key Storage Provider, Config Wizard

Register For User: Administrator

Domain: INTEGRATION2

Available Slots: 1 part1

Slot Password:

☐ Use PED

Register By: ● Slot Label ○ Slot Number

7. Register the same service or partition for the **NT_AUTHORITY\SYSTEM** user.
   a. Open the **Register for User** drop-down menu and select **NT_AUTHORITY\SYSTEM**.
   b. Open the **Domain** drop-down menu and select your domain.
   c. Open the **Available Slots** drop-down menu and select the relevant service or partition.
   d. Enter the Slot Password.
   e. Click Register Slot.
   f. On successful registration, a **Success!** message displays. Click **OK**.

NOTE: The SafeNet Luna HSM or 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.

To register the SafeNet CSP

SafeNet Luna CSP should be installed on the OCSP Server machine to use CSP generated keys for OCSP signing.

NOTE: If you want to use CSP generated OCSP signing keys you must register the SafeNet CSP. If you are configuring the Microsoft OCSP on multiple systems, the CSP must be configured and registered on both the Certificate Authority and OCSP server systems.

1. Log on to the OCSP Server as domain administrator.
2. Run the command, register.exe to register Luna CSP. The general form of command is:

   ```
   C:\Program Files\SafeNet\LunaClient\CSP>register.exe
   ```

3. Provide the partition password when asked.
4. List the Luna Cryptographic Services for Microsoft Windows and verify that the Luna CSP is available.

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

5. Restart the server for the changes to take effect.

2 Integrating Microsoft Online Certificate Service Protocol with SafeNet HSM (Windows Server 2008 R2)

Configuring SafeNet HSM for Online Certificate Status Protocol

To set up SafeNet Luna HSMs for Online Certificate Status Protocol (OCSP), complete the following:

- Setting up an Enterprise Root certificate authority
- Installing the Online Responder service
- Configuring the CA to issue the OCSP Response Signing Certificates
- Creating a Revocation Configuration
- Verifying Auto-enrollment
- Verifying the OCSP integration

Setting up an Enterprise Root certificate authority

An enterprise root CA issues certificates to the Online Responder service, client computers, and publish certificate information to the Active Directory Domain Services (ADDS).

> **NOTE:** If you are installing both the CA and OCSP on the same machine, you need to log in to OCSPSERV to install the CA role. For more information about the machines utilized in this setup see Setup Microsoft OCSP

To set up an Enterprise Root certificate authority

1. Log on to **OCSPCA** as a Domain Administrator.
2. From the **Start menu**, select **Control Panel** > **Administrative Tools** > **Server Manager**.
3. In the **Roles Summary** section (in the right pane of the window), click **Add Roles**.
4. On the welcome screen, click **Next**.
5. On the **Select Server Roles** window displays, select the **Active Directory Certificate Services** check box and click **Next** twice.

6. Select the **Certification Authority** and **Certification Authority Web Enrollment** check boxes and click **Next**.
7. In the **Specify Setup Type** window, select the **Enterprise** check box. Click **Next**.
8. On the **Specify CA Type** window, select the **Root CA** check box. Click **Next**.
9. On the **Setup Private Key** window, select the **Create a new private key** check box and click **Next**.
10. On the **Configure Cryptography for CA** window, open the **Cryptographic Provider** drop-down menu and select and set up the provider you wish to use for the CA.

    The following SafeNet Cryptographic Providers are available for use:

> **NOTE:** If the following objects are unavailable under the Cryptographic Provider drop-down menu then verify your KSP/CSP Registration.

```
- RSA#SafeNet Key Storage Provider
- DSA#SafeNet Key Storage Provider
- ECDSA_P256#SafeNet Key Storage Provider
- ECDSA_P384#SafeNet Key Storage Provider
- ECDSA_P521#SafeNet Key Storage Provider
```

> **NOTE**: When using SafeNet providers, ensure that you use a ‘sha’ hashing algorithm.

11. When you have selected and setup the Cryptographic Provider, click **Next.**
12. On the Configure CA Name, set the **Validity Period** and **Certificate Database** sections, or accept the default values and click **Next**.
13. The **Confirm Installation Selections** window displays. Verify that the CA you are about to configure is appropriate.
14. When setup completes, verify there are no issues with the installation. Click **Close.**

Installing the Online Responder service

The Online Responder Service is required to complete Online Certificate Service Protocol operations.

To install the Online Responder service

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start menu**, select **Control Panel** > **Administrative Tools** > **Server Manager**.
3. Expand the Roles section (in the left-hand section) and click on **Active Directory Certificate Services**. In the bottom right-hand section, click **Add Role Services**.
4. In the Select Role Services section, select **Online Responder**. A prompt displays asking you to install IIS 7.
5. Click **Add Required Role Services** and when the prompt disappears click **Next** twice.
6. In the **Select Role Services** window for Web Server (IIS), accept the default values and click **Next**.
7. In the **Confirm Installation Selections** window, check that everything is correct and click **Install**.
8. When setup completes, verify there are no issues with the installation. Click **Close.**

Configuring the CA to issue the OCSP Response Signing Certificates

To configure the CA to support the Online Responder Service you must configure the certificate templates and issuing properties for OCSP Response Signing Certificates depending on your KSP or CSP registration. To configure the CA to issue OCSP Response Signing certificates you must complete the following:

- To configure certificate templates for a test environment
- To configure OCSP to access the SafeNet Key Storage Provider
- To configure certificate templates using SafeNet CSP
- To configure the CA to support the Online Responder service

NOTE: If you have installed the CA and OCSP on same machine then you need to carry out these steps on OCSPSERV to configure OCSP Response Signing Certificate.

To configure certificate templates for a test environment

1. Log on to **OCSPCA** 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. In the mmc console, select **File** > **Add/Remove Snap-in…**
5. In the **Add or Remove Snap-Ins** dialog box, find the **Certificate Templates** snap-in (under the Available snap-ins section) and select it.
6. Click **Add**, and then click **OK**.
7. Under Console Root, expand the **Certificate Templates** snap-in.
8. Scroll down the central list until you locate the **OCSP Response Signing template**. Right-click the **OCSP Response Signing Template** and click **Properties**.
9. In the pop-up dialog box, select the **General** tab.
10. Select **Publish Certificate** in Active Directory check box.
11. Set the **Validity period** and **Renewal period**.

NOTE: We recommend setting the **Validity period** and **Renewal period** for four hours and one hour to test **Auto Renewal**.

12. Click the **Security** tab and click **Add**.
13. In the **Select User, Computers, or Groups** dialog, type the name of the machine which is hosting the Online Responder service (**OCSPSERV**).
14. Click **OK**. It should not be able to locate the machine, instead another dialog displays.
15. In this dialog, click **Object Types**. Ensure that the **Computers** check box is selected, and click **OK**.
16. In the **Select User, Computers, or Groups** dialog, re-enter **OCSPSERV**. Click **OK**.

    The machine hosting the Online Responder will be added to the Group and user names area under the Security tab.

17. Select **OCSPSERV** in the Group and user names area.
18. In the Permissions area, ensure that the **Read**, **Enroll**, and **Autoenroll** check boxes are selected.
19. Verify that the **Read, Write, Enroll, and Autoenroll** check boxes are selected for the **Domain Admins** and **Enterprise Admins** users.
20. Click **Apply** and then **OK**.

To configure OCSP to access the SafeNet Key Storage Provider

1. Log on to **OCSPCA** as a domain administrator.
2. From the **Start** menu, select **Run.**
3. Type **mmc** in the **Run** dialog box and click **OK**.
4. In the **mmc** console, select **File** and then click **Add/Remove Snap-in**.
5. In the **Add or Remove Snap-Ins** dialog box, select **Certificate Templates snap-in** (under the Available snap-ins section). Click **Add** and then click **OK**.
6. Click **Certificate Templates snap-in under Console Root** and expand it. Listed in the middle section will be all the available certificate templates that you can make your CA issue. Scroll down the list until you locate the **OCSP Response Signing template**.
7. Right-click the **OCSP Response Signing template** and click **Properties**.
8. On the dialog, click on the **Cryptography tab**.
9. Select the **Requests must use one of the following providers** radio button.
10. The dialog below the radio button becomes active. Select SafeNet **Key Storage Provider**.
11. Click **Apply** and then **OK**.

To configure certificate templates using SafeNet CSP

If you want to generate OCSP signing keys using the SafeNet CSP complete the following procedure. Ensure that you have registered the CSP on both the OCSPCA and OCSPSERV systems.

1. Log on to **OCSPCA** as a domain administrator.
2. Click the **Search** menu, type **MMC** and press **Enter** to open the console.
3. In the **mmc** console, select **File** and then click **Add/Remove Snap-in…**
4. In the **Add or Remove Snap-Ins dialog box**, find the **Certificate Templates** snap-in (under the Available snap-ins section) and select it.
5. Click **Add**, and then click **OK**.
6. Under Console Root, expand the **Certificate Templates** snap-in.
7. Scroll down the list until you locate the **OCSP Response Signing template**, right-click it and click **Duplicate Template** and select **windows Server 2003 Enterprise.**
8. Click the **General** tab. Enter the **name of template** in Template display name.
9. Select the **Publish Certificate in the Active Directory** check box.
10. Set the **Validity period** and **Renewal period**.

NOTE: We recommend setting the **Validity period** and **Renewal period** for four hours and one hour to test **Auto Renewal**.

11. Click the **Security** tab and click **Add**.
12. In the **Select User, Computers, Service Accounts, or Groups** dialog, enter the name of the machine (In this case **OCSPSERV)** which is hosting the Online Responder service.
13. Click **OK**. It should not be able to locate the machine, instead dialog displays.
14. In this dialog box, click **Object Types,** ensure that the **check-box next to Computers** is selected and click **OK**.
15. In the **Select User, Computers, or Groups** dialog, re-enter OCSPSERV. Click **OK**.

    The machine hosting the Online Responder will be added to the Group and user names area under the **Security** tab.
16. Click **OCSPSERV** in the Group and user names area.
17. In the **Permissions area**, ensure that the **Read**, **Enroll** and **Autoenroll** check boxes are **ticked**.
18. Verify that the **Read, Write, Enroll, and Autoenroll** check boxes are selected for the **Domain Admins** and **Enterprise Admins** users.
19. Click the **Request Handling** tab and click on **CSPs…** button.
20. Select the Requests must use one of the following CSPs radio button.
21. The dialog below the radio button becomes active. Select **Luna Cryptographic Services for Microsoft Windows**.
22. Click **Apply** and then **OK**.

To configure the CA to support the Online Responder service

1. Log on to **OCSPCA** as a domain administrator.
2. From the **Start menu** select **Control Panel** -> **Administrative Tools** -> **Certification Authority**.
3. In the console tree (left-hand section), click on the **CA**. (It has a computer and a green tick next to it.)
4. Open the **Action menu** and click **Properties**.
5. Click the **Security** tab and select **Add**.
6. In the **Select User, Computers, or Groups** dialog, enter the name of the machine which is hosting the Online Responder service (**OCSPSERV**).
7. Click **OK**. The system should not be able to locate the machine, instead another dialog displays.
8. In this dialog, click **Object Types**, select the **Computers** check box and click **OK**.
9. In the **Select User, Computers, or Groups** dialog, re-enter OCSPSERV. Click **OK**.

    The machine hosting the Online Responder will be added to the Group and user names area under the **Security** tab.
10. Click **OCSPSERV** in the Group and user names area.
11. In the **Permissions area**, ensure that the **Request Certificate** check box is selected.
12. For **Domain Admins**, **Enterprise Admins,** and **Administrators**, make sure that **Issue and Manage Certificate**, **Manage CA**, **Request Certificate check boxes** are selected.
13. Select the **Extensions tab**. In the **Select extension** list, click **Authority Information Access (AIA).**
14. Click **Add.** In the **Add Location** dialog box, Enter the URL in the below format:

    ```
    http://<nameofcomputerhostingOCSPhere>/ocsp.
    ```

    ```
    For example, the address when using
    OCSP would be http://OCSPSERV/ocsp.
    ```

15. Click **OK**.
16. On the **Extensions tab**:
    a. Ensure that the recently added **URL** is highlighted.
    b. Ensure that the Include in the AIA extension of issued certificates and Include in the online certificate status protocol (OCSP) extension check boxes are selected.
17. Click **Apply** and let the service restart. Click **OK**.
18. In the console tree of the **Certification Authority snap-in**, right-click **Certificate Templates**, and then click **New Certificate Templates to Issue**.
19. In **Enable Certificates Templates**, select the **OCSP Response Signing template** and any other previously configured certificate templates. Click **OK**.
20. Open Certificate Templates in the Certification Authority and verify that the modified certificate templates are included in the list.

Creating a Revocation Configuration

A revocation configuration includes all of the settings that are needed to respond to status requests regarding certificates that have been issued by using a specific CA key. Creating a revocation configuration involves the following:

- Modifying the Online Responder service to use SafeNet HSMs
- Setting up the Revocation Configuration

Modifying the Online Responder service to use SafeNet HSMs

To use OCSP in conjunction with SafeNet Luna HSMs or HSMoD services, you must configure the Online Responder service to use the HSM to protect the OCSP signing keys.

To modify the Online Responder service to use SafeNet HSMs

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start menu** select **Control Panel** -> **Administrative Tools** -> **Services**.
3. Locate the **Online Responder Service** in the list of services.
4. **Right-click** on the **Online Responder Service** and select **Properties**.
5. In the dialog box select the **Log on** tab.
6. Under the **Log on as** heading, hover over the radio button next to Local System account and select the **Allow service to interact with desktop** check box.
7. Click **Apply** and then **OK**.
8. Return to the services window. Right-click on the **Online Responder Service** and click **Restart**.

Setting up the Revocation Configuration

Once the Online Responder service is configured to use the HSM to protect the OCSP signing keys you can set up the certificate revocation configuration.

To set up the revocation configuration

1. Log on to **OCSPSERV** as a domain administrator.

2. From the **Start menu** select **Control Panel** -> **Administrative Tools** -> **Online Responder Management**.
3. In the left-hand pane select **Revocation Configuration**.
4. In the right-hand pane, under **Actions**, click **Add Revocation Configuration**. A dialog window displays.
5. On the **Getting started with adding a revocation configuration section** click **Next**.
6. In the **Name the Revocation Configuration** section, enter a name for the configuration in the text box. Click **Next.**
7. In the **Select CA Certificate Location** section, ensure that the **Select a certificate for an Existing enterprise CA** radio button is selected and click **Next**.
8. In the **Choose CA Certificate** section, ensure that the **Browse CA certificates published in Active Directory** radio button is selected and then click **Browse**.
9. In the **Select Certification Authority** dialog box, select the **CA authority** (in this case **OCSPCA**) and click **OK**. Click **Next**.
10. In the Select Signing Certificate section, accept the default setting **Automatically select a signing certificate** and make select the **Auto-enroll for OCSP signing certificate** check box. Click **Next**.
11. In the Revocation Provider section, click **Finish**.

    Once the wizard completes, the Revocation Configuration **Status Box** displays the Online Responder status. The status should display **Bad Signing on Array Controller.**
12. To correct this, click on **Revocation Configuration** in the left hand pane. The certificate displays in the right-pane.
13. Right-click the **certificate** and select **Edit Properties**.
14. Click on the **Signing tab**. Deselect the **Do not prompt for credentials for cryptographic operations** check box. Click **OK**.
15. Return to the Online Responder Management tool. Open **Actions** and click **Refresh**.
16. In the left-hand pane click on **Online Responder: Computer Name** and verify that the Revocation Configuration **Status Box** displays **Working**.

Verifying Auto-enrollment

You need to verify that the certificate will auto-renew after the expiry. Verification of auto renewal involves the expiration of the generated certificate and renewal of the certificate using new key pair. You can verify that auto-enrollment of a newly generated certificate is operating successfully by completing the following procedures:

- Viewing a generated certificate and key pair
- Viewing a renewed certificate and key pair

Viewing a generated certificate and key pair

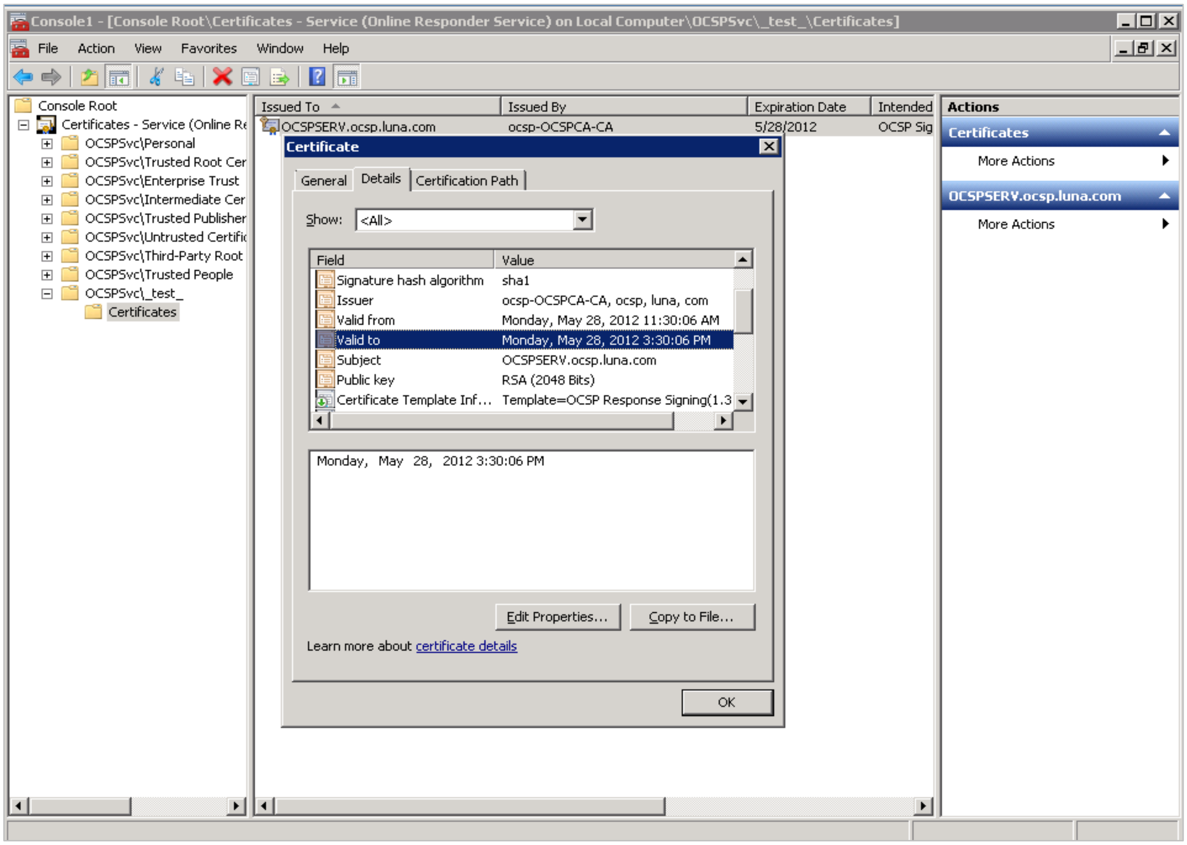
To verify that auto-enrollment is operating properly you need to verify that the service is capable of generating a certificate and key pair.

To view a generated certificate and key pair

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start menu**, select **Run**.
3. In the Run dialog, type **mmc** and click **OK**.
4. In the **mmc** console that displays, select **File** > **Add/Remove Snap-in…**
5. In the **Add or Remove Snap-Ins** dialog box, find the **Certificate snap-in** (under the Available snap-ins section) and select it.
6. Click **Add**, select **Service Account** and click **Next**.
7. Select **Local Computer**, and click **Next**.
8. Under **Certificate Snap-in**, click on the **Online Responder Services** in Service Account and click **Finish**.
9. Click **OK** and expand the **Online Responder Services** tree.
10. Expand the **OCSPSvc\CertificateName** (For Example: OCSPSvc_test_) and double click on **Certificates**.
11. A certificate will be shown, double click on the certificate to display.
12. Click the **Details** tab and verify the **Valid From** and **Valid To** date of certificate. It states the certificate expires **in next four hours**.

    You can connect with the SafeNet Luna HSM appliance and verify the **key pair** which was generated corresponds to the certificate.

    The generated certificate and key pair are shown in the screenshots below:



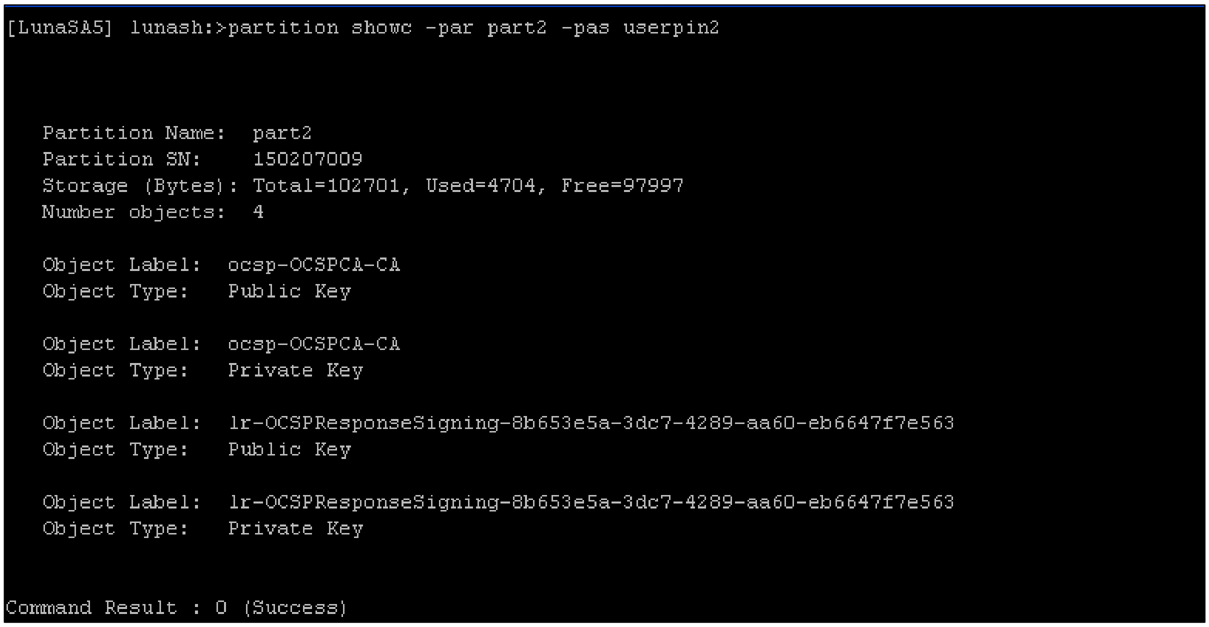
Console1 - [Console Root\Certificates - Service (Online Responder Service) on Local Computer\OCSPSvc_test_\Certificates]

Issued To	Issued By	Expiration Date	Intended
OCSPSERV.ocsp.luna.com	ocsp-OCSPCA-CA	5/28/2012	OCSP Sig

Field	Value
Signature hash algorithm	sha1
Issuer	ocsp-OCSPCA-CA, ocsp, luna, com
Valid from	Monday, May 28, 2012 11:30:06 AM
Valid to	Monday, May 28, 2012 3:30:06 PM
Subject	OCSPSERV.ocsp.luna.com
Public key	RSA (2048 Bits)
Certificate Template Inf…	Template=OCSP Response Signing(1.3

Monday, May 28, 2012 3:30:06 PM

The SafeNet Luna HSM appliance shows the Key Pair for CA certificate and Online Responder Service Certificate. If you are using an HSMoD service you can verify the partition contents by executing **partition contents** inside of **lunacm**.



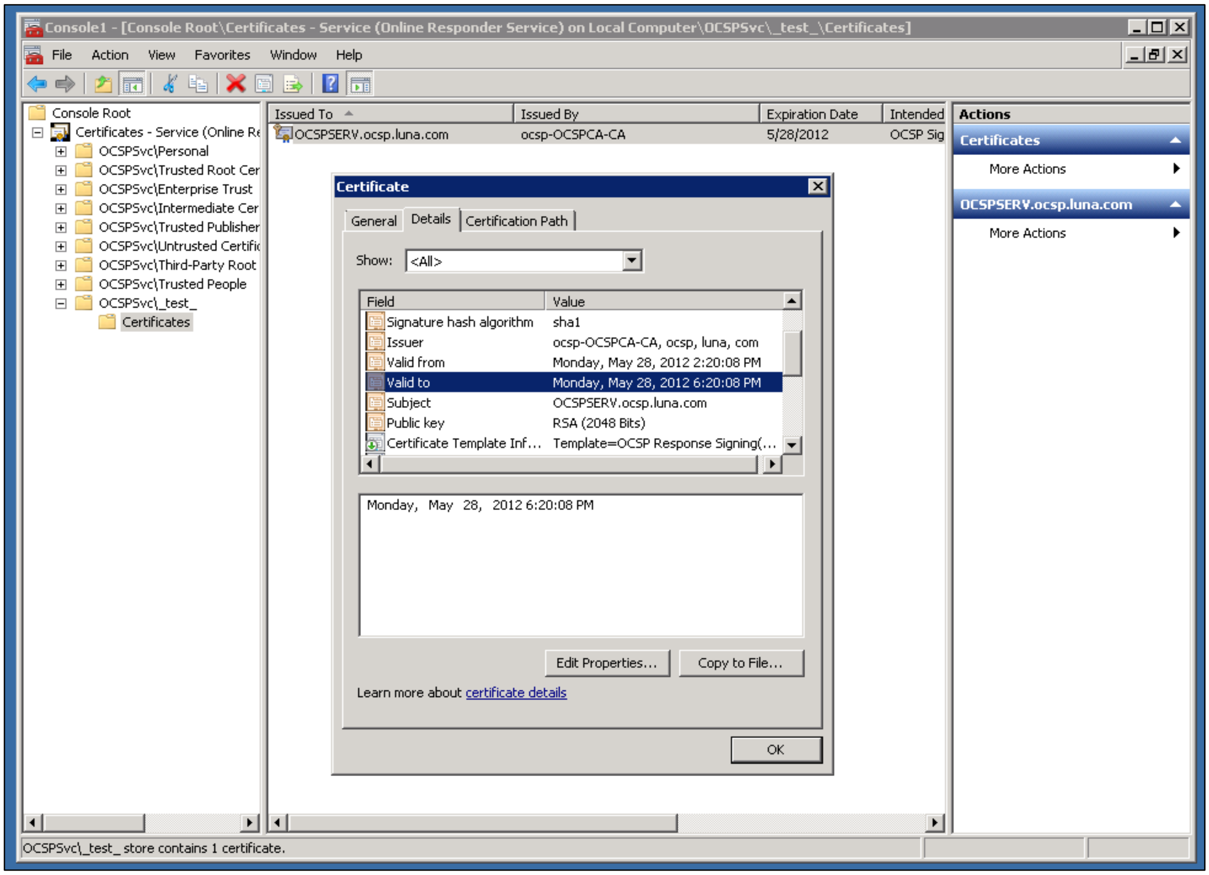
```
[LunaSA5] lunash:>partition showc -par part2 -pas userpin2



   Partition Name:  part2
   Partition SN:    150207009
   Storage (Bytes): Total=102701, Used=4704, Free=97997
   Number objects:  4

   Object Label:  ocsp-OCSPCA-CA
   Object Type:   Public Key

   Object Label:  ocsp-OCSPCA-CA
   Object Type:   Private Key

   Object Label:  lr-OCSPResponseSigning-8b653e5a-3dc7-4289-aa60-eb6647f7e563
   Object Type:   Public Key

   Object Label:  lr-OCSPResponseSigning-8b653e5a-3dc7-4289-aa60-eb6647f7e563
   Object Type:   Private Key


Command Result : 0 (Success)
```

You can see that only one key pair is generated for OCSP Response Signing. You need to wait for four hours to verify the auto-renewal of the certificate because the validity period of certificate is four hours.

Viewing a renewed certificate and key pair

After four hours have passed, you can verify that the **Valid From** and **Valid To** dates of the certificate have been updated. The new certificate is valid for the next four hours, and a new key pair for the renewed certificate has been generated.

Start -> Run -> MMC -> File -> Add/Remove Snap-in… -> Certificate -> Add -> Service Account -> Next -> Local Computer -> Online Responder Service -> Finish -> OK



Issued To	Issued By	Expiration Date	Intended
OCSPSERV.ocsp.luna.com	ocsp-OCSPCA-CA	5/28/2012	OCSP Sig

Field	Value
Signature hash algorithm	sha1
Issuer	ocsp-OCSPCA-CA, ocsp, luna, com
Valid from	Monday, May 28, 2012 2:20:08 PM
Valid to	Monday, May 28, 2012 6:20:08 PM
Subject	OCSPSERV.ocsp.luna.com
Public key	RSA (2048 Bits)
Certificate Template Inf…	Template=OCSP Response Signing(…

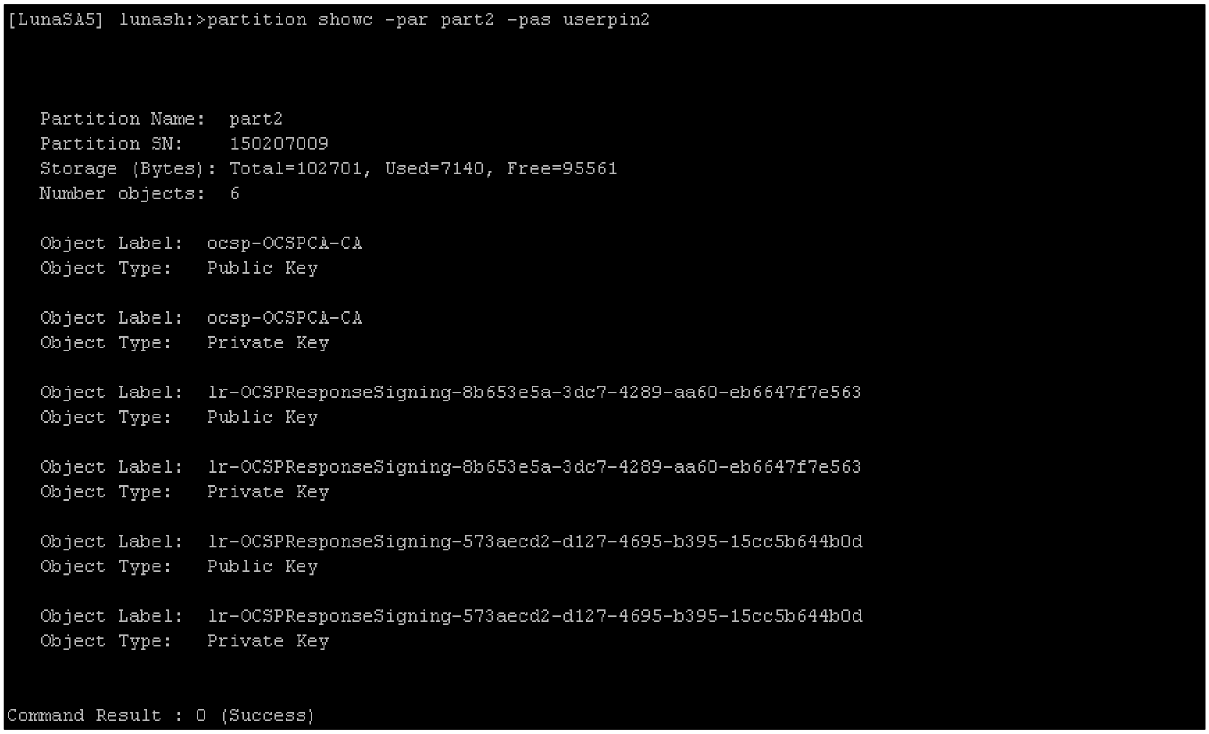
Monday, May 28, 2012 6:20:08 PM

Learn more about certificate details

OCSPSvc_test_ store contains 1 certificate.

This demonstrates that the certificate renews automatically every four hours. We had it set for testing purposes, but in a production environment we recommend setting the validity periods as required by your organization’s security infrastructure.

A new key pair has been generated on the SafeNet Luna HSM appliance when certificate is renewed.



```
[LunaSA5] lunash:>partition showc -par part2 -pas userpin2



   Partition Name:  part2
   Partition SN:    150207009
   Storage (Bytes): Total=102701, Used=7140, Free=95561
   Number objects:  6

   Object Label:  ocsp-OCSPCA-CA
   Object Type:   Public Key

   Object Label:  ocsp-OCSPCA-CA
   Object Type:   Private Key

   Object Label:  lr-OCSPResponseSigning-8b653e5a-3dc7-4289-aa60-eb6647f7e563
   Object Type:   Public Key

   Object Label:  lr-OCSPResponseSigning-8b653e5a-3dc7-4289-aa60-eb6647f7e563
   Object Type:   Private Key

   Object Label:  lr-OCSPResponseSigning-573aecd2-d127-4695-b395-15cc5b644b0d
   Object Type:   Public Key

   Object Label:  lr-OCSPResponseSigning-573aecd2-d127-4695-b395-15cc5b644b0d
   Object Type:   Private Key


Command Result : 0 (Success)
```

Verifying the OCSP integration

You can verify that the OCSP is operating properly following the integration with SafeNet Luna HSM or HSMoD service.

To generate a certificate request

1. Log on to the **OCSPCL** machine and generate a certificate request. We recommend using the below template structure. (You can try to use alternative vendors' cryptographic service providers, instead of the SafeNet Key Storage provider or SafeNet CSP).

   ```
   [Version]
   Signature = "$Windows NT$"
   [NewRequest]
   Subject = "C=IN,CN=OCSPCL"
   HashAlgorithm = SHA256
   KeyAlgorithm = RSA
   KeyLength = 2048
   ProviderName = "Provider_to_be_used"
   KeyUsage = 0xf0
   MachineKeySet = True
   RequestType = PKCS10
   [EnhancedKeyUsageExtension]
   OID = 1.3.6.1.5.5.7.3.1
   [Extensions]
   1.3.6.1.5.5.7.48.1.5 = Empty
   ```

2. Copy and paste the above template into a Notepad **.txt** file. Ensure that the Provider Name variable is provided with the quotation marks around it.

3. Once the template has been successfully setup, save it as `test.inf` on **C:\ drive.**
4. Open the command prompt window and go to the local drive, in this case C:\. Type `certreq -new test.inf test.req` command in the command prompt, a certificate request called `test.req` generates and is placed on the **C:\** drive.
5. Execute `certreq -submit -attrib "CertificateTemplate:WebServer" test.req` command in a command prompt. A pop up window displays confirming which CA to use. Click the **OCSPCA** entry and click **OK**. A dialog displays to save the certificate to a file.
6. Save the certificate file and click **OK**. After a short pause, a message "**Certificate Successfully Generated"** displays on the command prompt and a certificate file called test.cer generates on the **C:\** drive.

To test the certificate's origin

1. Log on to **OCSPCA** and go to the Certification Authority tool by navigating to **Start** > **Control Panel** > **Administrative Tools** > **Certification Authority**.
2. In the **Certification Authority snap-in**, publish a new CRL by clicking **Certification Authority (Computer)/CA name/Revoked Certificates** in the console tree. Then, right-click on the **Revoked Certificates folder**, point to **All Tasks**, and click **Publish**.
3. Open the Certification Authority snap-in and right-click on the **CA**, to remove all CRL distribution point extensions from the issuing CA.
4. In the dialog click **Properties**.
5. On the **Extensions tab**, confirm that **Select extension is set to CRL Distribution Point (CDP).**
6. Click any CRL distribution points that are listed, click **Remove**, and click **OK**.
7. Now click **Apply**. A **pop-up** box displays stating that you need to **restart** the service.
8. Click **OK** and watch the service **restart**.
9. Using the certificate called `test.cer` that was generated earlier on the OCSPCL machine, verify that clients can still obtain revocation data. On **OCSPCL**, execute the `certutil -url test.cer` command.
10. In the **URL Retrieval Tool** dialog box, select the radio button next to **CRLs (From CDP)** and click **Retrieve**.
11. Select the radio button **OCSP (From AIA)** and click **Retrieve**. The list should contain an OCSP entry showing the web address of your OCSP server. If it is working correctly, the word **Verified** displays in the first column in the list.
12. Select the radio button **Certs (from AIA)** and click **Retrieve**. One or two entries should be listed, with **Verified** next to them. If Certificate Authority Web Enrollment is not installed on the CA, an entry with AIA may display as Failed. However, as long as one of the entries in the Certs (from AIA) section reads **Verified** there should be no problems with the set-up.

NOTE: If Certificate Authority Web Enrollment is not installed on the CA, an entry with AIA may display as Failed. However, as long as one of the entries in the Certs (from AIA) section reads Verified there should be no problems with the set-up.

To verify the OCSP integration

1. Open a command prompt window and select the local drive, in this case **C:\.** Execute

```
certutil -verify test.cer > test.txt
```

2. When the `certutil -verify test.cer > test.txt` command completes, open the **test.txt** file on C:\. The file should contain the following information:

```
Issuer:
CN=Integration-OCSPSERV-CA
DC=Integration
DC=com
Subject:
CN=OCSPCL
C=IN
Cert Serial Number: 611362e4000000000003

 dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x20000000)
 dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000)
 ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000)
 HCCE_LOCAL_MACHINE
 CERT_CHAIN_POLICY_BASE
 -------- CERT_CHAIN_CONTEXT --------
 ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
 ChainContext.dwRevocationFreshnessTime: 17 Minutes, 42 Seconds

 SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
 SimpleChain.dwRevocationFreshnessTime: 17 Minutes, 42 Seconds

 CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0
 Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
 NotBefore: 5/23/2013 3:55 PM
 NotAfter: 5/23/2015 3:55 PM
 Subject: CN=OCSPCL, C=IN
 Serial: 611362e4000000000003
 Template: WebServer
 f0 e3 6b 9f f4 59 a6 64 18 f4 6f f6 a1 90 52 5b a3 3a 40 8c
 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)
 Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
 CRL 02:
 Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
 c1 32 12 a5 2f 82 d9 69 06 c0 28 1c 75 9d b1 5b 4c c5 4f 6d
 Delta CRL 02:
 Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
 b1 63 03 a3 b8 d0 c5 41 7c d9 2c 3f ae 87 b4 a3 27 bd e7 73
 Application[0] = 1.3.6.1.5.5.7.3.1 Server Authentication

 CertContext[0][1]: dwInfoStatus=10c dwErrorStatus=0
 Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
 NotBefore: 5/23/2013 3:30 PM
 NotAfter: 5/23/2018 3:40 PM
 Subject: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
  Serial: 6236c444f91af2a04fafdd311517307a
 c3 3b 1c 6a 7f 07 3d f9 63 2a d1 fd 62 ca eb 16 e5 04 0a d3
 Element.dwInfoStatus = CERT_TRUST_HAS_NAME_MATCH_ISSUER (0x4)
 Element.dwInfoStatus = CERT_TRUST_IS_SELF_SIGNED (0x8)
 Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)

 Exclude leaf cert:
 e9 a1 9d 87 ea 5f 8b 9f b1 cc 2d d5 3a 55 f2 d1 12 14 b8 a2
 Full chain:
 e5 79 bc 47 e8 b8 05 11 fa e4 0d 47 a8 3e 73 99 3d df cf 4f
 ------------------------------------
 Verified Issuance Policies: None
 Verified Application Policies:
 1.3.6.1.5.5.7.3.1 Server Authentication
 Leaf certificate revocation check passed
 CertUtil: -verify command completed successfully.
```

3. Ensure that the `certutil -verify test.cer > test.txt` commands output includes the following:

   ```
   Verified Issuance Policies: None
   Verified Application Policies:
   1.3.6.1.5.5.7.3.1 Server Authentication
   Leaf certificate revocation check passed
   CertUtil: -verify command completed successfully.
   ```

   These commands demonstrate that the OCSP server is operating correctly without any errors. The most important component of the above example is the **Leaf certificate revocation check passed** line as this demonstrates that the OCSP service is returning the certificate status as **Good**.

   If the log generated by the verify command does not include the above section (or similar) and has errors in the output, we recommend you restart the OCSP server and client machine, and run the **verify** command again on the certificate file.

3

Integrating Microsoft OCSP with SafeNet HSM (Windows Server 2016/2012 R2/2012)

Configuring SafeNet HSM for Online Certificate Status Protocol

To setup SafeNet Luna HSMs for Online Certificate Status Protocol (OCSP), complete the following steps:

- Setting up an Enterprise Root certificate authority
- Installing the Online Responder service
- Configuring the CA to issue the OCSP Response Signing Certificates
- Creating a Revocation Configuration
- Verifying Auto-enrollment
- Verifying the OCSP Integration

Setting up an Enterprise Root certificate authority

An enterprise root CA is used to issue certificates to the Online Responder service, client computers, and publish certificate information to the Active Directory Domain Services (ADDS).

NOTE: If you are installing both the CA and OCSP on the same machine, you need to log on to OCSPSERV to install the CA role.

To install ADCS and CA role

1. Log on to **OCSPCA** as a Domain Administrator.
2. From the **Start menu**, select **Administrative Tools** and click **Server Manager**.
3. In the Server Manager Dashboard (in the right pane of the window), click **Manage** and then select **Add Roles and Features.**
4. In the **Add Roles and Features Wizard**, click **Next**.
5. On the Installation Type page select the **Role-based or feature-based installation** check box. Click **Next**.
6. On the Server Selection screen select a server from the server pool and select the listed server then click **Next**.

7. Select **Active Directory Certificate Services** from the Roles list. The Add Features dialog displays. Click **Add Features**. Click **Next.**
8. On the Features page, click **Next.**
9. On the ADCS page, click **Next**.
10. On the **Role Services page**, select the **Certificate Authority** and **Certificate Authority Web Enrollment** check boxes in the **Role Services** list. The Add Features dialog displays.
11. Click **Add Features** and click **Next**.
12. On the Web Server Role (IIS) page click **Next**.
13. On the Role Services page click **Next**.
14. Select the **Restart the destination server automatically if required** check box. A confirmation message displays, click **Yes**.
15. Click **Install** on the Confirmation page and wait to finish the installation.

To configure ADCS and CA role

1. If continuing from the last procedure, click **Configure Active Directory Certificate Server** on the destination server. Alternatively, you can open the ADCS configuration wizard by clicking the **Notification Flag** and configuring the server role.

   The ADCS Configuration Wizard displays.
2. On the **Credentials** page, click **Next**.
3. On the Role services page select the **Certificate Authority** and **Certification Authority Web Enrollment** check boxes. Click **Next**.
4. On the Setup Type page select **Enterprise CA** . Click **Next**.
5. On the CA Type page select the **Root CA** radio button and click **Next**. Click **Next**.
6. On the Private Key page select the **Create a new private key** check box. Click **Next**.
7. In the **Cryptography for CA** window, select and set up the provider you wish to use for the CA.

   The following SafeNet Cryptographic Providers are available for use:

   NOTE: If the following objects are not available under the Cryptographic Provider drop-down menu you need to verify your KSP/CSP Registration.

   ```
   - RSA#SafeNet Key Storage Provider
   - DSA#SafeNet Key Storage Provider
   - ECDSA_P256#SafeNet Key Storage Provider
   - ECDSA_P384#SafeNet Key Storage Provider
   - ECDSA_P521#SafeNet Key Storage Provider
   ```

   NOTE: When using SafeNet providers ensure that you use a ‘sha’ hashing algorithm.

8. When you have selected and setup the Cryptographic Provider, click **Next**.
9. On the Configure CA Name page enter the **CA Name** or accept the default CA name. Click **Next**.
10. On the Validity Period page specify the certificate validity period. Click **Next**.

11. Specify the database location or accept the default location on the Certificate Database page and click **Next**.
12. Verify that the CA you are about to configure is appropriate. Click **Configure** and wait for the confirmation message. If everything is correct, the Configuration succeeded message will display when the configuration completes.
13. Click **Close** to exit the ADCS Configuration wizard.

Installing the Online Responder service

The Online Responder Service is required to complete Online Certificate Service Protocol operations.

To install the Online Responder Service

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start menu**, select **Administrative Tools** and click **Server Manager**.
3. In the **Server Manager Dashboard** (in the right pane of the window), click **Manage** and then click **Add Roles and Features**.
4. In the **Add Roles and Features Wizard**, click **Next**.
5. On the Installation Type page select the **Role-based or feature-based installation** check box. Click **Next**.
6. On the Server Selection screen click the **Select a server from the server pool** check box and select the listed server. Click **Next**.
7. Select the **Active Directory Certificate Services** check box in the Roles list. The **Add features** dialog displays. Click **Add Features** to add the required features for the server role. Click **Next.**
8. On the Features page click **Next**.
9. On the ADCS page click **Next**.
10. On the Role Services page deselect the **Certification Authority** check box and select the **Online Responder check box.** The **Add Features** dialog displays. Click **Add Features** to add the required features for the server role. Click **Next**.
11. On the features page click **Next**.
12. Select the **Restart the destination server automatically if required** check box. A confirmation message displays. Click **Yes**.
13. On the Confirmation page click **Install**.
14. Click **Configure Active Directory Certificate Server** on the destination server. The **ADCS Configuration Wizard** displays.

NOTE: You can access the ADCS Configuration Wizard by clicking the **Notification Flag**.

15. On the Credentials page click **Next**.
16. On the Role Services page select the **Online Responder** check box. Click **Next**.
17. On the **Confirmation** page, click **Configure** and wait for the confirmation message. A message displays after successful configuration.
18. On the Results page click **Close** to exit the ADCS Configuration Wizard.

Configuring the CA to issue the OCSP Response Signing Certificates

To configure the CA to support the Online Responder Service you must configure the certificate templates and issuing properties for OCSP Response Signing Certificates. To configure the CA to issue OCSP Response Signing certificates you must complete the following:

NOTE: If you have installed the CA and OCSP on same machine then you need to complete this procedure on OCSPSERV to configure OCSP Response Signing Certificate.

To configure certificate templates using the SafeNet KSP

If you want to generate the OCSP signing keys using SafeNet CSP instead of SafeNet KSP go to the next section. These steps are needed if you want to use SafeNet KSP for OCSP signing keys.

1. Log on to **OCSPCA** as a domain administrator.
2. Click **Search**, type **MMC** and press **Enter** to open the console.
3. In the **mmc** console, select **File** and click **Add/Remove Snap-in…**
4. In the **Add or Remove Snap-Ins** dialog box, select the **Certificate Templates** snap-in (under the Available snap-ins section).
5. Click **Add**, and then click **OK**.
6. Under **Console Root**, expand the **Certificate Templates** snap-in. The middle section lists all of the available certificate templates that your CA can issue.
7. Scroll down the list until you locate the **OCSP Response Signing template**. Right-click the template and select **Properties**. The Template properties dialog displays.
8. Click the **General** tab**,** and select the **Publish Certificate in the Active Directory** check box.
9. Set the **Validity Period** and **Renewal period**.

NOTE: We recommend setting the **Validity period** and **Renewal period** for four hours and one hour to test **Auto Renewal**.

10. Click the **Security** tab and select **Add**. The **Select User, Computers, Service Accounts, or Groups** dialog displays.
11. Enter the name of the machine which is hosting the Online Responder service. In this case, the machine name is **OCSPSERV.**
12. Click **OK**. The system should not be able to locate the machine, instead another dialog displays.
13. Click **Object Types.** Select the **Computers** check box. Click **OK**.
14. Re-enter **OCSPSERV** in the **Select User, Computers, Service Accounts, or Groups** dialog. Click **OK**.

    The machine hosting the Online Responder will be added to the Group and user names area under the **Security** tab.
15. Click on **OCSPSERV** in the Group and user names area.
16. Select the **Read**, **Enroll**, and **Autoenroll** check boxes.
17. Ensure that the **Read**, **Write**, **Enroll**, and **Autoenroll** check boxes are selected for both **Domain Admins** and **Enterprise Admins**. Click **Apply**.

18. Select the **Cryptography tab**. Select the **Requests must use one of the following providers** radio button. The dialog below the radio button activates.
19. Select **SafeNet Key Storage Provider**.
20. Click **Apply** and then **OK**.

To configure certificate templates using SafeNet CSP

If you want to generate OCSP signing keys using the SafeNet CSP complete the following procedure. Ensure that you have registered the CSP on both the OCSPCA and OCSPSERV systems.

1. Log on to **OCSPCA** as a domain administrator.
2. Click the **Search** menu, type **MMC** and press **Enter** to open the console.
3. In the **mmc** console, select **File** and click **Add/Remove Snap-in…**
4. In the **Add or Remove Snap-Ins dialog box**, select the **Certificate Templates** snap-in (under the Available snap-ins section).
5. Click **Add**, and then click **OK**.
6. Under Console Root, expand the **Certificate Templates** snap-in. The middle section lists all of the available certificate templates that your CA can issue.
7. Scroll down the list until you locate the **OCSP Response Signing template**. Right-click the **OCSP Response Signing Template** and click **Duplicate Template.**
8. In the pop-up dialog box, click the **Compatibility tab**.
9. In **Compatibility Settings**, under **Certificate Authority** select **Windows Server 2003.** The Resulting Changes window displays. Click **OK**.
10. Under **Certificate recipient**, select **Windows XP / Server 2003.** The Resulting Changes window displays**.** Click **OK**.
11. Click the **General** tab. Enter the **name of template** in Template display name.
12. Select the **Publish Certificate in the Active Directory** check box.
13. Set the **Validity period** and **Renewal period**.

> **NOTE:** We recommend setting the **Validity period** and **Renewal period** for four hours and one hour to test **Auto Renewal**.

14. Click the **Security** tab and select **Add**. The **Select User, Computers, Service Accounts, or Groups** dialog displays. Enter the name of the machine (**OCSPSERV)** which is hosting the Online Responder service.
15. Click **OK**. The system should not be able to locate the machine, instead another dialog displays.
16. Click **Object Types.** Select the **Computers** check box. Click **OK**.
17. Re-enter **OCSPSERV** in the **Select User, Computers, Service Accounts or Groups dialog**. Click **OK**.

    The machine hosting the Online Responder will be added to the Group and user names area under the **Security** tab.
18. Click **OCSPSERV** in the Group and user names area.
19. Select the **Read**, **Enroll**, and **Autoenroll** check boxes.
20. Ensure that the **Read**, **Write**, **Enroll**, and **Autoenroll** check boxes are selected for both **Domain Admins** and **Enterprise Admins**. Click **Apply**.

21. Select the **Cryptography** tab. Select the **Requests must use one of the following providers** radio button. The dialog below the radio button activates.
22. Select **Luna Cryptographic Services for Microsoft Windows**.
23. Click **Apply** and then **OK**.

To configure the CA to support the Online Responder service

1. Log on to **OCSPCA** as a domain administrator.
2. From the **Start** menu, select **Administrative Tools** and click **Certification Authority**.
3. In the console tree (left-hand section), click the **CA** name. (It has a computer and a green tick next to it.)
4. Open the **Action menu** and click **Properties**.
5. Click the **Security tab** and select **Add**. The **Select User, Computers, Service Accounts, or Groups** dialog displays.
6. Enter the name of the machine which is hosting the Online Responder service. In this case, the machine name is **OCSPSERV**.
7. Click **OK**. The system should not be able to locate the machine, instead another dialog displays.
8. Click **Object Types**. Select the **Computers** checkbox. Click **OK**.
9. Re-enter **OCSPSERV** in the **Select User, Computers, Service Accounts or Groups** dialog. Click **OK**.

   The machine hosting the Online Responder will be added to the Group and user names area under the **Security tab**.
10. Click **OCSPSERV** in the Group and user names area.
11. In the **Permissions area**, select the **Request Certificate** check box.
12. Ensure that the **Issue and Manage Certificates**, **Manage CA**, and **Request Certificates** check boxes are selected for **Domain Admins**, **Enterprise Admins**, and **Administrators**.
13. Select the **Extensions tab**. In the **Select extension** list, click **Authority Information Access (AIA).**
14. Click **Add.** In the **Add Location** dialog type under Location.

   ```
   http://<nameofcomputerhostingOCSPhere>/ocsp. For example, the address when using
   OCSPSERV would be http://OCSPSERV/ocsp.
   ```
15. Click **OK**.
16. On the **Extensions tab**
    a. Ensure that the recently added URL is highlighted.
    b. Ensure that the **Include in the AIA extension of issued certificates** and **Include in the online certificate status protocol (OCSP) extension** check boxes are selected.
17. Click **Apply.** Click **Yes** to restart the Active Directory Certificate Services.
18. When the services restarts, click **OK**.
19. In the console tree of the Certification Authority snap-in, right-click **Certificate Templates**, and then click **New Certificate Templates to Issue**.
20. In **Enable Certificates Templates**, select the **OCSP Response Signing template** and any other previously configured certificate templates. Click **OK.**
21. Open Certificate Templates in the Certification Authority and verify that the modified certificate templates are included in the list.

Creating a Revocation Configuration

A revocation configuration includes all of the settings that are needed to respond to status requests regarding certificates that have been issued by using a specific CA key. Creating a revocation configuration involves the following:

- Modifying the Online Responder service to use SafeNet HSMs
- Setting up the Revocation Configuration

Modifying the Online Responder service to use SafeNet HSMs

To use OCSP in conjunction with SafeNet Luna HSMs or HSMoD services, you must configure the Online Responder service to use the HSM to protect the OCSP signing keys.

To modify the Online Responder service to use SafeNet HSMs

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start menu** select **Administrative Tools** and then click **Services.**
3. Locate the **Online Responder Service** in the list of services.
4. **Right-click** on the **Online Responder Service** and select **Properties**.
5. In the dialog box select the **Log on** tab.
6. Under **Log on as**, select the **Local System Account** radio button and then select the **Allow services to interact with desktop** check box.
7. Click **Apply** and then **OK**.
8. Return to the services window. Right-click the **Online Responder Service** and click **Restart.** Wait to start the service again. Close the service window.

Setting up the Revocation Configuration

Once the Online responder Service is configured to use the HSM to protect the OCSP singing keys you can set up the certificate revocation configuration.

To set up the revocation configuration

1. Log on to **OCSPSERV** as a domain administrator.
2. From the **Start** menu, select **Administrative Tools** and then click **Online Responder Management**.
3. In the left-hand pane select **Revocation Configuration**.
4. In the right-hand pane, under Actions, click **Add Revocation Configuration**. A dialog window displays.
5. On the **Getting started with adding a revocation configuration section** click **Next.**
6. In the **Name the Revocation Configuration** section, enter a name for the configuration in the text box (For Example: Test). Click **Next**.
7. In the **Select CA Certificate Location** window, ensure that the **Select a certificate for an Existing enterprise CA** radio button is selected and click **Next**.
8. In the **Choose CA Certificate** section, ensure that the **Browse CA certificates published in Active Directory** radio button is selected and then click **Browse**.

9. In the Select **Certification Authority** dialog box, select the **CA authority** (in this case **OCSPCA**) and click **OK**. Click **Next**.
10. In the **Select Signing Certificate** window, accept the default setting **Automatically select a signing certificate** and select the **Auto-enroll for OCSP signing certificate** check box. Click **Next**.
11. In the **Revocation Provider** window, click **Finish**.

    Once the wizard completes, the Revocation Configuration **Status Box** displays the Online Responder status. The status should display **Bad Signing on Array Controller**.
12. To correct this, click on **Revocation Configuration** in the left hand pane. The certificate displays in the right-pane.
13. Right-click on the certificate and select **Edit Properties**.
14. Click the **Signing** tab. Deselect the **Do not prompt for credentials for cryptographic operations** check box. Click **OK**.
15. Return to the **Online Responder Management** tool. Open **Actions** and click **Refresh**.
16. In the left-hand pane click **Online Responder: Computer Name** and verify that the Revocation Configuration **Status Box** displays **Working**.

Verifying Auto-enrollment

You need to verify that the certificate will auto-renew after the expiry. Verification of auto renewal involves the expiration of the generated certificate and renewal of the certificate using a new key pair. You can verify that auto-enrollment of a newly generated certificate is operating successfully by completing the following procedures:

- Viewing a generated certificate and key pair
- Viewing a renewed certificate and key pair

Viewing a generated certificate and key pair

To verify that auto-enrollment is operating properly you need to verify that the service is capable of generating a certificate and key pair using the SafeNet Luna HSM or HSMoD service.

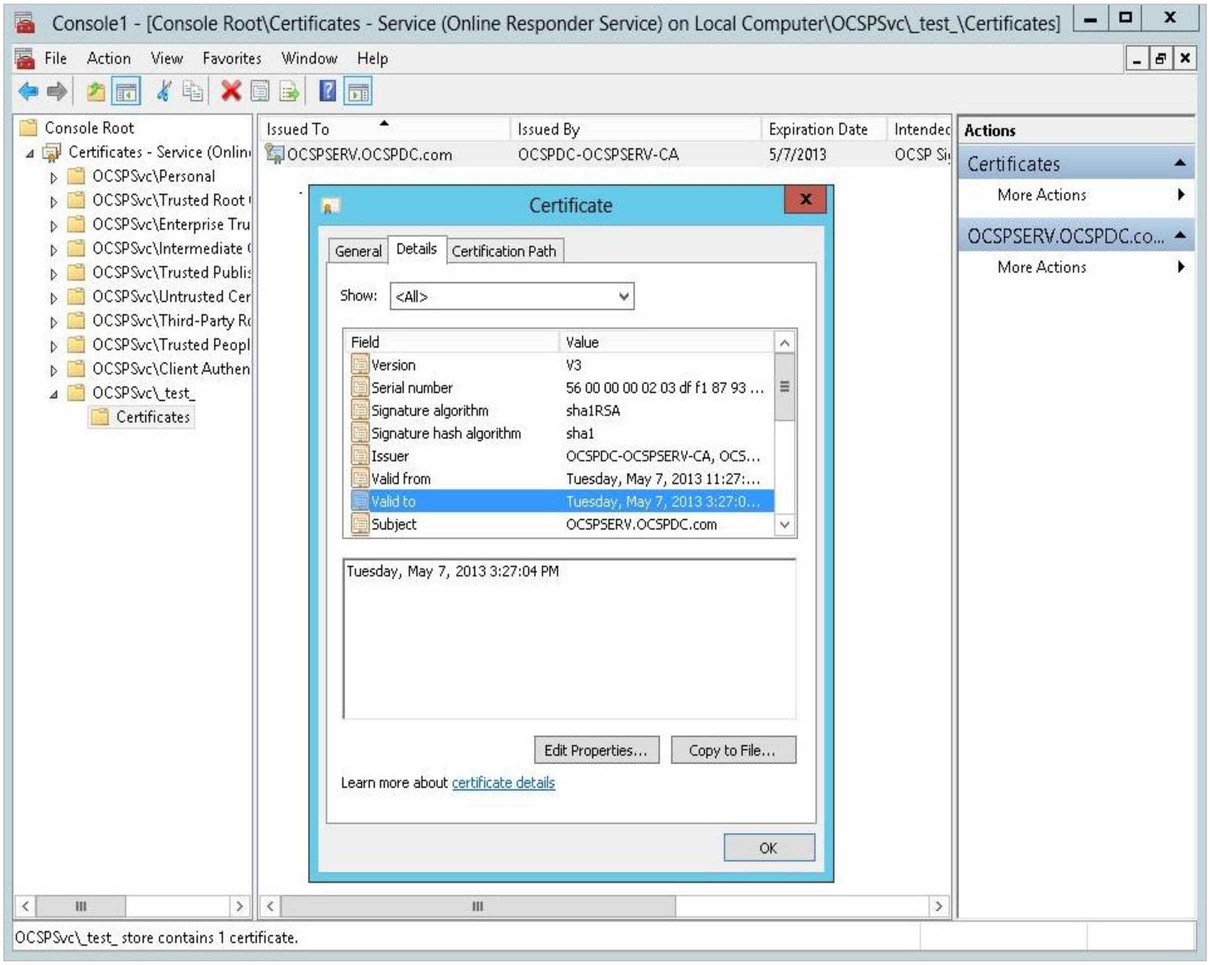
To view a generated certificate and key pair

1. Log on to **OCSPSERV** as a domain administrator.
2. Click **Search**, type **MMC** and press **Enter** to open the console.
3. In the **mmc** console, select **File** and click **Add/Remove Snap-in…**
4. In the **Add or Remove Snap-Ins** dialog box, find the **Certificate snap-in** (under the Available snap-ins section) and select it.
5. Click **Add**, select **Service Account** and click **Next**.
6. Select **Local Computer**, and click **Next.**
7. Under **Certificate Snap-in**, click on the **Online Responder Services** in Service Account and click **Finish**.
8. Click **OK** and expand the **Online Responder Services** tree.
9. Expand the **OCSPSvc\CertificateName** (for example “OCSPSvc_test_”) and double-click on **Certificates**.
10. A certificate displays, double-click the certificate to view the properties of the certificate.

11. Click the **Details** tab and verify the **Valid From** and **Valid To** date of the certificate. It states the certificate expires in the next four hours.

    You can connect with the SafeNet Luna HSM appliance or HSMoD service and verify the key pair which was generated corresponds to the certificate.

    The generated certificate and key pair are shown in the below screenshots:



Console1 - [Console Root\Certificates - Service (Online Responder Service) on Local Computer\OCSPSvc_test_\Certificates]

Issued To	Issued By	Expiration Date	Intended
OCSPSERV.OCSPDC.com	OCSPDC-OCSPSERV-CA	5/7/2013	OCSP Si

Certificate

Show: <All>

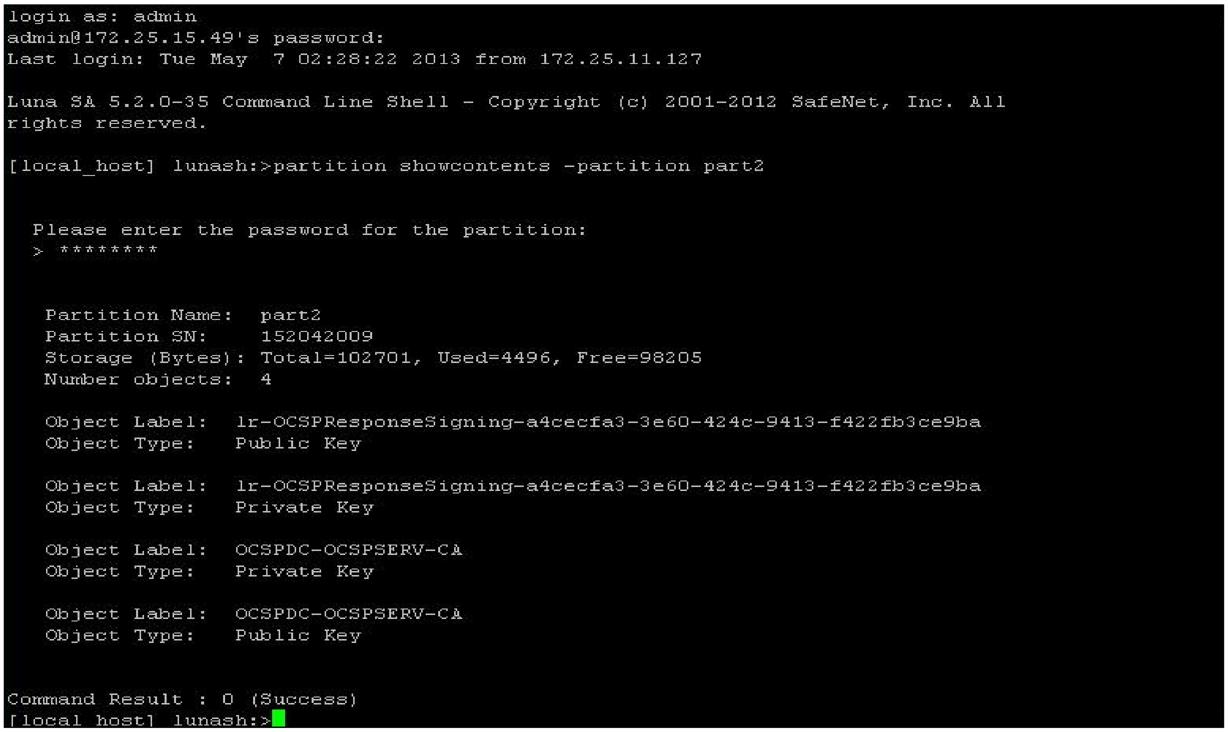
Field	Value
Version	V3
Serial number	56 00 00 00 02 03 df f1 87 93 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	OCSPDC-OCSPSERV-CA, OCS...
Valid from	Tuesday, May 7, 2013 11:27:...
Valid to	Tuesday, May 7, 2013 3:27:0...
Subject	OCSPSERV.OCSPDC.com

Tuesday, May 7, 2013 3:27:04 PM

Learn more about certificate details

OCSPSvc_test_ store contains 1 certificate.

The SafeNet Luna HSM appliance shows the Key Pair for CA certificate and Online Responder Service certificate. If you are using an HSMoD service you can verify the partition contents by executing **partition contents** inside of **lunacm**.



```
login as: admin
admin@172.25.15.49's password:
Last login: Tue May  7 02:28:22 2013 from 172.25.11.127

Luna SA 5.2.0-35 Command Line Shell - Copyright (c) 2001-2012 SafeNet, Inc. All
rights reserved.

[local_host] lunash:>partition showcontents -partition part2


  Please enter the password for the partition:
  > ********


   Partition Name:   part2
   Partition SN:     152042009
   Storage (Bytes): Total=102701, Used=4496, Free=98205
   Number objects:   4

   Object Label:  lr-OCSPResponseSigning-a4cecfa3-3e60-424c-9413-f422fb3ce9ba
   Object Type:   Public Key

   Object Label:  lr-OCSPResponseSigning-a4cecfa3-3e60-424c-9413-f422fb3ce9ba
   Object Type:   Private Key

   Object Label:  OCSPDC-OCSPSERV-CA
   Object Type:   Private Key

   Object Label:  OCSPDC-OCSPSERV-CA
   Object Type:   Public Key


Command Result : 0 (Success)
[local_host] lunash:>
```

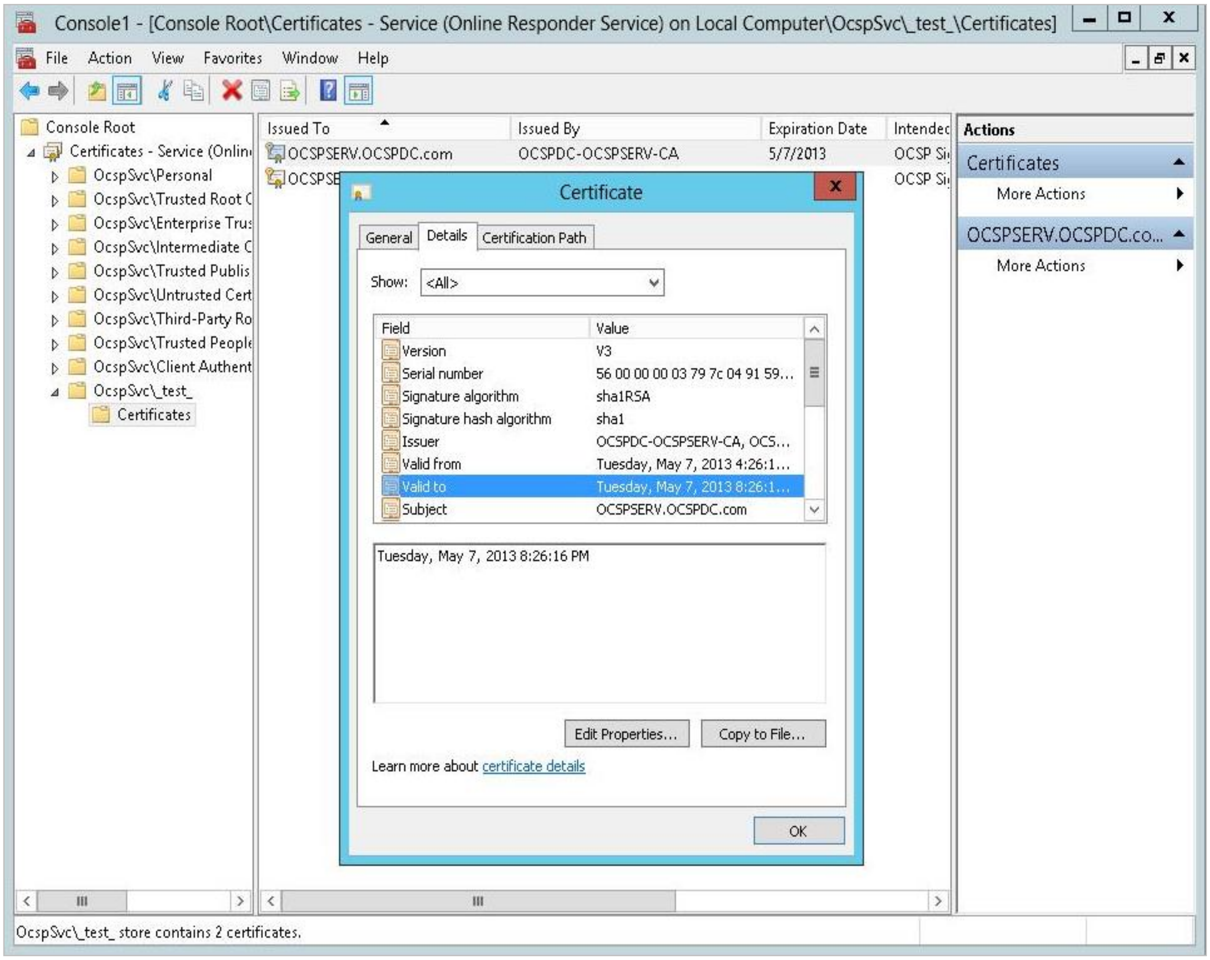
You can see that only one key pair is generated for OCSP Response Signing. You need to wait for four hours to verify the auto-renewal of the certificate because the validity period of the certificate is four hours.

Viewing a renewed certificate and key pair

After four hours have passed, you can verify that the **Valid From** and **Valid To** dates of the certificate have been updated. The new certificate is valid for the next four hours, and a new key pair for the renewed certificate has been generated.

Start -> Run -> MMC -> File -> Add/Remove Snap-in… -> Certificate -> Add -> Service Account -> Next -> Local Computer -> Online Responder Service -> Finish -> OK.

Expand the tree and view the certificate, it shows that the certificate is renewed by OCSP-CA for next four hours:



Issued To	Issued By	Expiration Date	Intendec
OCSPSERV.OCSPDC.com	OCSPDC-OCSPSERV-CA	5/7/2013	OCSP Si
OCSPSE			OCSP Si

Show: <All>

Field	Value
Version	V3
Serial number	56 00 00 00 03 79 7c 04 91 59...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	OCSPDC-OCSPSERV-CA, OCS...
Valid from	Tuesday, May 7, 2013 4:26:1...
Valid to	Tuesday, May 7, 2013 8:26:1...
Subject	OCSPSERV.OCSPDC.com

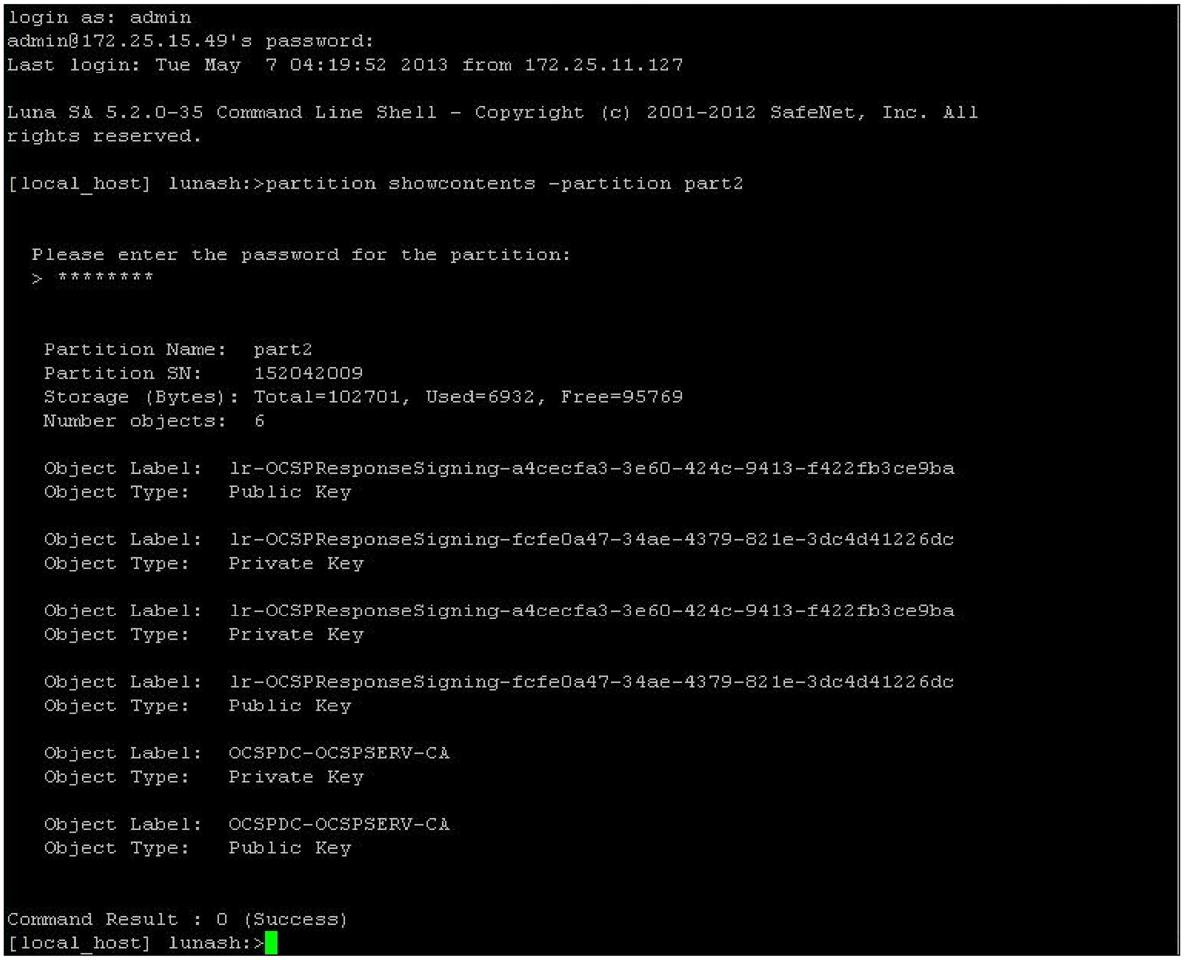
Tuesday, May 7, 2013 8:26:16 PM

Learn more about certificate details

OcspSvc_test_ store contains 2 certificates.

This demonstrates that the certificate renews automatically every four hours. We had it set for testing purposes, but in a production environment we recommend setting the validity periods as required by your organization’s security infrastructure.

A new key pair has been generated on the SafeNet Luna HSM appliance when certificate is renewed.



```
login as: admin
admin@172.25.15.49's password:
Last login: Tue May  7 04:19:52 2013 from 172.25.11.127

Luna SA 5.2.0-35 Command Line Shell - Copyright (c) 2001-2012 SafeNet, Inc. All
rights reserved.

[local_host] lunash:>partition showcontents -partition part2


   Please enter the password for the partition:
   > ********


     Partition Name:   part2
     Partition SN:     152042009
     Storage (Bytes): Total=102701, Used=6932, Free=95769
     Number objects:   6

     Object Label:  lr-OCSPResponseSigning-a4cecfa3-3e60-424c-9413-f422fb3ce9ba
     Object Type:   Public Key

     Object Label:  lr-OCSPResponseSigning-fcfe0a47-34ae-4379-821e-3dc4d41226dc
     Object Type:   Private Key

     Object Label:  lr-OCSPResponseSigning-a4cecfa3-3e60-424c-9413-f422fb3ce9ba
     Object Type:   Private Key

     Object Label:  lr-OCSPResponseSigning-fcfe0a47-34ae-4379-821e-3dc4d41226dc
     Object Type:   Public Key

     Object Label:  OCSPDC-OCSPSERV-CA
     Object Type:   Private Key

     Object Label:  OCSPDC-OCSPSERV-CA
     Object Type:   Public Key


Command Result : 0 (Success)
[local_host] lunash:>
```

Verifying the OCSP Integration

You can verify that the OCSP is operating properly following the integration with SafeNet Luna HSM or HSMoD service.

To generate a certificate request

1. Log on to the **OCSPCL** machine and generate a certificate request. We recommend using the below template structure. (Try to use different vendors' cryptographic service providers.)

```
[Version]
Signature = "$Windows NT$"
[NewRequest]
Subject = "C=IN,CN=OCSPCL"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "Provider_to_be_used"
KeyUsage = 0xf0
MachineKeySet = True
RequestType = PKCS10
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.1
```

```
[Extensions]
1.3.6.1.5.5.7.48.1.5 = Empty
```

2. Copy and paste the above template into a Notepad **.txt** file. Ensure that the Provider Name variable is provided with the quotation marks around it.
3. Once the template has been successfully setup, save it as test.inf on **C:\** drive.
4. Open the command prompt window and go to the local drive, in this case C:\. Execute `certreq –new test.inf test.req` . A certificate request called `test.req` generates and is placed on the **C:\** drive.
5. Execute `certreq –submit –attrib “CertificateTemplate:WebServer” test.req` command in the command prompt. A pop up window displays confirming which CA to use. Select the **OCSPCA** entry and click **OK**. A dialog displays to save the certificate to a file.
6. Save the certificate file and click **OK**. After a short pause, a message **Certificate Successfully Generated** displays on the command prompt and a certificate file called `test.cer` generates on the C:\ drive.

To test the certificate’s origin

1. Log on to **OCSPCA** and go to the Certification Authority tool by navigating to **Start** -> **Administrative Tools** -> **Certification Authority.**
2. In the **Certification Authority snap-in**, publish a new CRL by clicking **Certification Authority (Computer)/CA name/Revoked Certificates** in the console tree. Then, right-click on the **Revoked Certificates** folder, point to **All Tasks**, and click **Publish**.
3. Select **New CRL** and click **OK**.
4. Open the **Certification Authority snap-in** and right-click on the CA. Click **Properties**.
5. On the **Extensions tab,** verify that the extension is set to CRL Distribution Point (CDP) in the drop-down menu**.** Select any listed **CRL distribution points,** click **Remove,** and click **OK.**
6. Click **Apply**. A dialog displays stating that you need to restart the service.
7. Click **OK** and wait for the service restart.
8. Verify that clients can still obtain revocation data. Execute the following on OCSPCL:

   ```
   certutil -url test.cer
   ```

9. The URL Retrieval Tool dialog displays. Select the **CRLs (From CDP)** radio button and click **Retrieve**.
10. Select the **OCSP (From AIA)** radio button and click **Retrieve**. The list should contain an OCSP entry showing the web address of the OCSP server. If it is working correctly, the word **Verified** displays in the first column in the list.
11. Select the **Certs (from AIA)** radio button and click **Retrieve**. One or two entries should be listed, with **Verified** next to them.

NOTE: If Certificate Authority Web Enrollment is not installed on the CA, an entry with AIA may display as Failed. However, as long as one of the entries in the Certs (from AIA) section reads Verified there should be no problems with the set-up.

To verify the OCSP integration

1. Open a command prompt and select the local drive (**C:\**). Execute:

   ```
   certutil -verify test.cer > test.txt
   ```

2. When the `certutil -verify test.cer > test.txt` command has been completed, open the `test.txt` file on **C:\** drive. The file should contain the following information:

```
Issuer:
CN=Integration-OCSPSERV-CA
DC=Integration
DC=com
Subject:
CN=OCSPCL
C=IN
Cert Serial Number: 611362e4000000000003

dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x20000000)
dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000)
ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000)
HCCE_LOCAL_MACHINE
CERT_CHAIN_POLICY_BASE
-------- CERT_CHAIN_CONTEXT --------
ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
ChainContext.dwRevocationFreshnessTime: 17 Minutes, 42 Seconds

SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
SimpleChain.dwRevocationFreshnessTime: 17 Minutes, 42 Seconds

CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0
Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
NotBefore: 5/23/2013 3:55 PM
NotAfter: 5/23/2015 3:55 PM
Subject: CN=OCSPCL, C=IN
Serial: 611362e4000000000003
Template: WebServer
f0 e3 6b 9f f4 59 a6 64 18 f4 6f f6 a1 90 52 5b a3 3a 40 8c
Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)
Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
CRL 02:
Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
c1 32 12 a5 2f 82 d9 69 06 c0 28 1c 75 9d b1 5b 4c c5 4f 6d
Delta CRL 02:
Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
b1 63 03 a3 b8 d0 c5 41 7c d9 2c 3f ae 87 b4 a3 27 bd e7 73
Application[0] = 1.3.6.1.5.5.7.3.1 Server Authentication

CertContext[0][1]: dwInfoStatus=10c dwErrorStatus=0
Issuer: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
NotBefore: 5/23/2013 3:30 PM
NotAfter: 5/23/2018 3:40 PM
Subject: CN=Integration-OCSPSERV-CA, DC=Integration, DC=com
Serial: 6236c444f91af2a04fafdd311517307a
c3 3b 1c 6a 7f 07 3d f9 63 2a d1 fd 62 ca eb 16 e5 04 0a d3
Element.dwInfoStatus = CERT_TRUST_HAS_NAME_MATCH_ISSUER (0x4)
Element.dwInfoStatus = CERT_TRUST_IS_SELF_SIGNED (0x8)
Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)

Exclude leaf cert:
e9 a1 9d 87 ea 5f 8b 9f b1 cc 2d d5 3a 55 f2 d1 12 14 b8 a2
Full chain:
```

```
e5 79 bc 47 e8 b8 05 11 fa e4 0d 47 a8 3e 73 99 3d df cf 4f
------------------------------------
Verified Issuance Policies: None
Verified Application Policies:
1.3.6.1.5.5.7.3.1 Server Authentication
Leaf certificate revocation check passed
CertUtil: -verify command completed successfully.
```

3. Ensure that the `certutil –verify test.cer > test.txt` output includes the following:

```
Verified Issuance Policies: None
Verified Application Policies:
1.3.6.1.5.5.7.3.1 Server Authentication
Leaf certificate revocation check passed
CertUtil: -verify command completed successfully.
```

These commands demonstrate that the OCSP server is operating correctly without any errors. The most important component of the above example is the **Leaf certificate revocation check passed** line as this demonstrates that the OCSP service is returning the certificate status as **Good**.

If the log generated by the verify command does not include the above section (or similar) and has errors in the output, we recommend you restart the OCSP server and client machine, and run the **verify** command again on the certificate file.

4

Troubleshooting

Bad signing certificate on array controller

Problem: Online Responder reports “Bad Signing Certificate on Array Controller”.

Reason: This error displays when the CA certificate cannot be located by the Online Responder client.

Solution: Ensure that the points mentioned in the Create Revocation Configuration have been correctly carried out. Verify that the CA is correctly configured and that a valid CA certificate Exists for OCSP Signing.

‘Failed’ next to AIA entry in URL Retrieval tool

Problem: Using certutil –url <certnamehere.cer> and selecting Certs (from AIA) shows an entry in the list called AIA with “Failed” next to it.

Reason: This error displays when Certificate Authority Web Enrollment is not installed on the CA.

Solution: Install Certificate Authority Web Enrollment on the CA machine.

NOTE: AIA failing does not adversely impact the OCSP setup. As long as both items in the Certs (from AIA) do not fail there should not be a problem with the setup

Unrecognized/Untrusted Certificate Authority

Problem: When viewing a newly generated certificate from the CA it is reported as untrusted.

Reason: This error displays when the CA has not been added to the **Trusted Root Certification Authorities** certificate store.

Solution: Double-click the newly generated certificate. Under the **General** tab, click I**nstall Certificate…** On the first screen that is displayed click **Next**, select the radio button next to **Place all certificates in the following store** and click **Browse**. In the **Select Certificate Store** window that is displayed click **Trusted Root Certification Authorities** and click **OK**. When the window disappears click **Next** and on the next window click **Finish**.

‘Invalid Provider Specified’ error when using ‘certreq –new’ command

Problem: Using the certreq –new <.req file here> command throws an **Invalid Provider Specified error**.

Reason: This error displays when the CSPs are not installed and set up on the client machine not set up correctly.

Solution: Ensure that the SafeNet Luna CSP or CNG providers are correctly installed and set up. (To overcome this issue, execute the CSP Install Wizard and CNG Configuration Wizard under the SafeNet Luna HSM Installation folder) or you can use Microsoft Cryptographic Service Provider or any other service provider that is registered on the client machine.