Microsoft® Authenticode and Luna SA/Luna PCI

Integration Guide

SafeNet. THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-009988-001 (Rev F)
Release Date	August 2014

Trademarks

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimer

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520

Contents

CHAPTER 1 Introduction 5
Scope 5
Prerequisites 6

CHAPTER 2 Integrating Microsoft Authenticode (Windows SDK for Windows Server 2003 SP1) with Luna SA/Luna PCI 8

CHAPTER 3 Integrating Microsoft Authenticode (Windows SDK for Windows Server 2008) with Luna SA 10

CHAPTER 4 Integrating Microsoft Authenticode (Windows SDK for Windows Server 2012) with Luna HSM 13

CHAPTER 5 Integrating MS Strong Name (Windows Server 2012 R2) with Luna HSM 15

CHAPTER 6 Integrating MS Mage/ClickOnce (Windows Server 2012 R2) with Luna HSM 19

CHAPTER 7 Integrating Microsoft HCK (Windows Server 2012) with Luna HSM 24

CHAPTER 8 Troubleshooting Tips 33

CHAPTER 1
Introduction

This document covers the necessary information to install, configure and integrate Microsoft Authenticode with SafeNet Luna Hardware Security Modules (HSM).

Microsoft™ Authenticode™ permits end users to identify who published a software component and verify that no one tampered with it before downloading it from the Internet. Authenticode assures end users of the identity of the software publisher and that the code has not been altered after the signature was applied, before they download signed code from the Internet.

Authenticode relies on proven cryptographic techniques and the use of one or more private keys to sign and time-stamp the published software. It is important to maintain the confidentiality of these keys. The SafeNet Luna Hardware Security Module (HSM) integrates with Microsoft Authenticode to provide a trusted system for protecting the organizational credentials of the software publisher. The SafeNet Luna HSMs secures the code-signing key within an industry standard FIPS 140-2 level 3 validated HSM.

Scope

3rd Party Application Details

- Microsoft Authenticode (Microsoft Windows SDK 6.1)
- Microsoft Authenticode (Microsoft Windows SDK 8.1)

Supported Platforms

Operating System	SafeNet Luna HSM	Microsoft SDK	Microsoft Office Smart Tags SDK (Optional)
Windows Server 2003 SP1	Luna SA v4.4 Luna PCI v3.0	v6.1	Office XP SDK
Windows Server 2008 (64 bit) Windows Server 2008 (32 bit)	Luna SA v5.1	v6.1	Office 2003 SDK
Windows Server 2012 Standard	Luna v5.2.1 Luna v5.4.1	v8.1	Office 2003 SDK
Windows Server 2012 R2	Luna v5.4.1	v8.1	

HSMs and Firmware Version

- K6 HSM f/w 6.21.0 (Luna SA)
- K6 HSM f/w 6.10.1 (Luna SA)
- K6 HSM f/w 6.2.1 (Luna SA)
- K5 HSM f/w 4.6.8 (Luna SA)
- K5 HSM f/w 4.7.1 (Luna PCI)

Library and Driver Support

- PKCS#11 v2.01 dynamic library
- PCKS#11 v2.20 dynamic library

Distributions

- Luna Client s/w v5.4.1 (64 bit)
- Luna Client s/w v5.2.1
- Luna SA Client s/w v5.1 (32 bit)
- Luna SA Client s/w v4.4
- Luna PCI Client s/w v3.0

Prerequisites

Luna SA Setup

Please refer to the **Luna SA** documentation for installation steps and details regarding to configure and setup the box on Windows systems. Before you get started ensure the following:

- Luna SA appliance a secure admin password
- Luna SA a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance.
- Created and exchanged certificates between the Luna SA and your "Client" system.
- Created a partition on the HSM, remember the partition password that will be later used by Microsoft Authenticode. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from Luna SA. The general form of command is "C:\Program Files\LunaSA\vtl verify".
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Luna PCI Setup

Please refer to the **Luna PCI** documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started ensure the following:

- Initialize the HSM on the Luna PCI appliance
- Create a partition on the HSM that will be later used by Microsoft Authenticode.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna PCI with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Microsoft Authenticode Setup

Installing the Windows SDK

The Authenticode programs (makecert, cert2spc etc.,) are installed with Microsoft Visual Studio and Microsoft Windows SDK.

Refer to the appropriate Microsoft Windows SDK installation documentation.

Installing the Office Smart Tags SDK

In order to demonstrate the Authenticode technology the Microsoft Office Smart Tags SDK is required.

Refer to the appropriate Microsoft Office Smart Tags SDK installation documentation.

CHAPTER 2
Integrating Microsoft Authenticode (Windows SDK for Windows Server 2003 SP1) with Luna SA/Luna PCI

1. In order to integrate the Luna SA / Luna PCI Hardware Security Module with Microsoft Authenticode, the Luna CSP "**Luna Cryptographic Services for Microsoft Windows**" must be used with the makecert command:

   makecert -sk noi1-501706key -sp "Luna Cryptographic Services for Microsoft Windows" -r -n CN=noi1-501706 -ss TestStore noi1-501706.cer

   where:

   -sk The location of the subject's key container which holds the private key

   -sp Subject CryptoAPI's provider name

   -r Create a self –signed certificate

   -n The name of the publisher's certificate

   -ss The name of the subject's certificate store in which the generated certificate will be stored

2. Create a Software Publishing Certificate (SPC) from the generated certificate.

   - Traverse to the Microsoft Platform SDK bin directory, i.e. **C:\Program Files\Microsoft Platform SDK\Bin**
   - Cert2Spc noi1-501706.cer noi1-501706.spc

3. Sign and Time Stamp the code.

   Steps are mentioned below:

   - Open the command prompt.
   - Traverse to the Microsoft Platform SDK **bin** directory, i.e. **C:\Program Files\Microsoft Platform SDK\Bin**
   - Run the command **signtool signwizard** to launch the digital signing wizard.
   - Click **Next** on the Welcome screen.
   - Select the desired file (.dll, .exe etc.,) to sign. Click **Next**.
     e.g. C:\Program Files\Smart Tag SDK\Simple VB Sample\SimpleTerm.dll installed with the Smart Tag SDK
   - Choose the **Custom** option in the **Signing Options** window and click **Next**.

- In the **Signature Certificate** Window, Click **Select from File**… and browse to the generated **Software Publishing Certificate (.spc file)**. Click **Next**.
- Select **Private Key in a CSP** if key is generated using Cryptographic Service Provider (CSP) i.e. "**Luna Cryptographic Services for Microsoft Windows**", select the appropriate **CSP, Key container**, click **Next**.
- Select the desired **Hash Algorithm** and Click **Next**.
- Click **Next** on the **Additional Certificates** window.
- Optionally add a description on **Data Description** window and Click **Next**.
- Select **Add a timestamp to the data** and give the time stamping URL, i.e. **http://timestamp.verisign.com/scripts/timstampdll**.
- Click **Finish** on the **Complete the Digital Signature Wizard** window.
- Click **OK** in the "**The Digital Signing Wizard was completed successfully**" information window.

Microsoft Authenticode configuration with Luna SA / Luna PCI HSM is completed and ready for use.

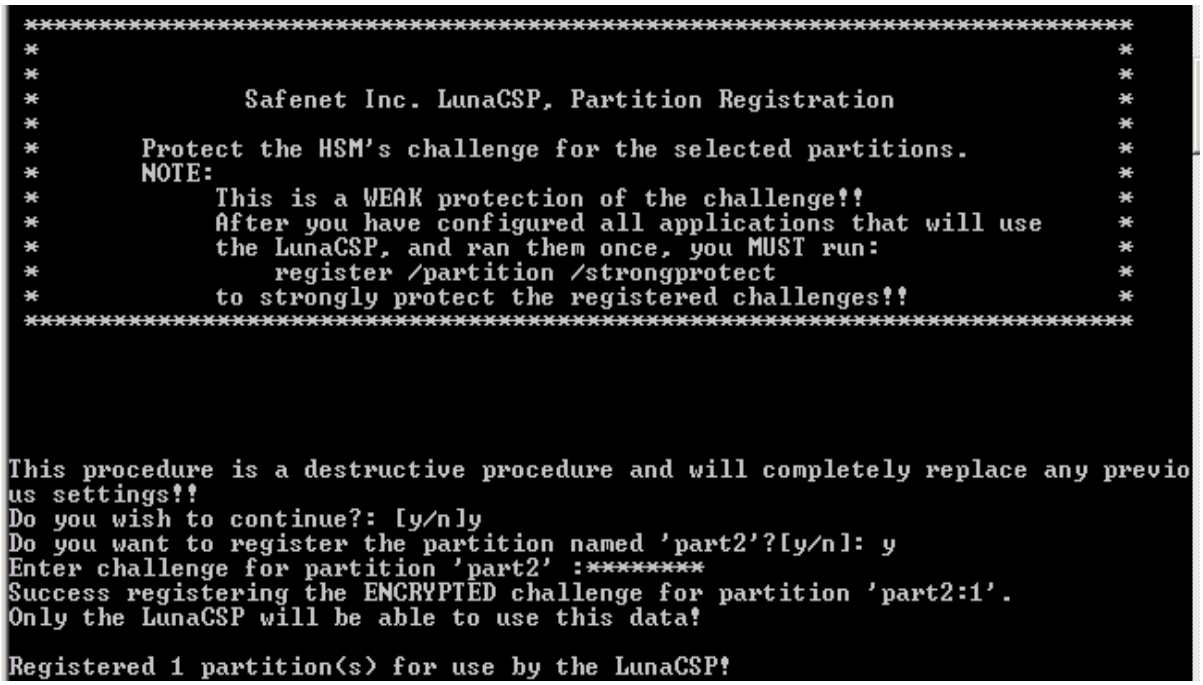
CHAPTER 3
Integrating Microsoft Authenticode (Windows SDK for Windows Server 2008) with Luna SA

1. Install Luna Cryptographic Service Provider (CSP) on Windows Server 2008

   - Run the command, register.exe to register Luna CSP. The general form of command is

   Windows Server 2008 (32 bit) - C:\Program Files\LunaSA\CSP>Register.exe

   Windows Server 2008 (64 bit) - C:\Program Files (x86)\LunaSA\CSP>Register.exe



   - To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is

   Windows Server 2008 (32 bit) - C:\Program Files\LunaSA\CSP>Register.exe /l

   Windows Server 2008 (64 bit) - C:\Program Files (x86)\LunaSA\CSP>Register.exe /l

2. In order to integrate the Luna SA Hardware Security Module with Microsoft Authenticode, the Luna CSP **"Luna Cryptographic Services for Microsoft Windows"** must be used with the makecert command:

Example:

C:\>makecert -sk mykey -sp "Luna Cryptographic Services for Microsoft Windows" –n CN=WIN2008-TEST1 -ss mycert Test.cer

where:

-sk The location of the subject's key container which holds the private key

-sp Subject CryptoAPI's provider name

-n The name of the publisher's certificate

-ss The name of the subject's certificate store in which the generated certificate will be stored

```
C:\>"\Program Files\Microsoft SDKs\Windows\v6.1\Bin\makecert.exe" -sk mykey -sp
"Luna Cryptographic Services for Microsoft Windows" -n CN=WIN2008-TEST1 -ss myce
rt Test.cer
Succeeded
```

3. Create a Software Publishing Certificate (SPC) from the generated certificate.

   Example:

   C:\>cert2spc Test.cer Test.spc

```
C:\>"\Program Files\Microsoft SDKs\Windows\v6.1\Bin\Cert2Spc.exe" Test.cer Test.
spc
Succeeded
```

4. Signing and Time Stamping the code.

   The following steps illustrate how to Sign and Time Stamp the code using signtool GUI:

   - Open the command prompt (Start -> Run –> type cmd –>press Enter).
   - Traverse to the Microsoft Platform SDK **bin** directory, i.e. **C:\Program Files\Microsoft SDKs\Windows\v6.1\Bin**
   - Run the command **signtool signwizard** to launch the digital signing wizard.
   - Click **Next** on the Welcome screen.
   - Select the desired file (.dll, .exe etc.,) to sign and click **Next**.
     Example:
     C:\Program Files\Microsoft Office 2003 Developer Resources\Microsoft Office 2003 Smart Tag SDK\Samples\Visual Basic 6.0 Sample\SimpleTerm\SimpleTerm.dll
   - Choose the **Custom** option in the **Signing Options** window and click **Next**.
   - In the **Signature Certificate** Window, Click **Select from File…** and browse to the generated **Software Publishing Certificate (.spc file)** and click **Next**.
   - Select **Private Key in a CSP** if key is generated using Cryptographic Service Provider (CSP), select the appropriate **CSP** i.e. **"Luna Cryptographic Services for Microsoft Windows", Key container** and click **Next**.
   - Select the desired **Hash Algorithm** and Click **Next**.
   - Click **Next** on the **Additional Certificates** window.

- Optionally add a description on **Data Description** window and Click **Next**.
- Select **Add a timestamp to the data** and give the time stamping URL and click **Next**.
- Click **Finish** on the **Complete the Digital Signature Wizard** window.
- Click **OK** in the **"The Digital Signing Wizard was completed successfully"** information window.

You can use signtool command without GUI using the following command:

C:\> signtool sign /v /s storename /csp "Cryptographic Service Provider Name" /kc "KeyContainerName" /t timestamp URL "File to be signed"

IMPORTANT: Any names that contain spaces must be in double quotes.

```
C:\>"\Program Files\Microsoft SDKs\Windows\v6.1\Bin\signtool.exe" sign /v /s myc
ert /csp "Luna Cryptographic Services for Microsoft Windows" /kc mykey /t http:/
/timestamp.globalsign.com/scripts/timstamp.dll "\Program Files (x86)\Microsoft O
ffice 2003 Developer Resources\Microsoft Office 2003 Smart Tag SDK\Samples\Visua
l Basic 6.0 Sample\SimpleTerm\SimpleTerm.dll"
The following certificate was selected:
    Issued to: WIN2008-TEST1
    Issued by: Root Agency
    Expires:   1/1/2040 5:29:59 AM
    SHA1 hash: 3DABFCF6D28AE6086919B942E82A8E2140C28EAD

Done Adding Additional Store

Attempting to sign: \Program Files (x86)\Microsoft Office 2003 Developer Resourc
es\Microsoft Office 2003 Smart Tag SDK\Samples\Visual Basic 6.0 Sample\SimpleTer
m\SimpleTerm.dll
Successfully signed and timestamped: \Program Files (x86)\Microsoft Office 2003
Developer Resources\Microsoft Office 2003 Smart Tag SDK\Samples\Visual Basic 6.0
 Sample\SimpleTerm\SimpleTerm.dll

Number of files successfully Signed: 1
Number of warnings: 0
Number of errors: 0

C:\>_
```

Microsoft Authenticode configuration with Luna SA HSM is completed and ready for use.

CHAPTER 4
Integrating Microsoft Authenticode (Windows SDK for Windows Server 2012) with Luna HSM

1. Install Luna Cryptographic Service Provider (CSP) on Windows Server 2012
   - Run the command, *register.exe* to register Luna CSP. The general form of command is

     <Luna Client Installation Directory>\CSP>register.exe
   - To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is

     <Luna Client Installation Directory>\CSP>register.exe /l
2. In order to integrate the Luna SA Hardware Security Module with Microsoft Authenticode, the Luna CSP **"Luna Cryptographic Services for Microsoft Windows"** must be used with the makecert command:

   ---

   makecert -sk mykey -sp "Luna Cryptographic Services for Microsoft Windows" –n "CN=Common Name" -r -ss mystore Test.cer

   ---

   where:

   -sk The location of the subject's key container which holds the private key

   -sp Subject CryptoAPI's provider name

   -n The name and details of the publisher's certificate

   -ss The name of the subject's certificate store in which the generated certificate will be stored.

   NOTE: Anything that contains spaces must be in double quotes ("").

3. Create a Software Publishing Certificate (SPC) from the generated certificate.

   ---

   cert2spc Test.cer Test.spc

   ---

4. Signing and Time Stamping the code.

You can Sign and Time Stamp the code using signtool as follows:

---

signtool sign /v /f Certificate /p Pin /csp “Cryptographic Service Provider Name" /k "Key Container Name" /t timestamp URL “File to be signed”

---

where:

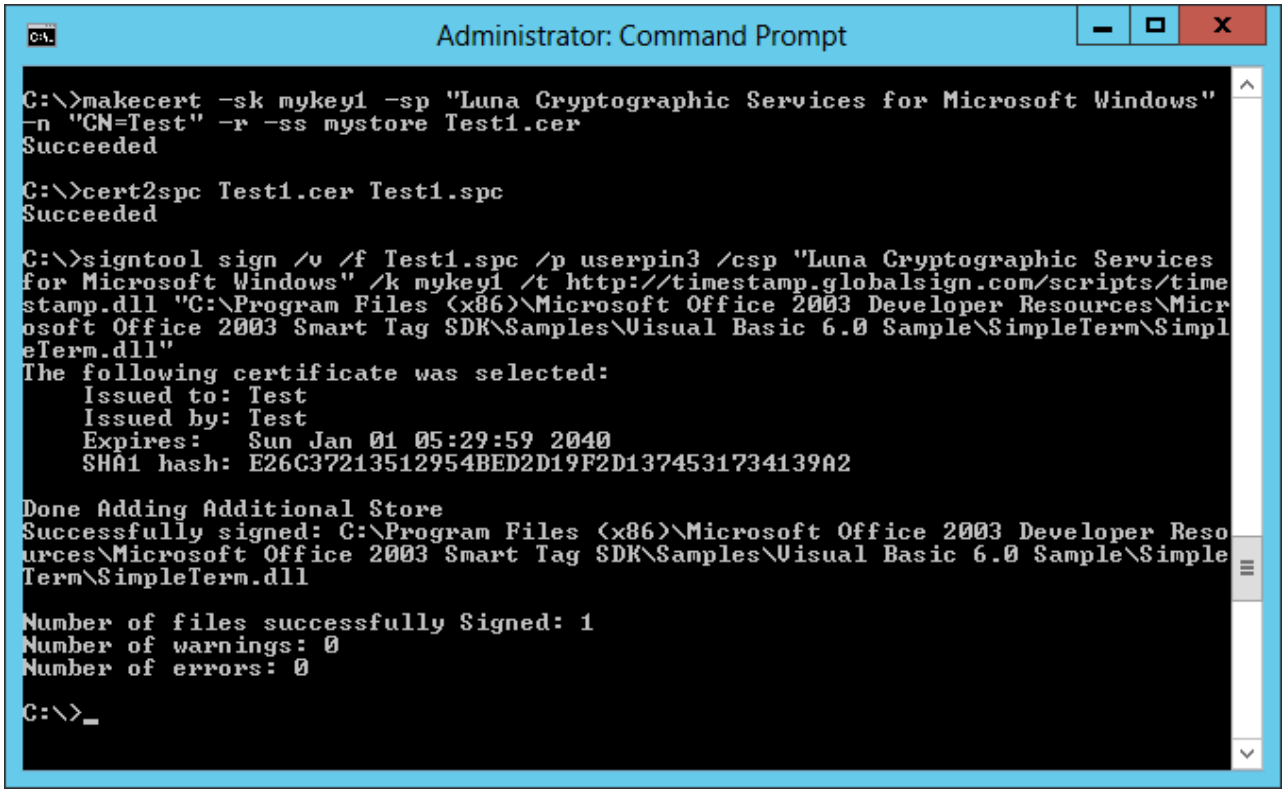
/f Publisher’s Certificate.

/p HSM partition password.

/k Container Name that contains the signing key.

/t URL used for Time Stamping.

IMPORTANT: Any names that contain spaces must be in double quotes.



Microsoft Authenticode configuration with Luna HSM is completed and ready for use.

CHAPTER 5
Integrating MS Strong Name (Windows Server 2012 R2) with Luna HSM

Strong Name is the part of Microsoft SDK that offers a powerful mechanism for giving .NET Framework assemblies unique identities. To get a valid strong name, an assembly is strong-name signed during the build process. This is done using the private key that corresponds to the public key in the strong name. The strong name signature can then be verified using the public key. Strong names prevent spoofing of your code by a third party (that is, of course, as long as you keep the private key secure).

You can secure the strong name private key on Luna HSM.

1. Install Luna Cryptographic Service Provider (CSP) on Windows Server.
    - Open the command prompt and run *register.exe* to register Luna CSP. The general form of command is

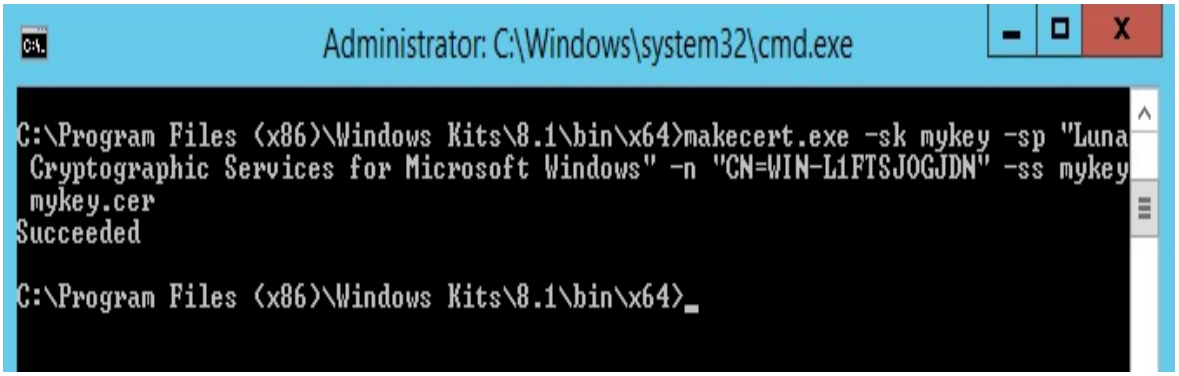
      <Luna Client Installation Directory>\CSP>register.exe
    - To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is

      <Luna Client Installation Directory>\CSP>register.exe /l
2. In order to integrate the Luna SA Hardware Security Module with Microsoft Strong Name, the Luna CSP **"Luna Cryptographic Services for Microsoft Windows"** must be used with the makecert command, open the command prompt and run the following command:

    ---

    makecert -sk <keyContainer> -sp "Luna Cryptographic Services for Microsoft Windows" –n "CN=Common Name" -ss <certStore> CertificateName.cer

    ---

    Where:

-sk The location of the subject's key container which holds the private key

-sp Subject CryptoAPI's provider name

-n The name and details of the signer's certificate

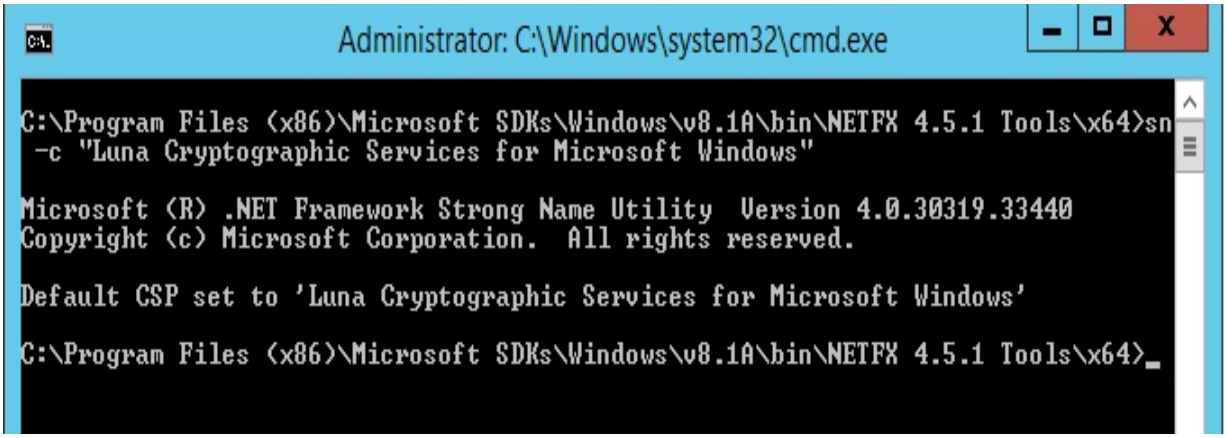
-ss The name of the subject's certificate store in which the generated certificate will be stored.

NOTE: Anything that contains spaces must be in double quotes ("").

3. Make the Luna CSP as a default CSP to use with Microsoft Strong Name using the following command:

---

sn.exe -c "Luna Cryptographic Services for Microsoft Windows"

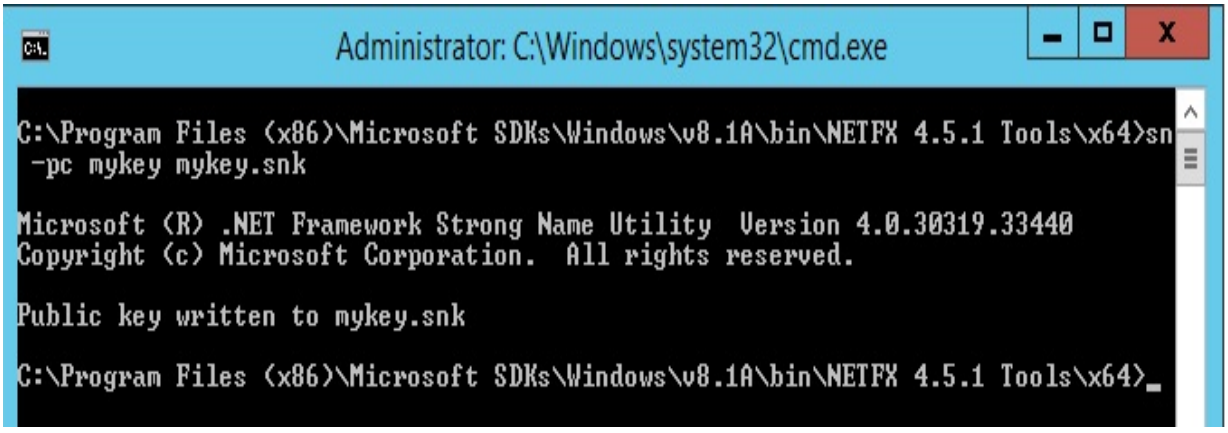


4. Extract the public key from the key-pair generated in step 2 using the following command:

---

sn.exe -pc mykey mykey.snk

Where "mykey" is the name of key container and "mykey.snk" is name of public key file.



5. To sign a .NET assembly, write any C# program and open the Visual Studio command prompt to compile the program and delay sign the generated exe file. Use the following command:

---

csc /delaysign+ /keyfile:"C:\Program Files (x86)\Microsoft SDKs\Windows\v8.1A\bin\NETFX 4.5.1 Tools\x64\mykey.snk" C:\Users\Administrator\Desktop\myapp.cs

---

Where "/keyfile" is the public key extracting from the key-pair in the previous command.

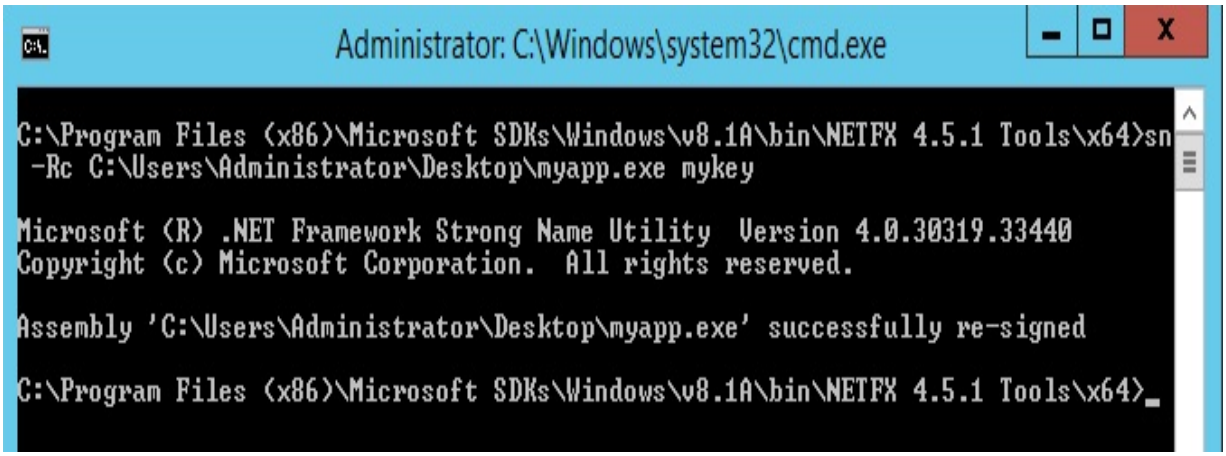
NOTE: Anything that contains spaces must be in double quotes ("").

6. Sign the generated exe with Strong Name using the following command:

---

sn.exe -Rc C:\Users\Administrator\Desktop\myapp.exe mykey

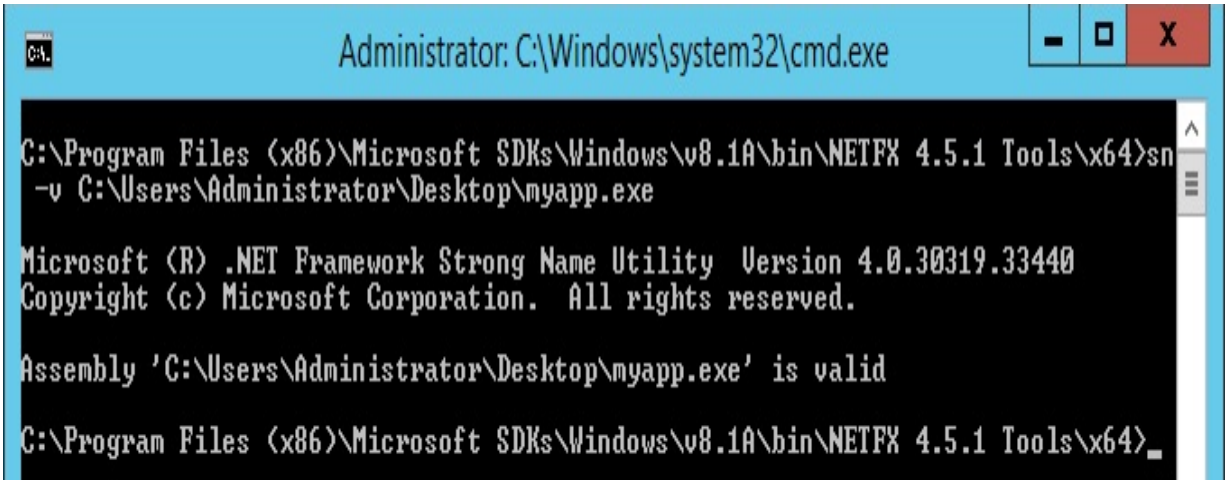
Where "mykey" is the key container in which you have generated the key-pair.



7. Verify the assembly is Strong Name signed using the following command:

---

sn.exe -v C:\Users\Administrator\Desktop\myapp.exe



You have successfully signed and verified a .Net assembly using the key-pair generated on Luna HSM with Strong Name.

CHAPTER 6
Integrating MS Mage/ClickOnce (Windows Server 2012 R2) with Luna HSM

Microsoft's Mage.exe is a Manifest Generation and Editing command line Tool for .NET Framework applications. There is also a UI version MageUI.exe. A typical use is manually creating your ClickOnce deployment manifests. This guide assumes that you have a Windows application that you are ready to deploy. This application will be referred to as AppToDeploy.

For more details about mage/ClickOnce signing refer Microsoft Documentation.

Luna HSM is used to secure the signing keys so that your signing keys never access by any unauthorized entity.

Mage.exe is a 32 bit application so you have to use the 32 bit Luna Client with 32 bit CSP.

1. Install Luna Cryptographic Service Provider (CSP) on Windows Server.
    - Open the command prompt and run *register.exe* to register Luna CSP. The general form of command is

      <Luna Client Installation Directory>\win32\csp>register.exe
    - To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is

      <Luna Client Installation Directory>\win32\csp>register.exe /l
2. In order to integrate the Luna SA Hardware Security Module with Microsoft Mage\ClickOnce Signing, the Luna CSP **"Luna Cryptographic Services for Microsoft Windows"** must be used with the makecert command, open the command prompt and run the following command:

    ---

    makecert -sk <keyContainer> -sp "Luna Cryptographic Services for Microsoft Windows" –n "CN=Common Name" -ss <certStore> CertificateName.cer

    ---

    Where:

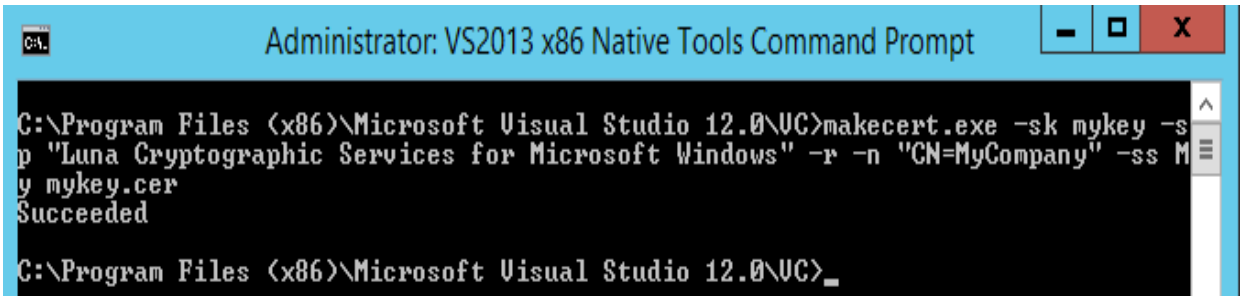
    -sk The location of the subject's key container which holds the private key

    -sp Subject CryptoAPI's provider name

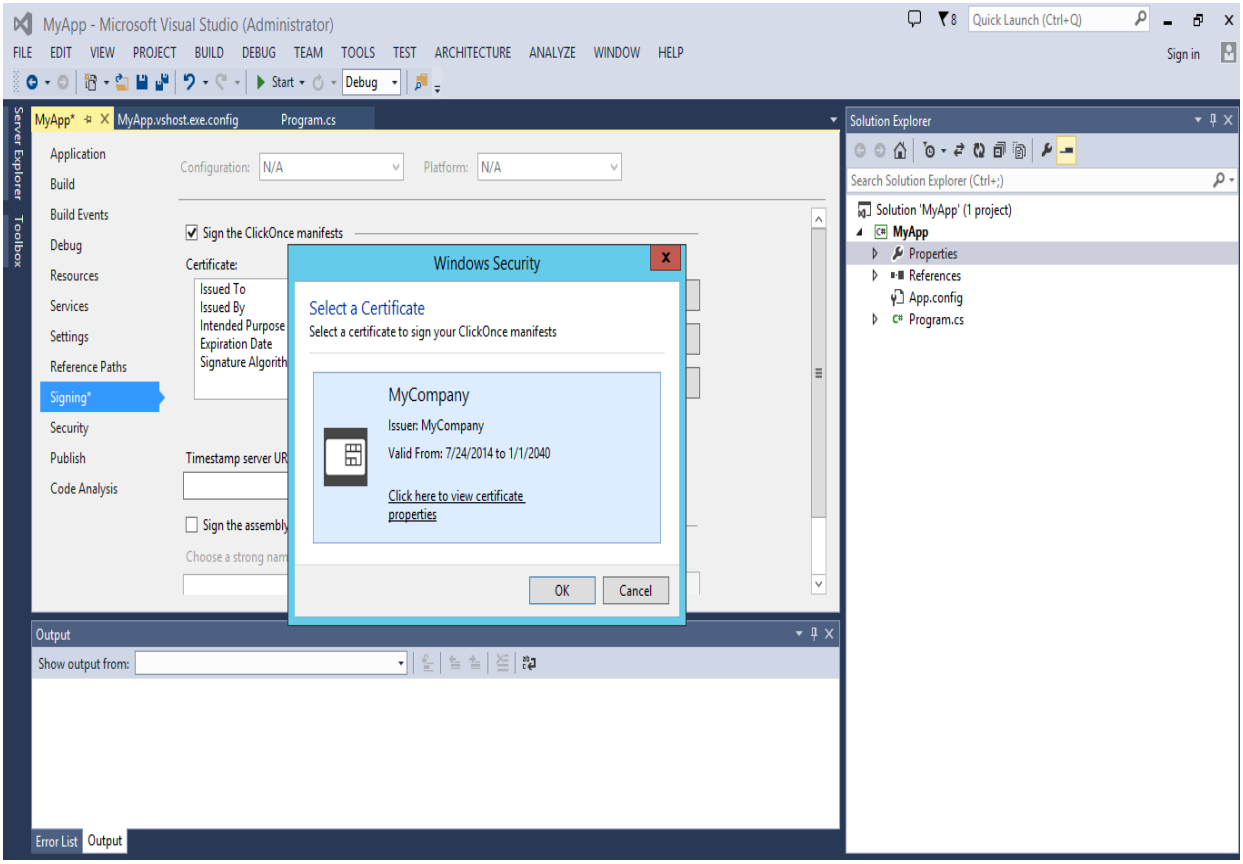
    -n The name and details of the signer's certificate

    -ss The name of the subject's certificate store in which the generated certificate will be stored. Use "My" which is the default user cert store where the application is looking for certificate.

NOTE: Anything that contains spaces must be in double quotes ("").



NOTE: After generating the certificate, you can use this certificate in Visual Studio to sign the Application/Deployment manifest. You need to open the Properties window of the project and click on the Signing and then select Sign the ClickOnce manifests. Click on Select from Store… and click OK after choosing the certificate you have generated in step 1.



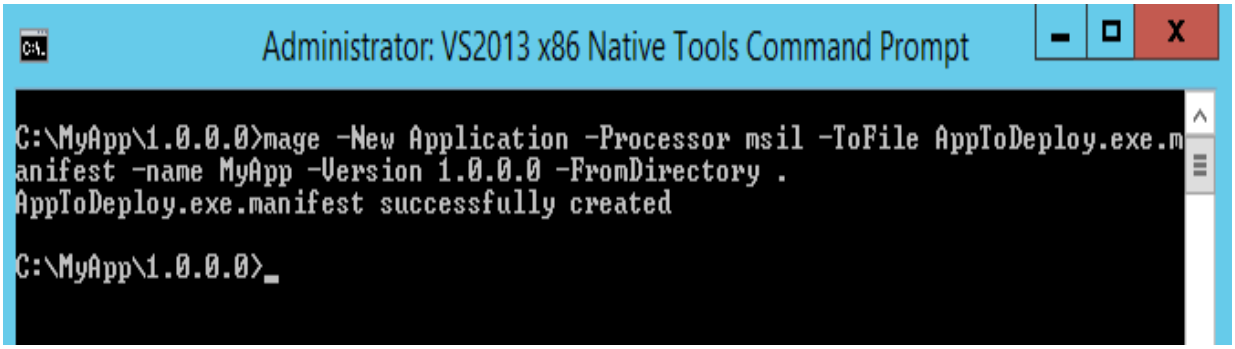
To deploy an application with the Mage.exe command-line tool

1. Create a directory where you will store your ClickOnce deployment files.
2. In the deployment directory you just created, create a version subdirectory. If this is the first time that you are deploying the application, name the version subdirectory 1.0.0.0.
3. Copy all of your application files to the version subdirectory, including executable files, assemblies, resources, and data files. If necessary, you can create additional subdirectories that contain additional files.
4. Open the Windows SDK or Visual Studio command prompt and change to the version subdirectory.
5. Create the application manifest with a call to Mage.exe. The following statement creates an application manifest for code compiled to run on the msil processor.

   ---

   mage -New Application -Processor msil -ToFile AppToDeploy.exe.manifest -name "MyApp" -Version 1.0.0.0 -FromDirectory .

   NOTE: Be sure to include the dot (.) after the -FromDirectory option, which indicates the current directory. If you do not include the dot, you must specify the path to your application files.

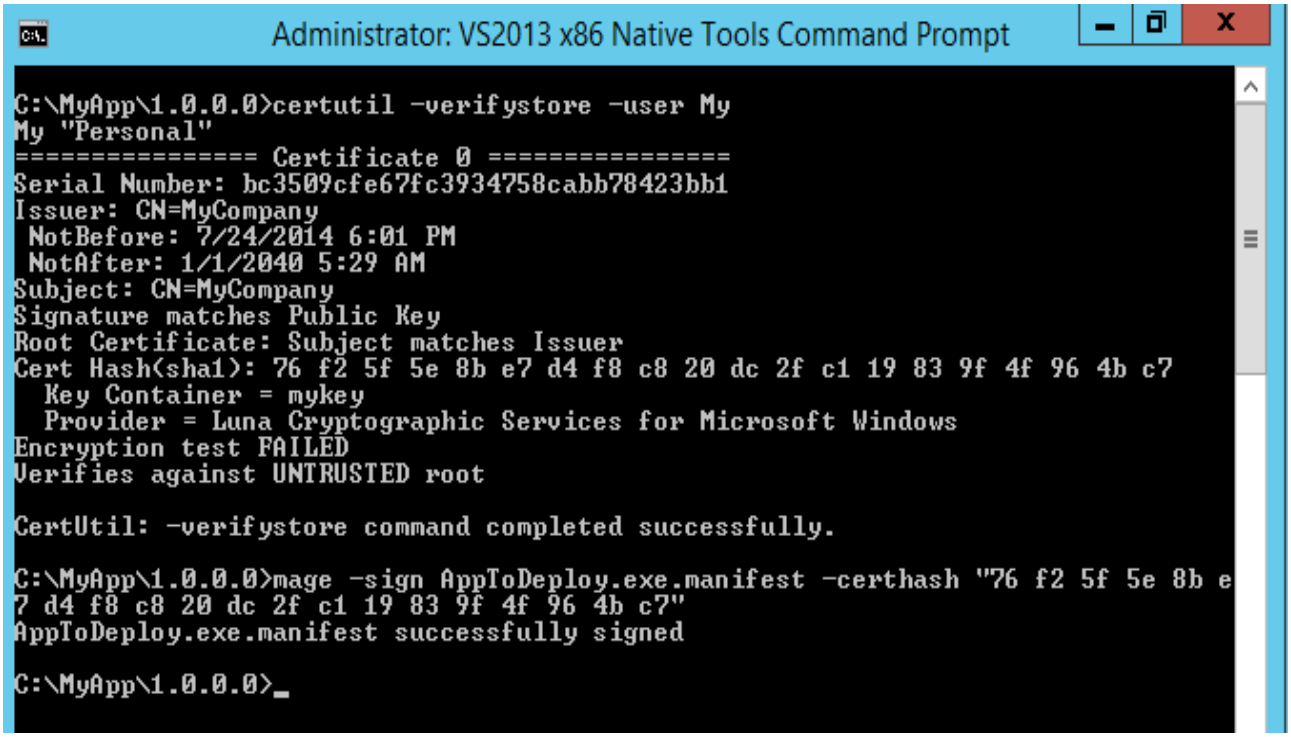
6. Sign the application manifest with your Authenticode certificate.

   ---

   mage -Sign AppToDeploy.exe.manifest -CertHash “Certificate Hash”

   NOTE: Run the certutil.exe to know the certificate hash value the command would be “Certutil -verifystore -user My”

   “My” is the user cert store where you have generated the certificate using Makecert.



7. Change to the root of the deployment directory.
8. Generate the deployment manifest with a call to Mage.exe. By default, Mage.exe will mark your ClickOnce deployment as an installed application, so that it can be run both online and offline. To make the application available only when the user is online, use the -Install option with a value of false. If you use the default, and users will install your application from a Web site or file share, make sure that the value of the -ProviderUrl option points to the location of the application manifest on the Web server or share.

   ---

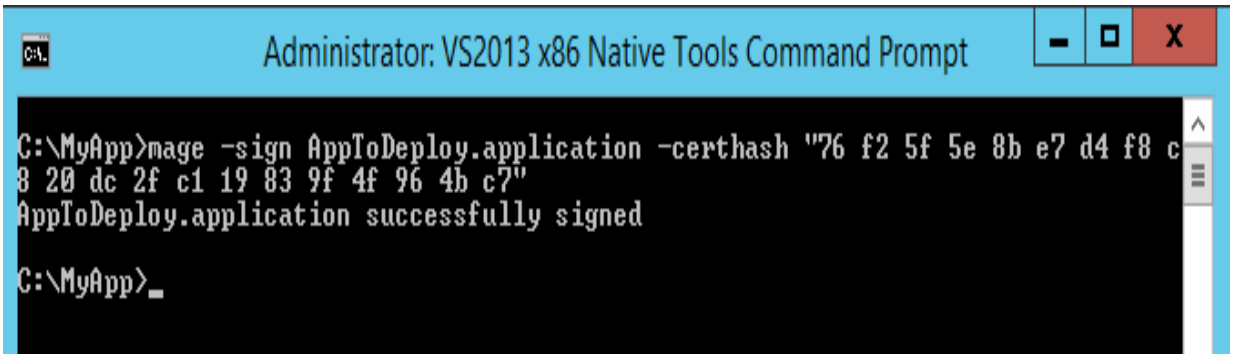
   mage -New Deployment -Processor msil -Install true -Publisher "My Company" -ProviderUrl “\\myServer\myShare\AppToDeploy.application" -AppManifest 1.0.0.0\AppToDeploy.exe.manifest -ToFile AppToDeploy.application

   ---

9. Sign the deployment manifest with your Authenticode certificate.

   ---

   mage -Sign AppToDeploy.application -CertHash “Certificate Hash”



10. Copy all of the files in the deployment directory to the deployment destination or media. This may be either a folder on a Web site or FTP site, a file share, or a CD-ROM.
11. Provide your users with the URL, UNC, or physical media required to install your application. If you provide a URL or a UNC, you must give your users the full path to the deployment manifest. For example, if AppToDeploy is deployed to http://webserver01/ in the AppToDeploy directory, the full URL path would be http://webserver01/AppToDeploy/AppToDeploy.application.

CHAPTER 7
Integrating Microsoft HCK (Windows Server 2012) with Luna HSM

Microsoft's Windows Certification Program is designed to help your company deliver compatible and reliable systems, software, and hardware products. End users trust the logo as an assurance of compatibility and reliability. This program is intended to help you develop systems and devices that have been tested to ensure that they meet Microsoft standards for Windows 8.1 as well as the quality level that ensures a great Windows experience for end users.

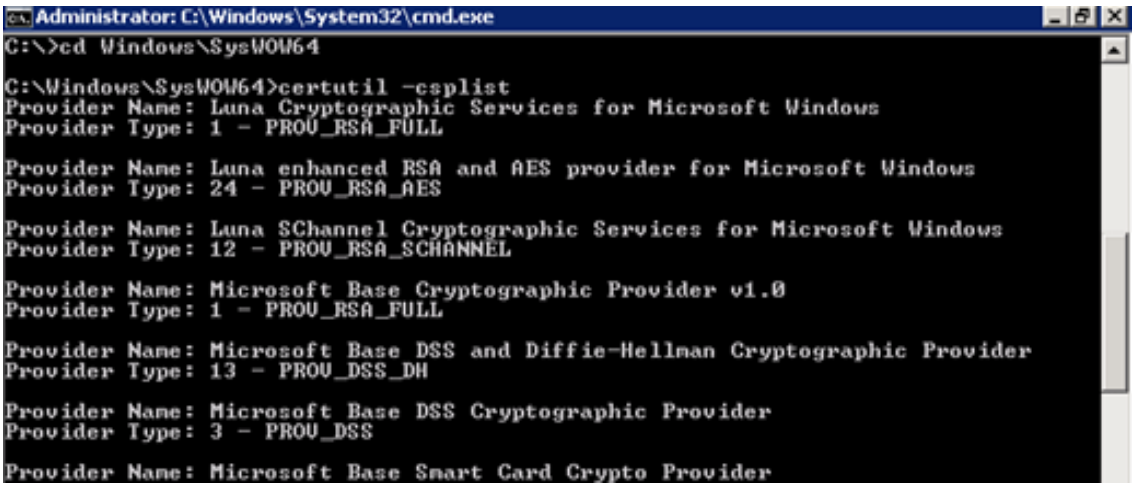
Luna HSM is used to secure the signing keys so that your signing keys never access by any unauthorized entity. Microsoft HCK uses the RSA keys for signing the packages.

Microsoft HCK is a 32 bit application so you have to use the 32 bit Luna Client with 32 bit CSP.

1. Install Luna Cryptographic Service Provider (CSP) on Windows Server.
    - Open the command prompt and run *register.exe* to register Luna CSP. The general form of command is

      <Luna Client Installation Directory>\win32\csp>register.exe
    - To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is

      <Luna Client Installation Directory>\win32\csp>register.exe /l
2. As this is a 32 bit setup, to verify the registered cryptographic providers, browse to "C:\Windows\SysWOW64" and execute "certutil –csplist"



3. In order to integrate the Luna SA Hardware Security Module with Microsoft HCK, the Luna CSP **"Luna Cryptographic Services for Microsoft Windows"** must be used to generate the certificate. The

certificate must be signed and the signer certificate must be present in the “Trusted Root Certificate Authority”. You can use the CA signed certificate of self-signed certificate both. There are two method that you can use to generate the signing certificate:

Method 1:

a) Create an inf file with the following attributes:

[Version]

Signature="$Windows NT$"

[NewRequest]

Subject = "C=US,O=SafeNet,CN=HCK,OU=HCKIntegration"

KeySpec = 1

KeyLength = 2048

Exportable = FALSE

MachineKeySet = TRUE

KeyContainer = HCK

ProviderName = "Luna Cryptographic Services for Microsoft Windows"

ProviderType = 1

KeyUsage = 0x04

---

b) Generate a certificate request using the created inf. Make sure to use the 32 bit certreq utility from “C:\Windows\SysWOW64” directory. A success message is displayed after this command has been executed.

c) Take the generated certificate request to a CA and get it signed to obtain a signed certificate.

d) Now we have to import this obtained certificate in the user’s personal certificate store. As this setup is 32 bit, ensure to use the 32 bit microsoft certificate manager console.

   C:\Windows\SysWOW64\certmgr.msc

e) Right Click on Personal -> All Task -> Import… and follow the instruction to import the signed certificate. Verify the certificate is successfully imported.

f) Double click the certificate and confirm that there is a private key mapped with this certificate. Check the message at the bottom.

g) In case, the private key is not mapped correctly, repair the certificate using the “certutil –repairstore” utility.

h) Open the certificate.

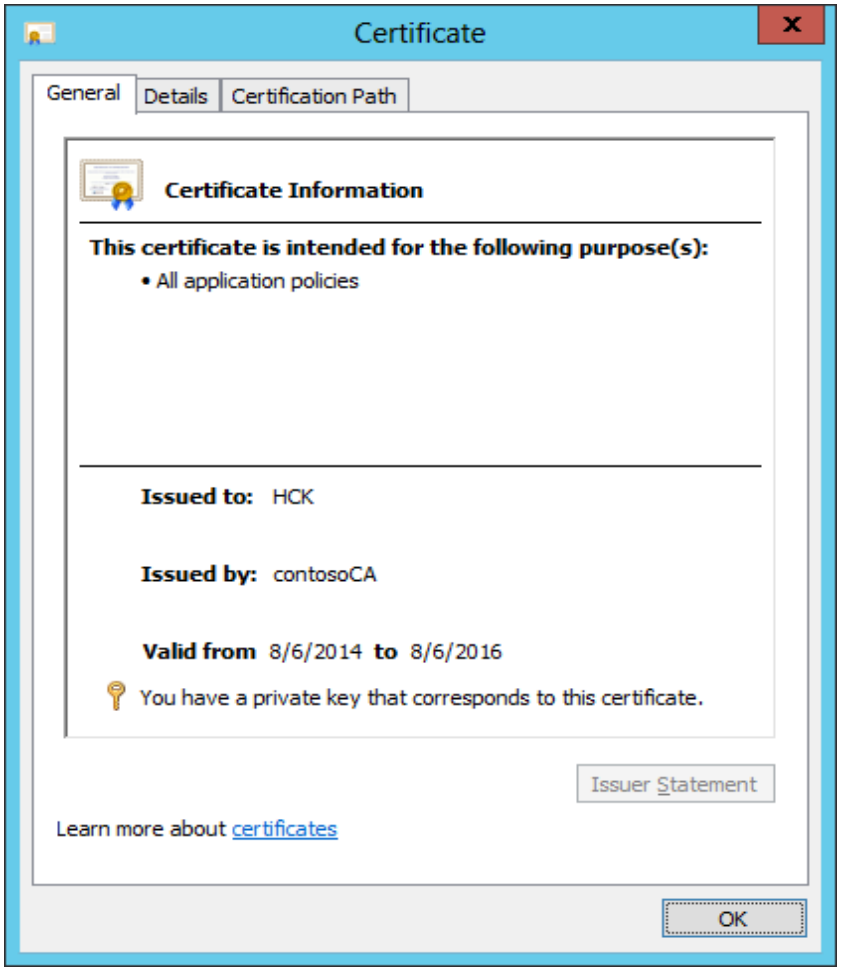
i) Browse to the details tab.

j) Select the serial number field.

k) Copy the serial number or thumb print.

l) Execute the “certutil -repairstore -user My “SerialNumber or ThumbPrint”” command from the SysWOW64 directory to map the private key (on the HSM) with the certificate.

m) After the repairstore command has been successfully executed, refresh the certificate manager snap in, open the certificate and confirm the message at the bottom is displayed.



Method 2:

a) Use the makecert utility to generate a self signed certificate. Browse to the “C:\Program Files (x86)\Windows Kits\8.1\bin\x86” directory and execute the following command:

---

makecert -sk <keyContainer> -sp "Luna Cryptographic Services for Microsoft Windows" -r -n “CN=Common Name” -ss <certStore> CertificateName.cer

---

Where:

-sk The location of the subject's key container which holds the private key

-sp Subject CryptoAPI's provider name

-n The name and details of the signer's certificate

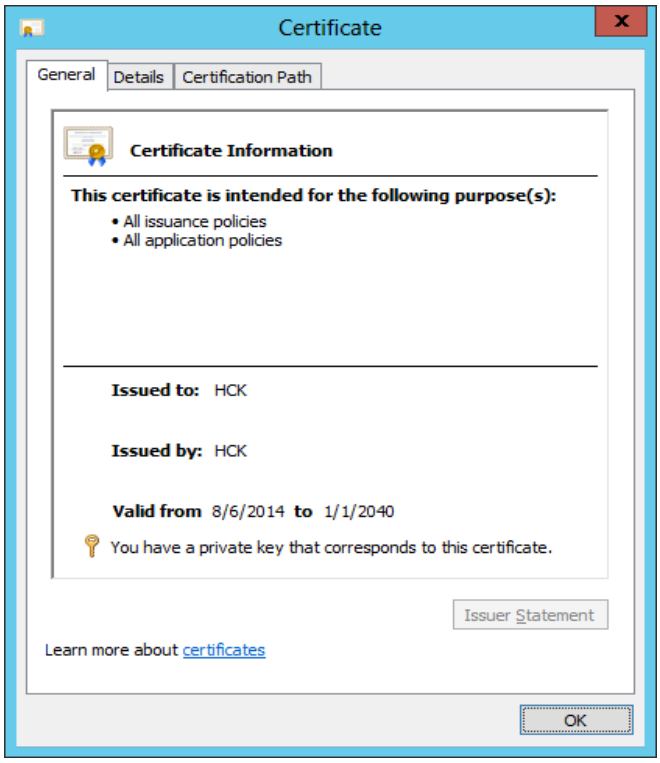
-ss The name of the subject's certificate store in which the generated certificate will be stored. Use "My" which is the default user cert store where the application is looking for certificate.

NOTE: Anything that contains spaces must be in double quotes ("").

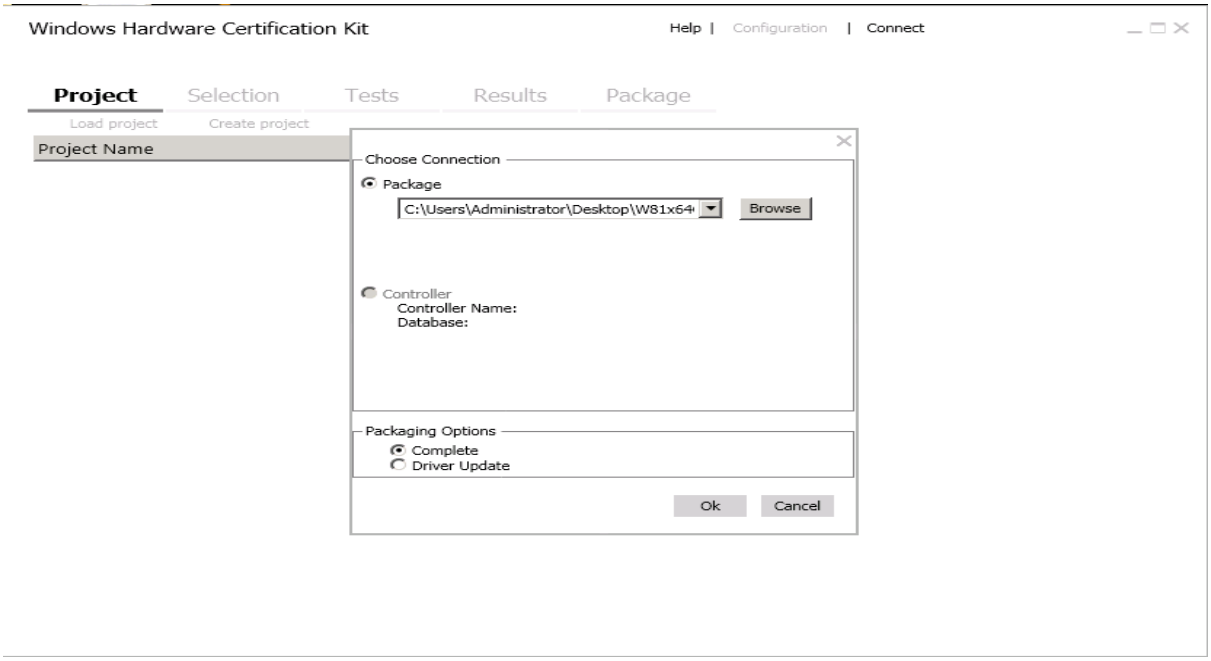
b) Open the certmgr.msc from the "C:\Windows\SysWOW64" directory and export the generated certificate from the Personal folder.

c) Import the certificate in the "Trusted Root Certificate Authority" Folder. Verify that certificate imported successfully.

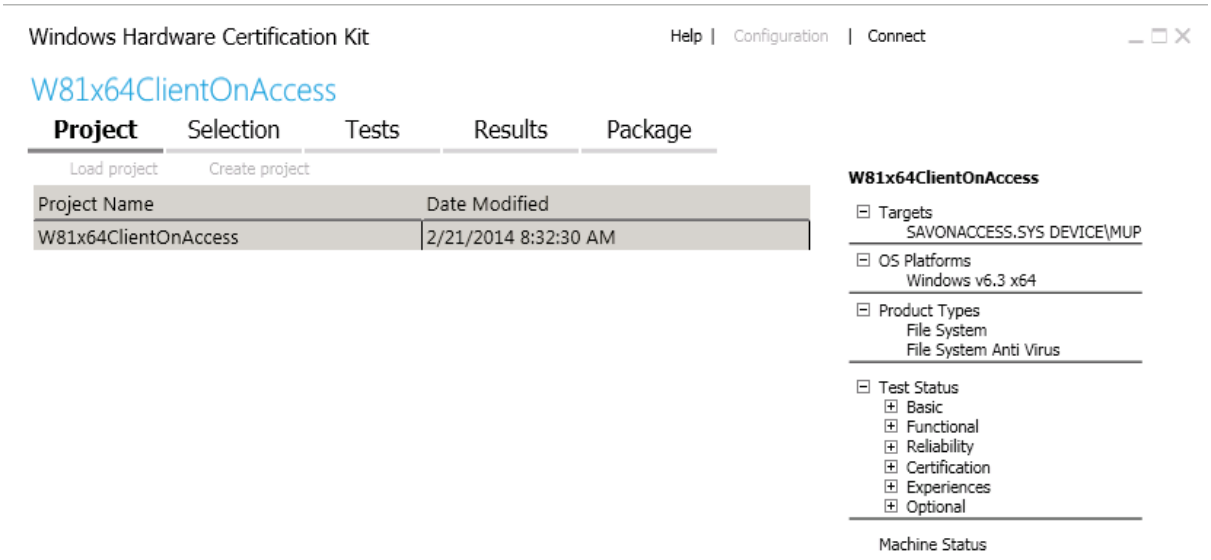
NOTE: We need to import the certificate because the signing certificate must be trusted.

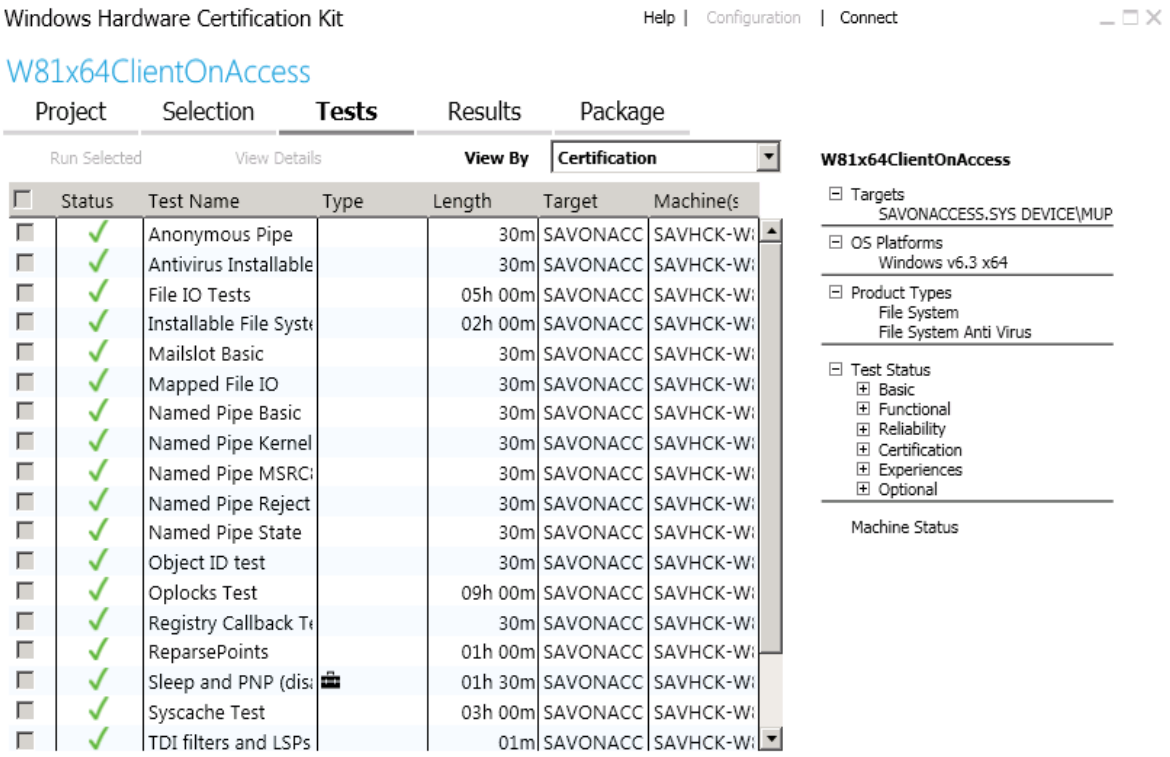


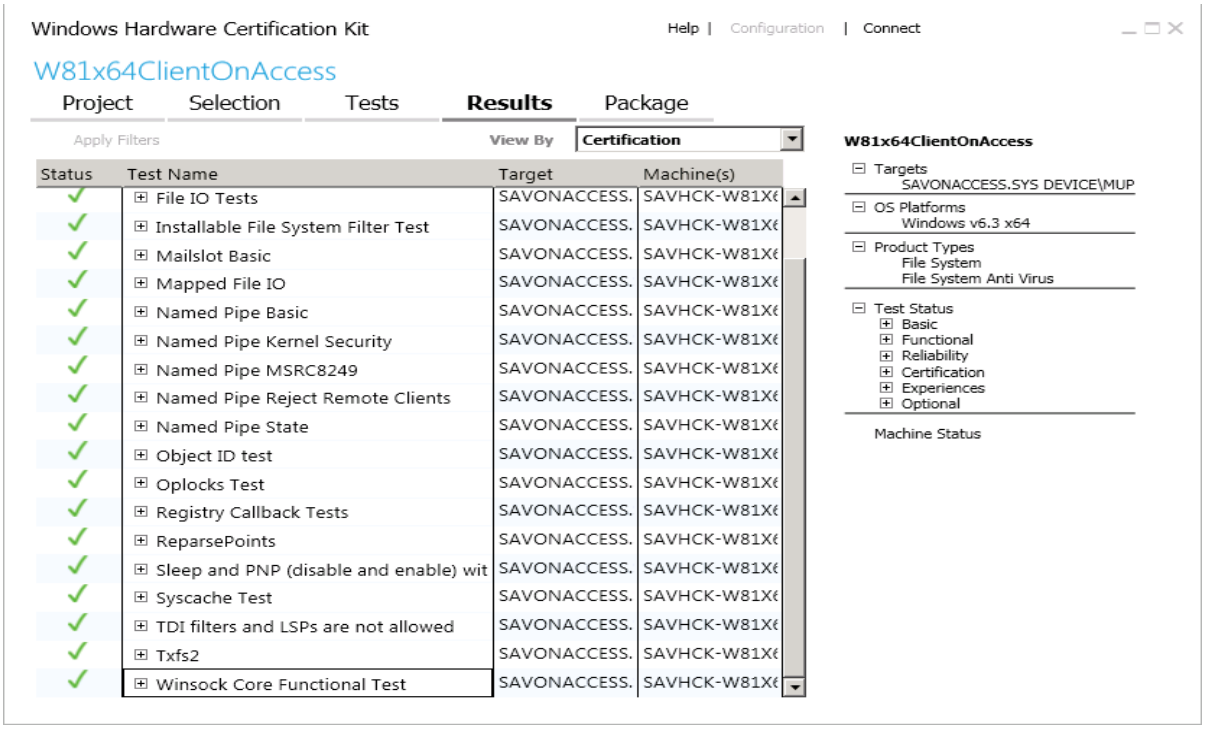
4. Now, as the certificate and the private is ready for signing, open Windows Hardware Certification Kit and import the project that you want to sign.



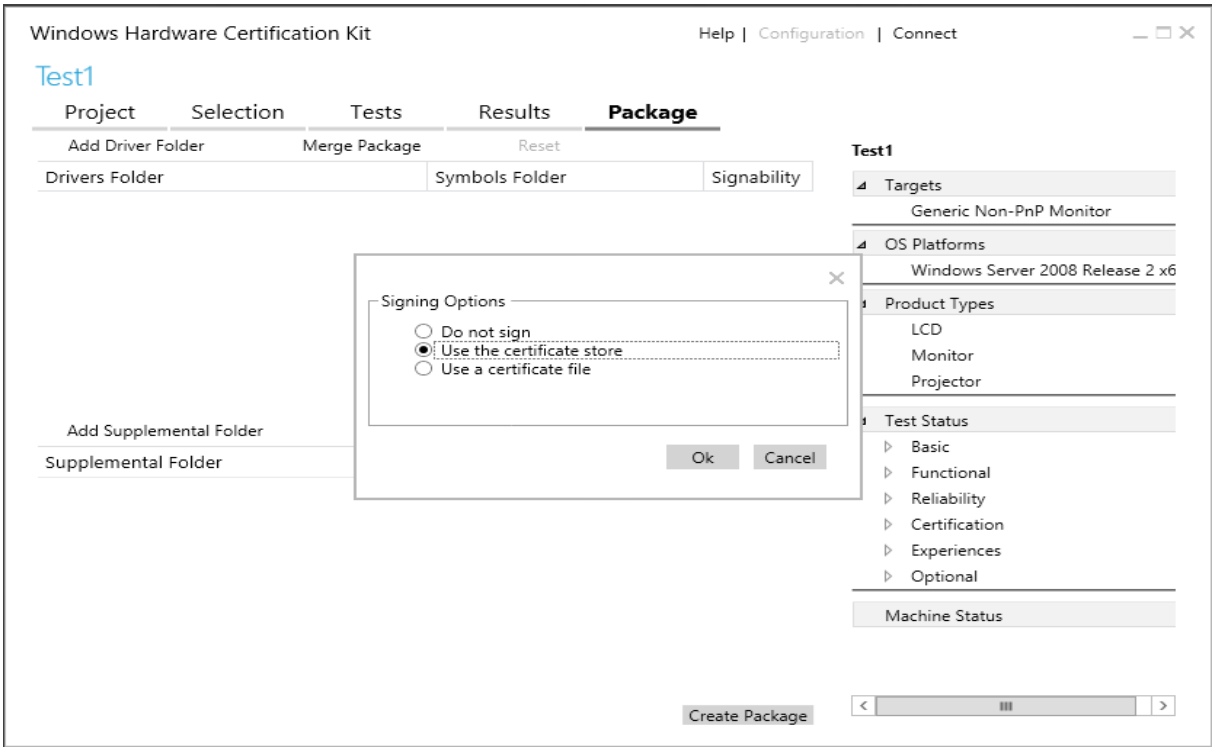
5. Browse through the various tabs to check if the project imported the correct one.



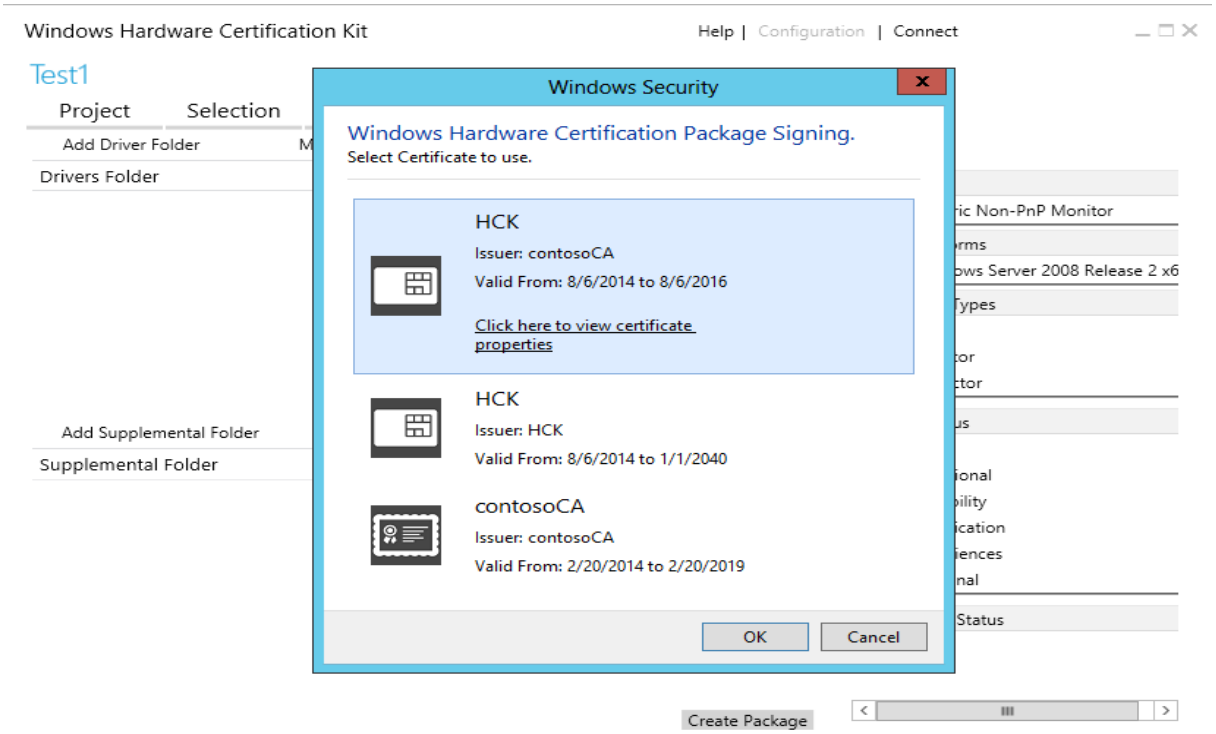

Windows Hardware Certification Kit
Help | Configuration | Connect
W81x64ClientOnAccess
Project Selection Tests Results Package
Run Selected View Details View By Certification
Status Test Name Type Length Target Machine(s
Anonymous Pipe 30m SAVONACC SAVHCK-W
Antivirus Installable 30m SAVONACC SAVHCK-W
File IO Tests 05h 00m SAVONACC SAVHCK-W
Installable File Syste 02h 00m SAVONACC SAVHCK-W
Mailslot Basic 30m SAVONACC SAVHCK-W
Mapped File IO 30m SAVONACC SAVHCK-W
Named Pipe Basic 30m SAVONACC SAVHCK-W
Named Pipe Kernel 30m SAVONACC SAVHCK-W
Named Pipe MSRC 30m SAVONACC SAVHCK-W
Named Pipe Reject 30m SAVONACC SAVHCK-W
Named Pipe State 30m SAVONACC SAVHCK-W
Object ID test 30m SAVONACC SAVHCK-W
Oplocks Test 09h 00m SAVONACC SAVHCK-W
Registry Callback T 30m SAVONACC SAVHCK-W
ReparsePoints 01h 00m SAVONACC SAVHCK-W
Sleep and PNP (dis 01h 30m SAVONACC SAVHCK-W
Syscache Test 03h 00m SAVONACC SAVHCK-W
TDI filters and LSPs 01m SAVONACC SAVHCK-W
W81x64ClientOnAccess
Targets
SAVONACCESS.SYS DEVICE\MUP
OS Platforms
Windows v6.3 x64
Product Types
File System
File System Anti Virus
Test Status
Basic
Functional
Reliability
Certification
Experiences
Optional
Machine Status


Windows Hardware Certification Kit
Help | Configuration | Connect
W81x64ClientOnAccess
Project Selection Tests Results Package
Apply Filters View By Certification
Status Test Name Target Machine(s)
File IO Tests SAVONACCESS. SAVHCK-W81X
Installable File System Filter Test SAVONACCESS. SAVHCK-W81X
Mailslot Basic SAVONACCESS. SAVHCK-W81X
Mapped File IO SAVONACCESS. SAVHCK-W81X
Named Pipe Basic SAVONACCESS. SAVHCK-W81X
Named Pipe Kernel Security SAVONACCESS. SAVHCK-W81X
Named Pipe MSRC8249 SAVONACCESS. SAVHCK-W81X
Named Pipe Reject Remote Clients SAVONACCESS. SAVHCK-W81X
Named Pipe State SAVONACCESS. SAVHCK-W81X
Object ID test SAVONACCESS. SAVHCK-W81X
Oplocks Test SAVONACCESS. SAVHCK-W81X
Registry Callback Tests SAVONACCESS. SAVHCK-W81X
ReparsePoints SAVONACCESS. SAVHCK-W81X
Sleep and PNP (disable and enable) wit SAVONACCESS. SAVHCK-W81X
Syscache Test SAVONACCESS. SAVHCK-W81X
TDI filters and LSPs are not allowed SAVONACCESS. SAVHCK-W81X
Txfs2 SAVONACCESS. SAVHCK-W81X
Winsock Core Functional Test SAVONACCESS. SAVHCK-W81X
W81x64ClientOnAccess
Targets
SAVONACCESS.SYS DEVICE\MUP
OS Platforms
Windows v6.3 x64
Product Types
File System
File System Anti Virus
Test Status
Basic
Functional
Reliability
Certification
Experiences
Optional
Machine Status

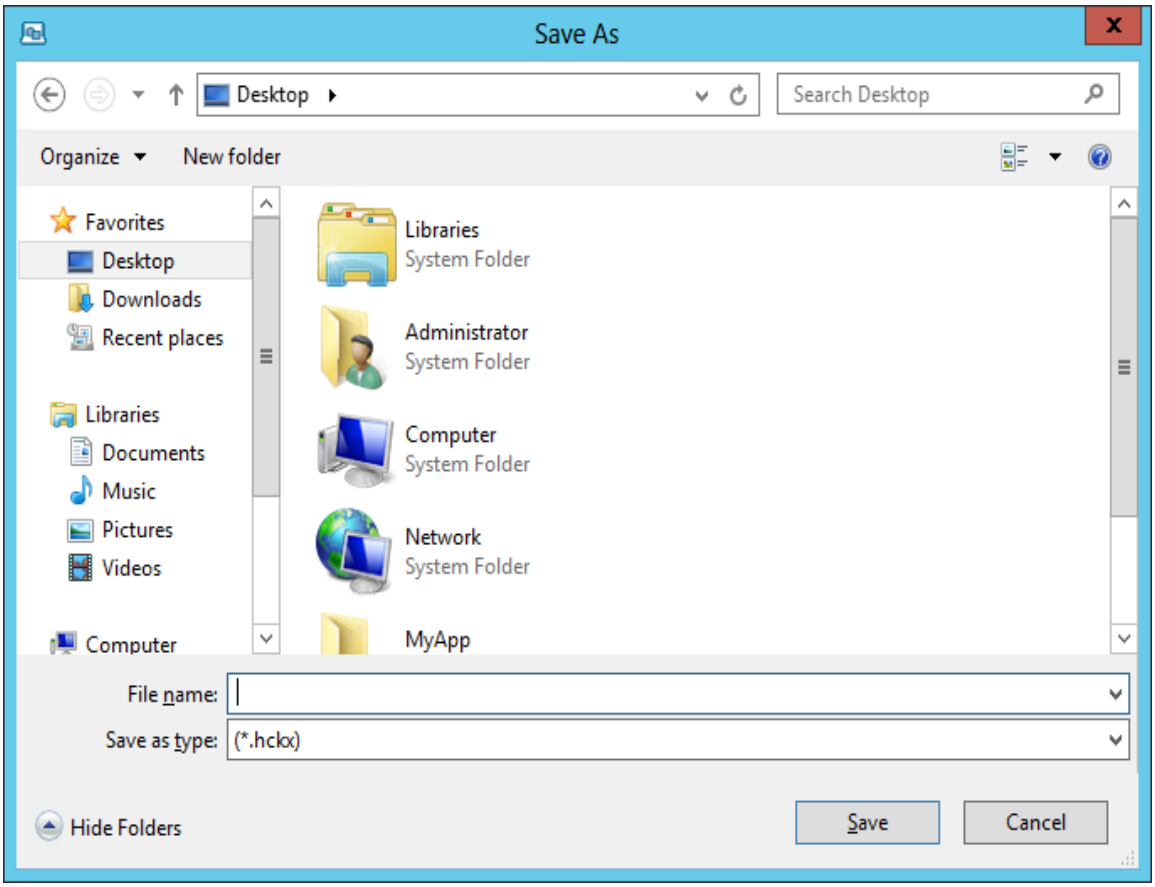
6. After verification, go to the package tab and click on create package to sign the package. You will be asked for how do you want to sign the package? Select “Use certificate Store” and click on Ok.



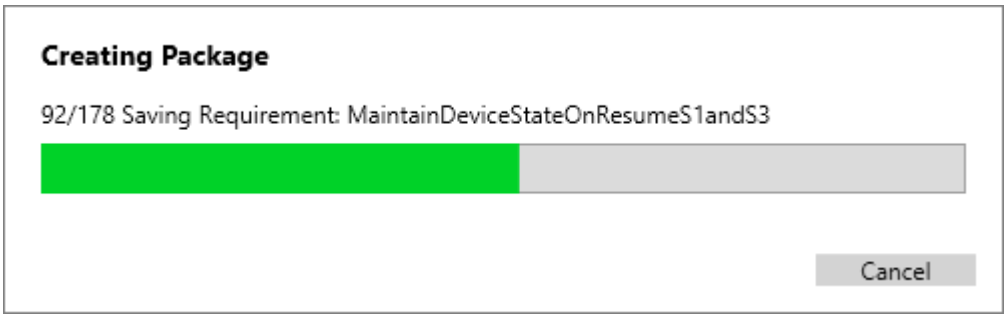
7. Next is to select the signing certificate. From the pop up, select the certificate that was imported earlier on the local machine’s personal certificate store and click OK.



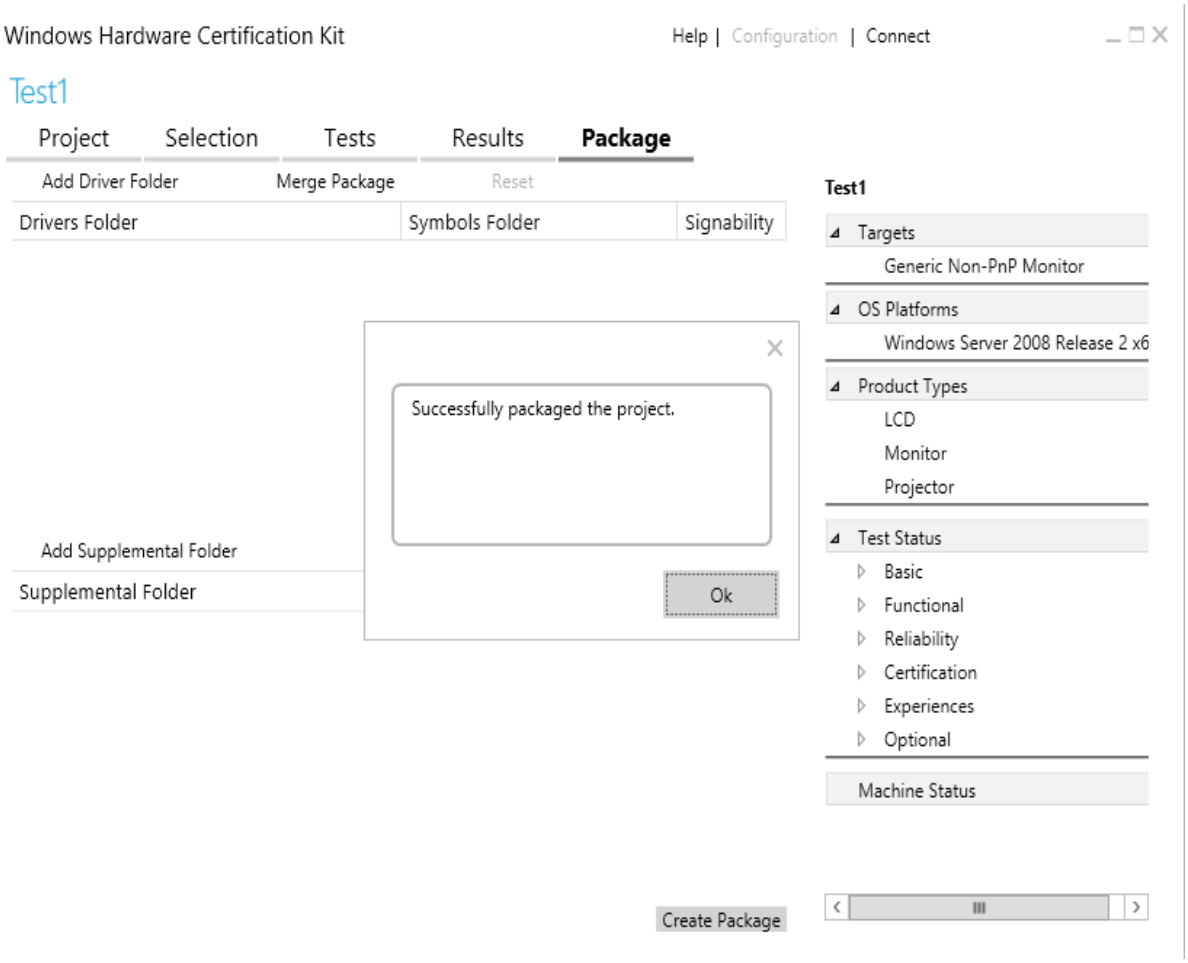
8. Select a location to save the signed package and click on Save.



9. As soon as you click on Save, signing will begin with a 'Creating Package' window.



10. In the end, if the certificate and the private key are correctly mapped, a success message is displayed and you can verify the signed package in the location you saved it.


Windows Hardware Certification Kit
Help | Configuration | Connect
Test1
Project
Selection
Tests
Results
Package
Add Driver Folder
Merge Package
Reset
Drivers Folder
Symbols Folder
Signability
Successfully packaged the project.
Ok
Add Supplemental Folder
Supplemental Folder
Create Package
Test1
Targets
Generic Non-PnP Monitor
OS Platforms
Windows Server 2008 Release 2 x6
Product Types
LCD
Monitor
Projector
Test Status
Basic
Functional
Reliability
Certification
Experiences
Optional
Machine Status

CHAPTER 8
Troubleshooting Tips

Problem: If you are operating HSM in FIPS Mode and you are facing the following problem while running the Makecert command to generate the certificate:

Error: CryptHashPublicKeyInfo failed => 0x80090005 (-2146893819) Failed.

Solution: The cert always has an MD5 hash in it. Configure the Luna CSP to do MD5 in software. The general form of command is as follows:

Windows Server 2008 (32 bit) - C:\Program Files\LunaSA\CSP>Register.exe /algorithms

Windows Server 2008 (64 bit) - C:\Program Files (x86)\LunaSA\CSP>Register.exe /algorithms

It will prompt you to register the various algorithms; you need to register the MD5 algorithms in software.