Microsoft Windows Hardware Lab Kit (HLK)

Integration Guide

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: 007-000099-001, Rev. A

Release Date: May 2018

Contents

Preface

This document is intended to guide security administrators to configure and integrate Windows Hardware Lab Kit (HLK) with SafeNet Luna Hardware Security Module (HSM).

Scope

This document describes the steps necessary to configure and integrate Windows Hardware Lab Kit (HLK) with SafeNet Luna HSM and signing of a HLK package.

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

The Windows Hardware Lab Kit (Windows HLK) is a test automation framework provided by Microsoft to certify devices for Windows. Microsoft's Windows Certification Program (previously known as the Windows Logo Program (WLP)), lays out procedures for submitting hardware and software modules, including drivers, for Microsoft quality assurance tests. Passing the tests qualifies the hardware/software for Microsoft certification, which verifies both the driver provider's authenticity and the driver's safety and functionality.

To digitally sign and certify a device driver, a Windows Hardware Lab Kit (HLK) package, which includes the driver and the related hardware, should be submitted to the Windows Certification Program for testing, using the Windows Dev Center Hardware Dashboard Services (the Hardware Dashboard). SafeNet Luna HSM is used to secure the package signing keys.

The benefits of using SafeNet HSMs to generate the RSA signing keys for Windows HLK are:

- Secure generation, storage and protection of the signing private keys on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- HSM audit trail.
- Significant performance improvements by off-loading cryptographic operations from signing servers.

Understanding Windows Hardware Lab Kit (Windows HLK)

Windows Hardware Lab Kit (Windows HLK) is a test framework used to test hardware devices for Windows 10/Windows 2016.

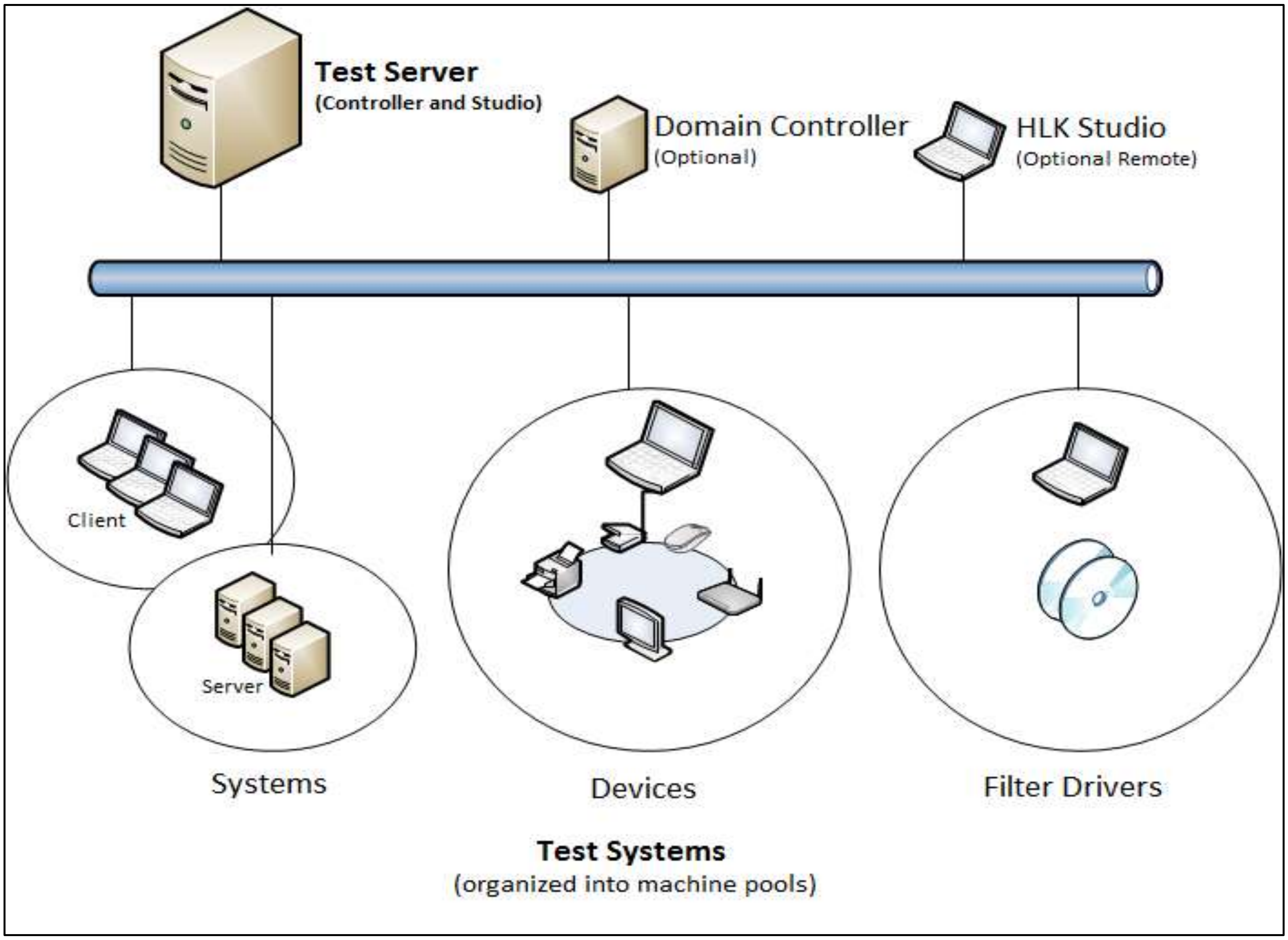
Windows HLK is comprised of two components: an HLK test server and one or more test systems.

HLK test server. Often referred to as the *controller*, a test server has two parts: Windows HLK Controller and Windows HLK Studio. The Controller software is the engine that manages tests that are run on test systems. The Studio software is the management tool that lets you select and schedule tests against any test system connected to the test server. Controller and Studio are installed from the Windows HLK installation source. After installation, the test server contains separate installers to install a remote Windows HLK Studio and Windows HLK Client.
One controller governs a collection of client computers. Controllers can manage and access only the client computers that they govern.

Test system. Also referred to as a client computer, each test system can have a different configuration that's appropriate for various testing scenarios, including different hardware, operating systems, service packs, and drivers. Each test system can be associated with only one test server. You can configure each test system by running the Windows HLK Client software installer directly from a shared network location on the test server.

To test systems and filter drivers, you need at least 1 test server and 1 test system.
To test external devices, you need at least 1 test server, 1 test system, and the external device(s) to be tested.

The following image shows a sample test environment.



3rd Party Application Details

Windows Hardware Lab Kit (HLK)

Supported Platforms

Microsoft Windows HLK has been tested with the following:

Platforms Tested	SafeNet Luna HSM Appliance Software version	SafeNet Luna HSM Client Software version	Firmware Version
Window Server 2016	7.1.0	7.1.0	7.1.0
Window Server 2016	6.3.0	6.3.0	6.27.0

NOTE: HLK is tested with SafeNet Luna HSM in FIPS and Non FIPS Mode.

Prerequisites

Configuring SafeNet Luna Network HSM 7.x

SafeNet Luna Network HSM allows to create Per-Partition Security Officer (PPSO) partition. HSM Administrator is not Security Officer (SO) for PPSO partitions. The HSM SO/Administrator elects to create a partition as PPSO-type, which creates an empty structure that is handed to the new owner, who initializes the partition to create the Partition Security Officer (PSO) role or identity for management functions. The PSO in turn creates the partition Crypto Officer (CO) to control client cryptographic operations on the partition.

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX/Windows systems. Before you get started ensure the following:

- SafeNet Luna Network HSM appliance and a secure admin password.
- SafeNet Luna Network HSM, and a hostname, suitable for your network.
- SafeNet Luna Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Luna Network HSM appliance.
- Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
- Create a partition on the HSM that will be later used by HLK.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Luna HSM. The general form of command is `"C:\Program Files\SafeNet\LunaClient> vtl verify"` for Windows.
- Initialize the Partition and its roles as mentioned in SafeNet Luna HSM documentation.

- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Luna Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Configuring SafeNet Luna Network HSM (6.x)

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX systems. Before you get started ensure the following:

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

Using Luna 6.x/7.x in FIPS Mode

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

NOTE: The above configuration is valid for Luna 7.x and Luna 6.x (F/W Version 6.22.0 and above only).

Windows HLK Setup

There are two deployment scenarios for Windows HLK:

1. **Domain-joined environment:** In a domain-joined environment, a domain controller is present and all computers designated for Windows HLK features are joined to the same domain controller. If you plan to deploy Windows HLK in a domain-joined environment, you need a minimum of three computers: a Windows domain controller, a Windows HLK test server, and at least one Windows HLK test system. Ensure that Microsoft Active Directory is configured and running on the domain controller. Your domain controller and HLK test server cannot be on the same box.

2. **Workgroup environment:** A workgroup environment has no domain controller. If you plan to deploy Windows HLK in a workgroup, you need at least two computers: a test server and a test system joined to the same workgroup. Don't use the Default Administrator account. In this configuration, you must enable the Guest account.

For Installing and Configuring Windows HLK, refer to the *Microsoft Windows Hardware Lab Kit documentation.*

2
Integrating SafeNet Luna HSM with Windows HLK

Configuring Windows HLK to use SafeNet Luna HSM for Package Signing

Perform the following steps to secure the HLK signing keys on SafeNet Luna HSM:

Register CSP

SafeNet Luna CSP must be installed on the HLK Test Server machine to use CSP generated keys for HLK signing.

- Log on to **HLK Test Server** as domain administrator.
- Run the command, **register.exe** to register Luna CSP. The general form of command is as follows:

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

  Provide the partition password when prompt.
- To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is as follows:

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

Creating Code Signing certificate

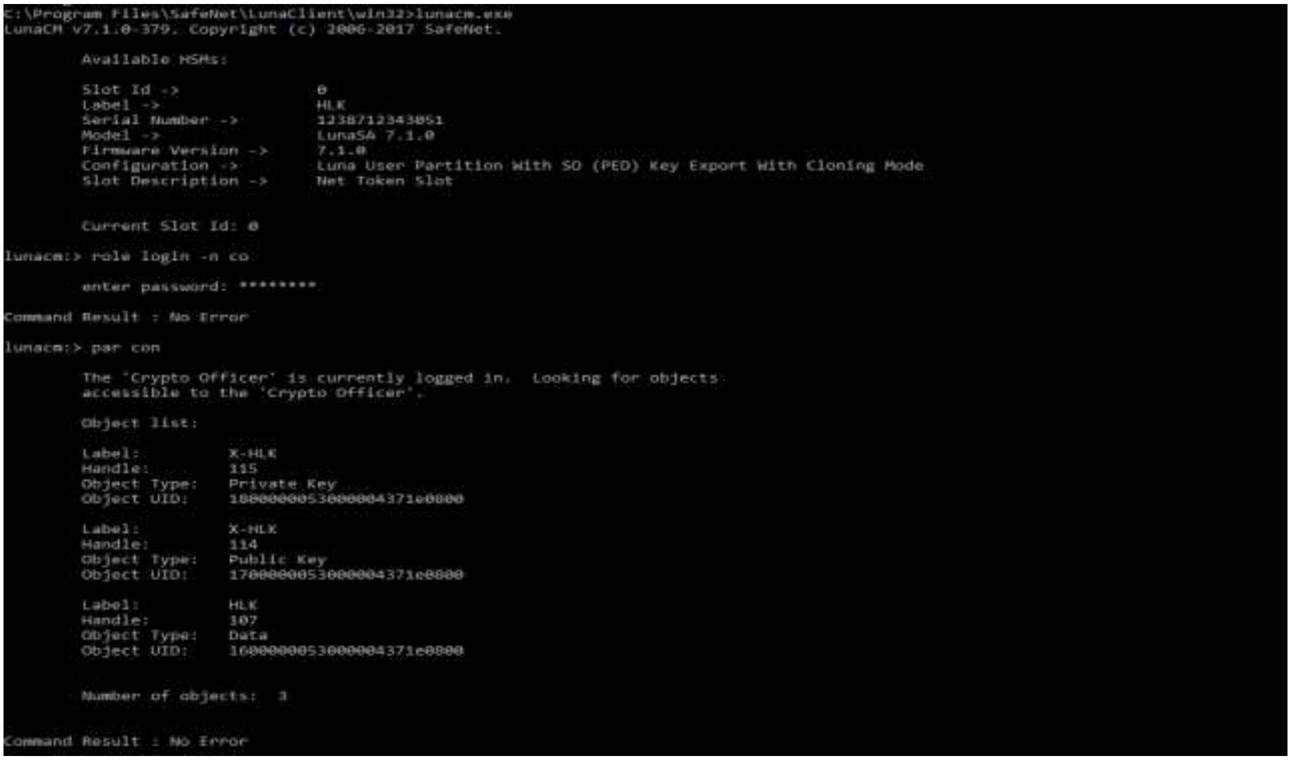
In order to integrate the SafeNet Luna HSM with Windows HLK, **Luna Cryptographic Services for Microsoft Windows** must be used to generate the certificate. The certificate must be signed and the signer certificate must be present in the "**Trusted Root Certificate Authority**".

1. Create a **request.inf** file with the following attributes on HLK Test Server:

   ```
   [Version]
   Signature="$Windows NT$"
   [NewRequest]
   Subject = "C=IN,O=Gemalto,CN=HLK,OU=HLKIntegration"
   KeySpec = 1
   KeyLength = 2048
   Exportable = FALSE
   MachineKeySet = FALSE
   KeyContainer = HLK
   ProviderName = "Luna Cryptographic Services for Microsoft Windows"
   ProviderType = 1
   ```

```
KeyUsage = 0x04
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.3
```

You can view the RSA keys generated on the Luna SA HSM partition.



```
C:\Program Files\SafeNet\LunaClient\win32>lunacm.exe
LunaCM v7.1.0-379. Copyright (c) 2006-2017 SafeNet.

        Available HSMs:

        Slot Id ->                      0
        Label ->                        HLK
        Serial Number ->                1238712343051
        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

        Current Slot Id: 0

lunacm:> role login -n co

        enter password: ********

Command Result : No Error

lunacm:> par con

        The 'Crypto Officer' is currently logged in.  Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          X-HLK
        Handle:         115
        Object Type:    Private Key
        Object UID:     18000000530000004371e00800

        Label:          X-HLK
        Handle:         114
        Object Type:    Public Key
        Object UID:     17000000530000004371e08800

        Label:          HLK
        Handle:         107
        Object Type:    Data
        Object UID:     16000000530000004371e08800

        Number of objects:  3

Command Result : No Error
```

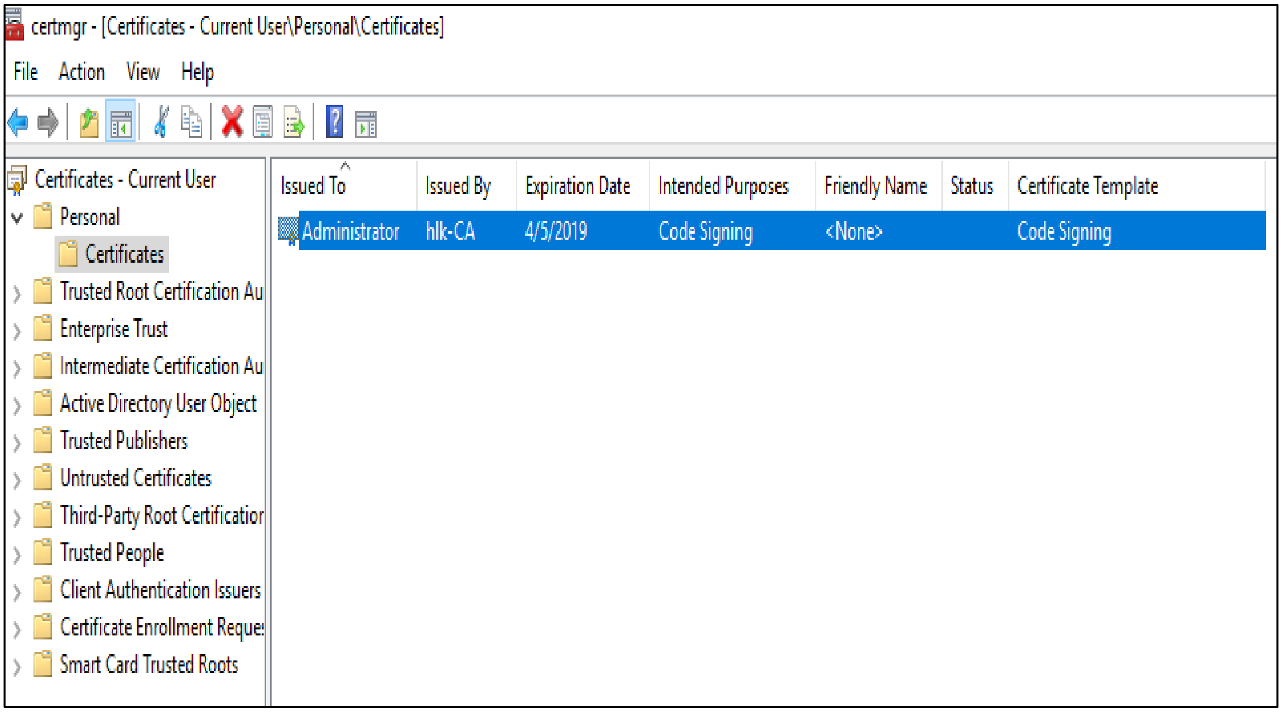
2. Generate a certificate request using the **request.inf** file. To create the certificate request for the HLK signing, execute the command:
   `certreq.exe -new request.inf request.req`

   This creates a certificate request file **request.req** that is required to send to a Certificate Authority for Signing Certificate. Submit the generated certificate request to your CA, select **Code Signing** template and get it signed to obtain a signed certificate.

3. Now import the signed certificate in the user's personal certificate store. To import the signed certificate execute the below command:

   ```
   certreq.exe -accept <Path to the Signed Certificate>
   ```

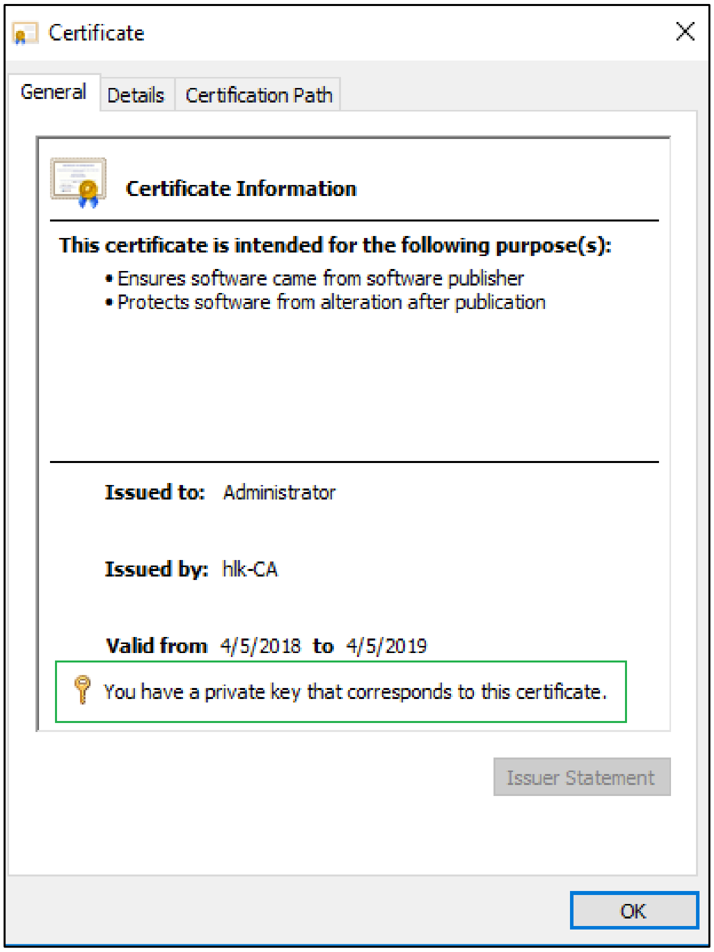
4. Open the **certmgr.msc,** double click on **Personal** -> **Certificates** and verify the certificate is successfully imported.



certmgr - [Certificates - Current User\Personal\Certificates]
File Action View Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Certificate Enrollment Reque:
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
Administrator	hlk-CA	4/5/2019	Code Signing	<None>		Code Signing

5. Double-click the certificate and check the message at the bottom to confirm that there is a private key mapped with this certificate.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Administrator

Issued by: hlk-CA

Valid from 4/5/2018 **to** 4/5/2019

You have a private key that corresponds to this certificate.

In case, the private key is not mapped correctly, repair the certificate. Open the certificate and go to the **Details** tab. Copy the **serial number** or **thumb print** of the certificate.

Execute the following command to map the private key with the certificate.

```
certutil -repairstore –csp "Luna Cryptographic Services for Microsoft Windows" -user My
"SerialNumber or ThumbPrint"
```

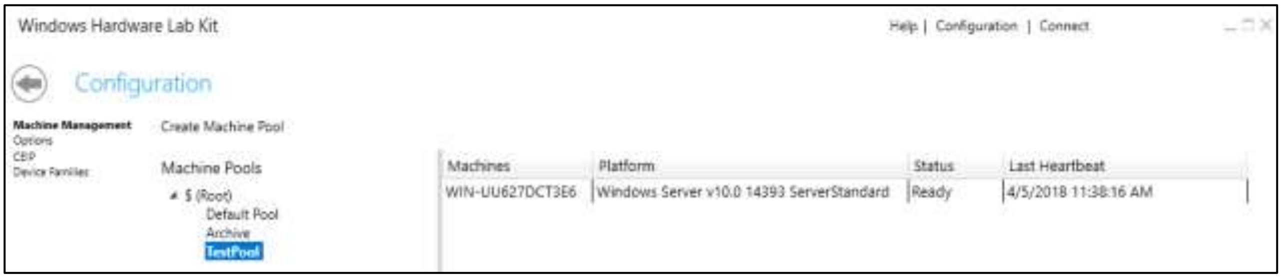
After the `repairstore` command has been successfully executed, refresh the certificate manager snap in, open the certificate and confirm the message at the bottom "**You have a private key that corresponds to this certificate**" is displayed.

Signing the HLK Packages

After generating the certificate and private keys on SafeNet Luna HSM. Perform the below steps for signing the package:

1. Open **Windows HLK Studio** on HLK Test Server

   Ensure that **HLK Test Clients** are listed in **Configuration** Tab under **Default Pool.** Create the new pool and move the machine to the newly created pool. Ensure the status is "**Ready**".

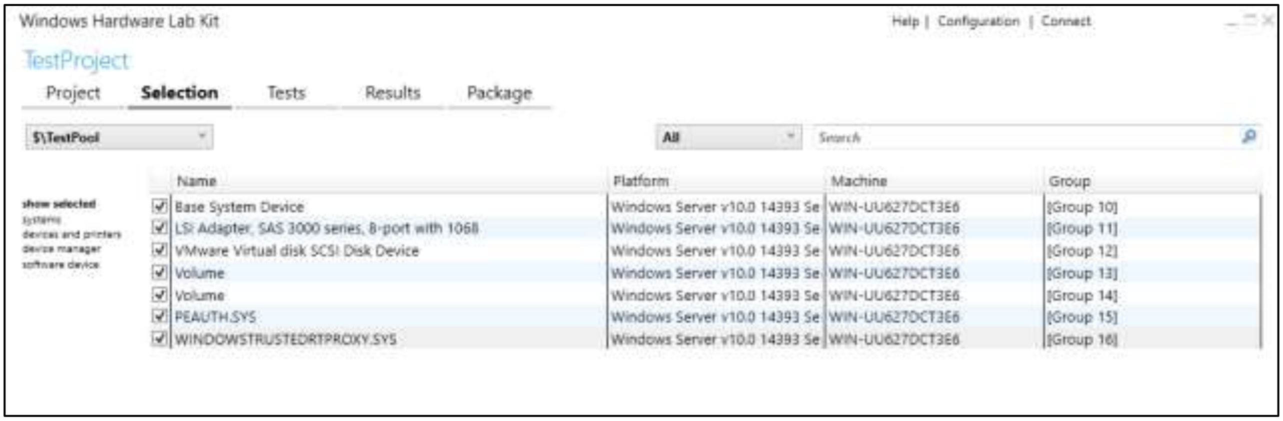


Machines	Platform	Status	Last Heartbeat
WIN-UU627DCT3E6	Windows Server v10.0 14393 ServerStandard	Ready	4/5/2018 11:38:16 AM

NOTE: If the HLK Test Client is not listed in Default Pool or the status is stuck at "Initializing", try rebooting the HLK Test Client machine.

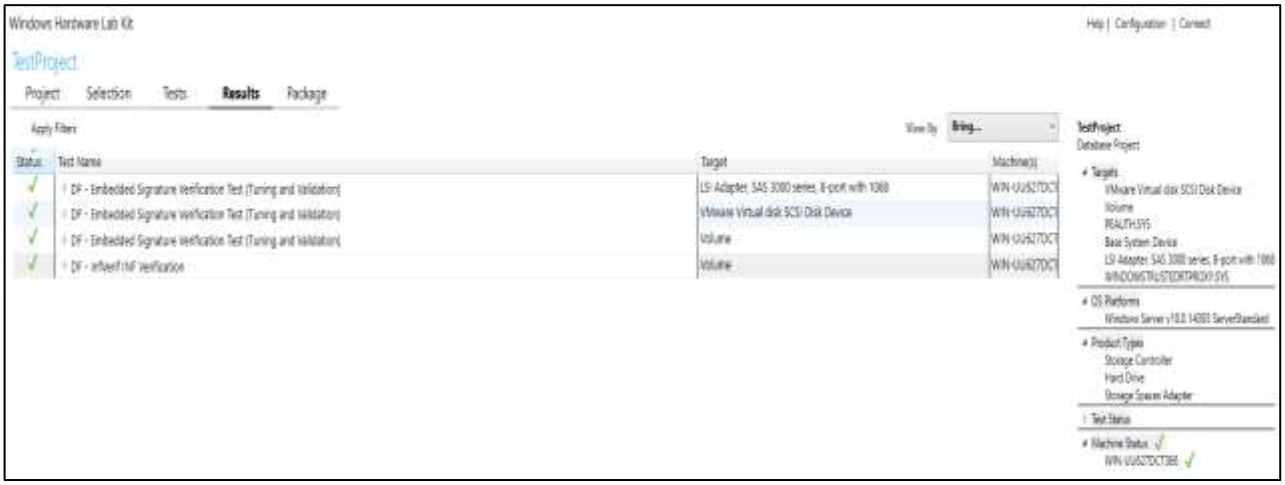
Create a new project or import an existing project for signing.

2. Browse through the **Selection** tab to check if the project created/imported is listed. Select the packages for signing.



	Name	Platform	Machine	Group
☑	Base System Device	Windows Server v10.0 14393 Se	WIN-UU627DCT3E6	[Group 10]
☑	LSI Adapter, SAS 3000 series, 8-port with 1068	Windows Server v10.0 14393 Se	WIN-UU627DCT3E6	[Group 11]
☑	VMware Virtual disk SCSI Disk Device	Windows Server v10.0 14393 Se	WIN-UU627DCT3E6	[Group 12]
☑	Volume	Windows Server v10.0 14393 Se	WIN-UU627DCT3E6	[Group 13]
☑	Volume	Windows Server v10.0 14393 Se	WIN-UU627DCT3E6	[Group 14]
☑	PEAUTH.SYS	Windows Server v10.0 14393 Se	WIN-UU627DCT3E6	[Group 15]
☑	WINDOWSTRUSTEDRTPROXY.SYS	Windows Server v10.0 14393 Se	WIN-UU627DCT3E6	[Group 16]

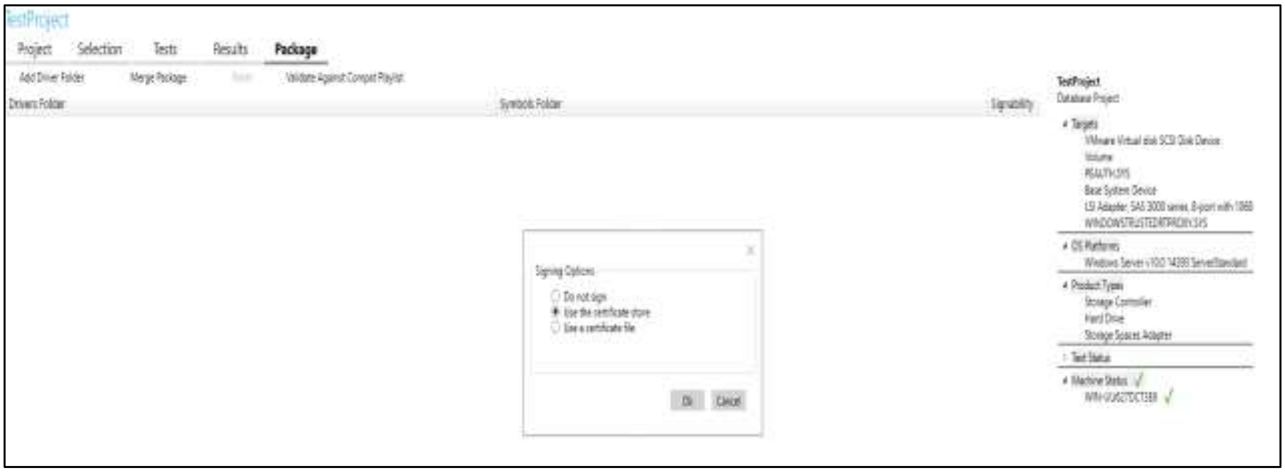
3. Browse through the **Test** tab to test selected packages and ensure that **Result** tab displays Test Verification as successful.



Status	Test Name	Target	Machine(s)
✓	DF - Embedded Signature Verification Test (Tuning and Validation)	LSI Adapter, SAS 3000 series, 8-port with 1068	WIN-UU627DCT
✓	DF - Embedded Signature Verification Test (Tuning and Validation)	VMware Virtual disk SCSI Disk Device	WIN-UU627DCT
✓	DF - Embedded Signature Verification Test (Tuning and Validation)	Volume	WIN-UU627DCT
✓	DF - InfVerif INF Verification	Volume	WIN-UU627DCT

TestProject
Database Project
- Targets
  - VMware Virtual disk SCSI Disk Device
  - Volume
  - PEAUTH.SYS
  - Base System Device
  - LSI Adapter, SAS 3000 series, 8-port with 1068
  - WINDOWSTRUSTEDRTPROXY.SYS
- OS Platforms
  - Windows Server v10.0 14393 ServerStandard
- Product Types
  - Storage Controller
  - Hard Drive
  - Storage Spaces Adapter
- Test Status
- Machine Status ✓
  - WIN-UU627DCT3E6 ✓

4. After successful Test Verification, select the **Package** tab and click on **Create Package** to sign the package. When prompted for **Signing Options** Select **Use the certificate store** and click **OK.**



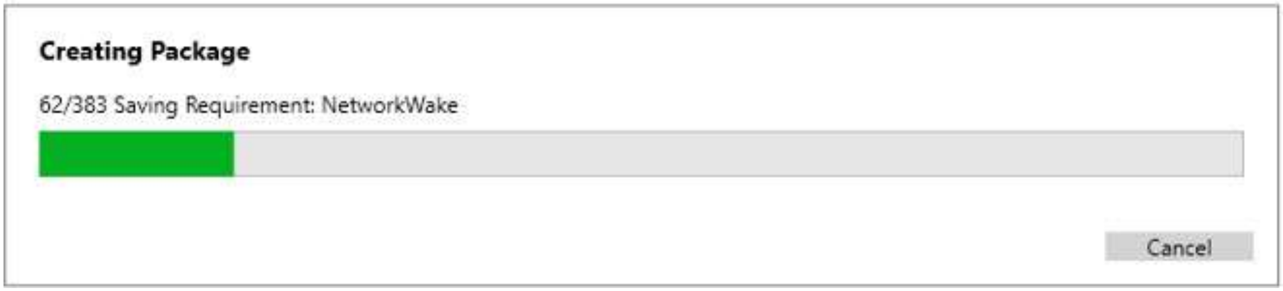
Signing Options
○ Do not sign
● Use the certificate store
○ Use a certificate file

TestProject
Database Project
- Targets
  - VMware Virtual disk SCSI Disk Device
  - Volume
  - PEAUTH.SYS
  - Base System Device
  - LSI Adapter, SAS 3000 series, 8-port with 1068
  - WINDOWSTRUSTEDRTPROXY.SYS
- OS Platforms
  - Windows Server v10.0 14393 ServerStandard
- Product Types
  - Storage Controller
  - Hard Drive
  - Storage Spaces Adapter
- Test Status
- Machine Status ✓
  - WIN-UU627DCT3E6 ✓

5. From the pop up window, select the signing certificate created using Luna CSP and imported earlier on the local machine's personal certificate store and click **OK**.

6. Select a location to save the signed package.

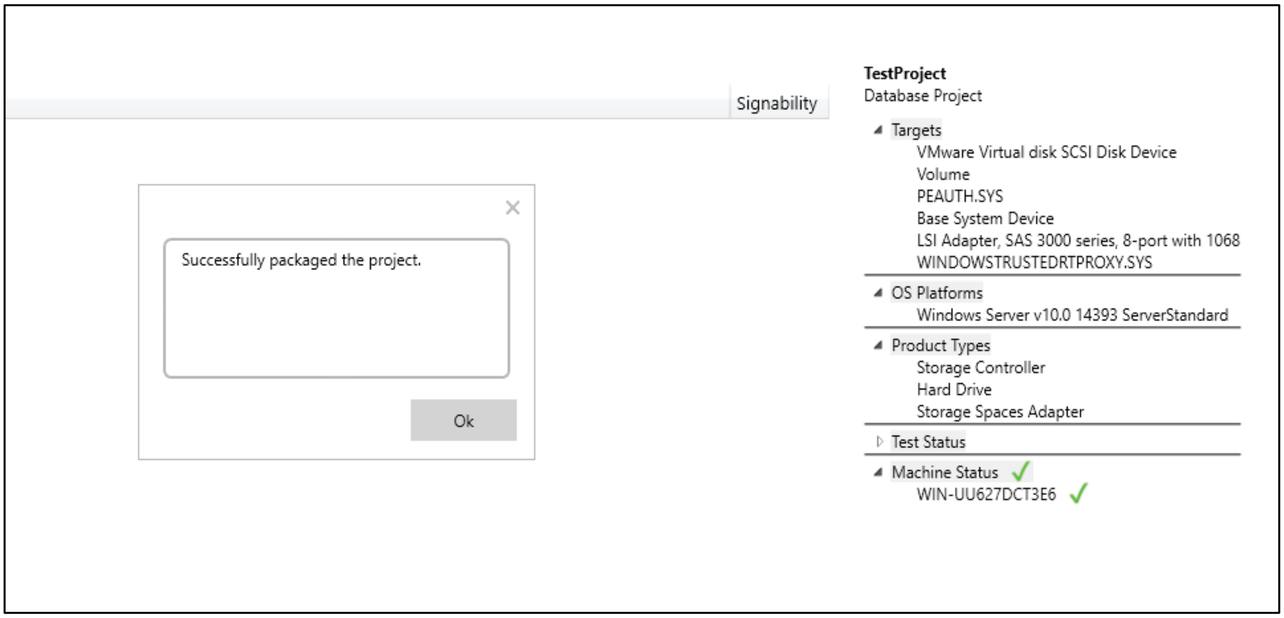
7. Click **Save** to start signing. Signing starts with a **Creating Package** window.



Creating Package

62/383 Saving Requirement: NetworkWake

8. At the end, **Successfully packaged the project** message displays and the package is signed.



Successfully packaged the project.

TestProject
Database Project

- Targets
  - VMware Virtual disk SCSI Disk Device
  - Volume
  - PEAUTH.SYS
  - Base System Device
  - LSI Adapter, SAS 3000 series, 8-port with 1068
  - WINDOWSTRUSTEDRTPROXY.SYS
- OS Platforms
  - Windows Server v10.0 14393 ServerStandard
- Product Types
  - Storage Controller
  - Hard Drive
  - Storage Spaces Adapter
- Test Status
- Machine Status ✓
  - WIN-UU627DCT3E6 ✓

It completes the Windows Hardware Lab Kit (HLK) integration with SafeNet Luna HSM and package signing with keys created on SafeNet Luna HSM.