Microsoft
Windows Hardware Lab Kit

Integration Guide

CryptoServer HSM

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH
	Krefelder Straße 220
	52070 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-05-20
Status	PUBLISHED
Document No.	IG-2026-0042

Table of Contents

1 Introduction

The Windows Hardware Lab Kit (Windows HLK) is a test framework used to test hardware devices for Windows 10. To qualify for the Windows Hardware Compatibility Program, your product must pass certain tests using the Windows HLK. CryptoServer HSM is used to secure the signing keys so that your signing keys never access by any unauthorized entity. Microsoft HLK uses RSA keys for signing the packages. Microsoft HLK is a 32 bit application so you have to use the 32 bit Utimaco CryptoServer CSP 32 bit.

2 Setting Up CryptoServer Device

To set up a CryptoServer device for Utimaco CSP open the **Control Panel** and select **Utimaco CSP Configuration** applet.

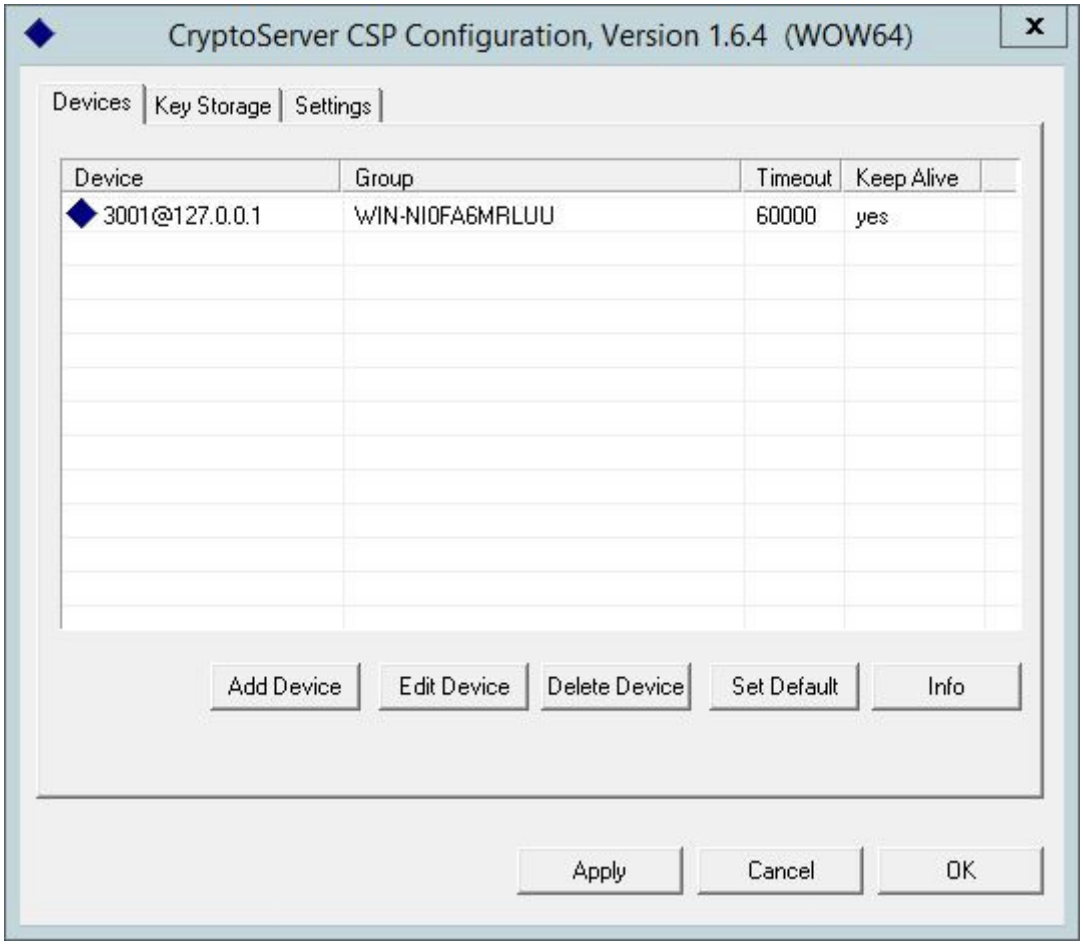

Figure 1 : CryptoServer CSP configuration

1. Go to the **Devices** tab in the **CryptoServer CSP Configuration** window.
2. Click the **Add Device** button.

This opens the **Device Settings** dialog box. In **Device Specifier**, enter the device specifier relevant for your CryptoServer device.

- If this is a CryptoServer PCI or PCIe card, this is *PCI:0*.
- If this is a CryptoServer LAN, enter an IP address (for example *192.168.5.17*).

• If you want to use the CryptoServer Simulator, enter *3001@127.0.0.1* as the device address.

3. In **Group** you now see the name of a computer. You may change this to your or keep it as default.

4. Click on the **OK** button. This opens the **User Logon** dialog box. This window displays all users available in the user database of the given CryptoServer device.

5. Select the **ADMIN** user in the user list.

6. Click on the **Logon** button. The authentication with Key dialog box opens.

7. Select the source of private user key, either **smartcard token** or **key file**.

8. Click the **OK** button.

9. Authenticate yourself with the intended authentication method. Once you have successfully authenticated yourself to the CryptoServer, you see a key lock symbol in the **User Logon** dialog box next to the entry for the **ADMIN** user.

10. Click **OK** to close the **User Logon dialog** box.

11. Click **OK** to close the **CryptoServer CSP Configuration** window and the **CSP Configuration** applet.

3 Create HLK Signing Certificate

In order to integrate the CryptoServer Hardware Security Module with Microsoft HLK, the Utimaco CSP Utimaco CryptoServer CSP must be used to generate the certificate signing request.

1. Create an `inf` file `hlksigning.inf` with the following attributes:

```
[Version]

Signature="$Windows NT$"

[NewRequest]

Subject= "C=DE, CN=UtimacoHLKSigning,OU=System Engineering HSM, O=Utimaco IS
GmbH,L=Aachen,S=NRW"

KeySpec=1 KeyLength=2048 Exportable=FALSE MachineKeySet=FALSE KeyContainer=HLK1

ProviderName="Utimaco CryptoServer CSP" ProviderType=1

KeyUsage=0x04
```

2. Generate a certificate request using the created `inf`. Make sure to use the 32 bit certreq utility. A success message is displayed after this command has been executed.

›_ Console

```
C:\>certreq -new hlksigning.inf hlksigning.req CertReq: Request Created
```

3. Take the generated certificate request to a Certificate Authority and get it signed to obtain a signed certificate.
4. Now we have to import this obtained certificate in the users personal certificate store. As this setup is 32 bit, ensure to use the 32 bit **Microsoft Certificate Manager Console**.

›_ Console

```
C:\>certmgr.msc
```

5. Right-click on **Personal > All Task > Import..** and follow the instructions to import the signed certificate. Verify the certificate is successfully imported.

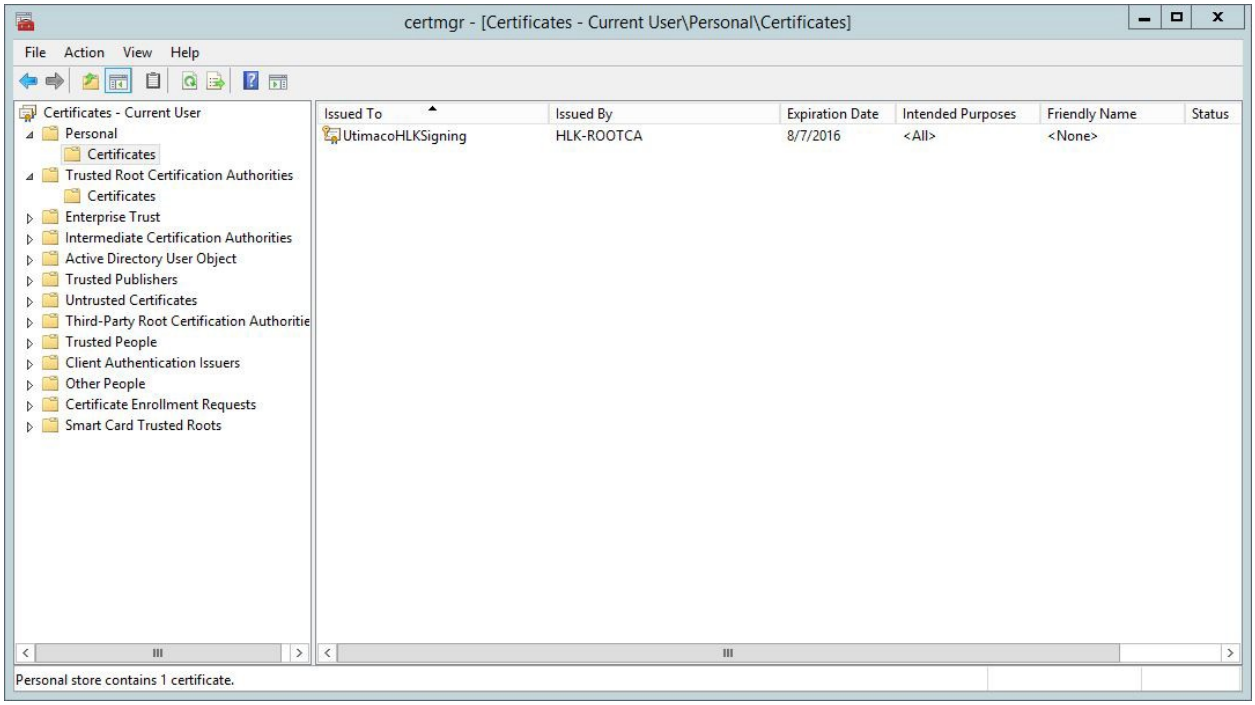

Figure 2 : Microsoft Certificate Manager Console

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

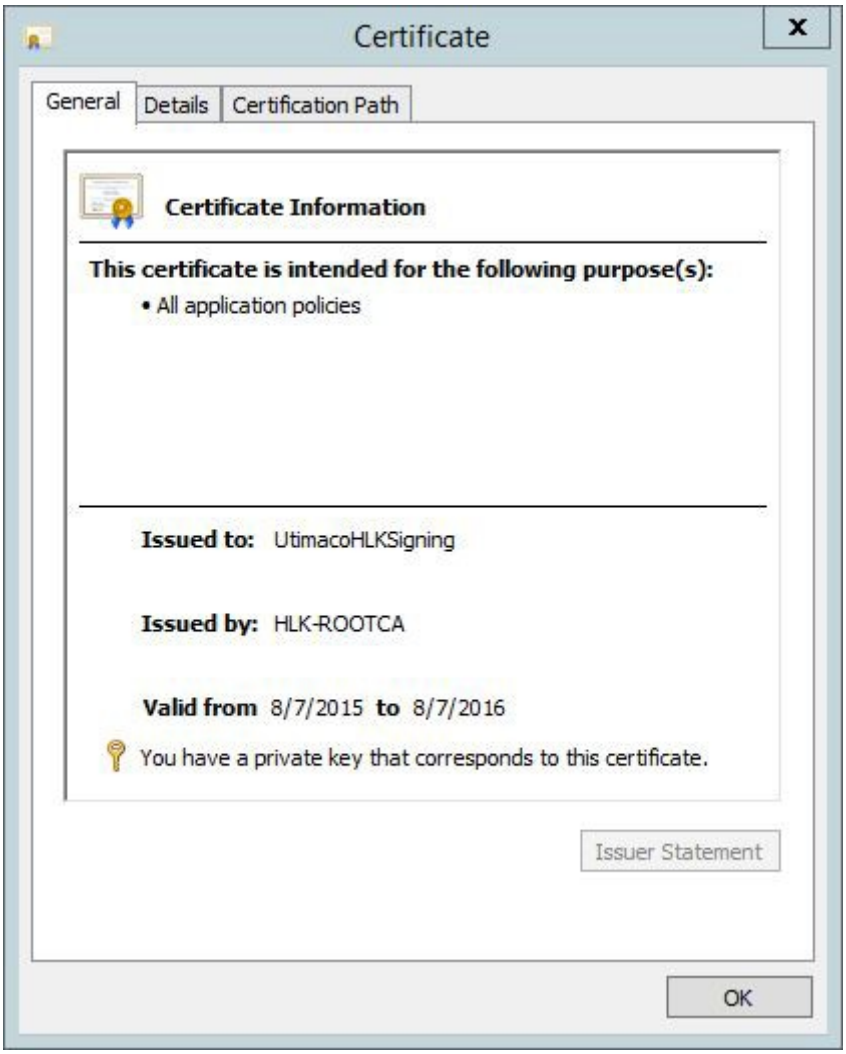

Figure 3 : Certificate Information

7. In case the private key is not mapped correctly, repair the certificate using the `certutil repairstore` utility.

- Open the certificate.
- Browse to the details tab.
- Select the serial number field.
- Copy the **serial number** or **thumb** print.
- Execute the `certutil -repairstore -user My SerialNumber or ThumbPrint` command to map the private key on the HSM with the certificate.

›_ Console

```
C:\>certutil -repairstore my <serial number>
```

8. 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.

4 Create And Sign Package

Now, as the certificate and the private key are ready for signing, open Windows Hardware Lab Kit Studio and import/open the HLK project that you want to sign. Browse through the various tabs to check if the project imported is the correct. After verification, go to the **Package** tab and click on **Create Package** to sign the package. You will be asked about how you want to sign the package.

1. Select **Use the certificate store** and click on the **OK** button.

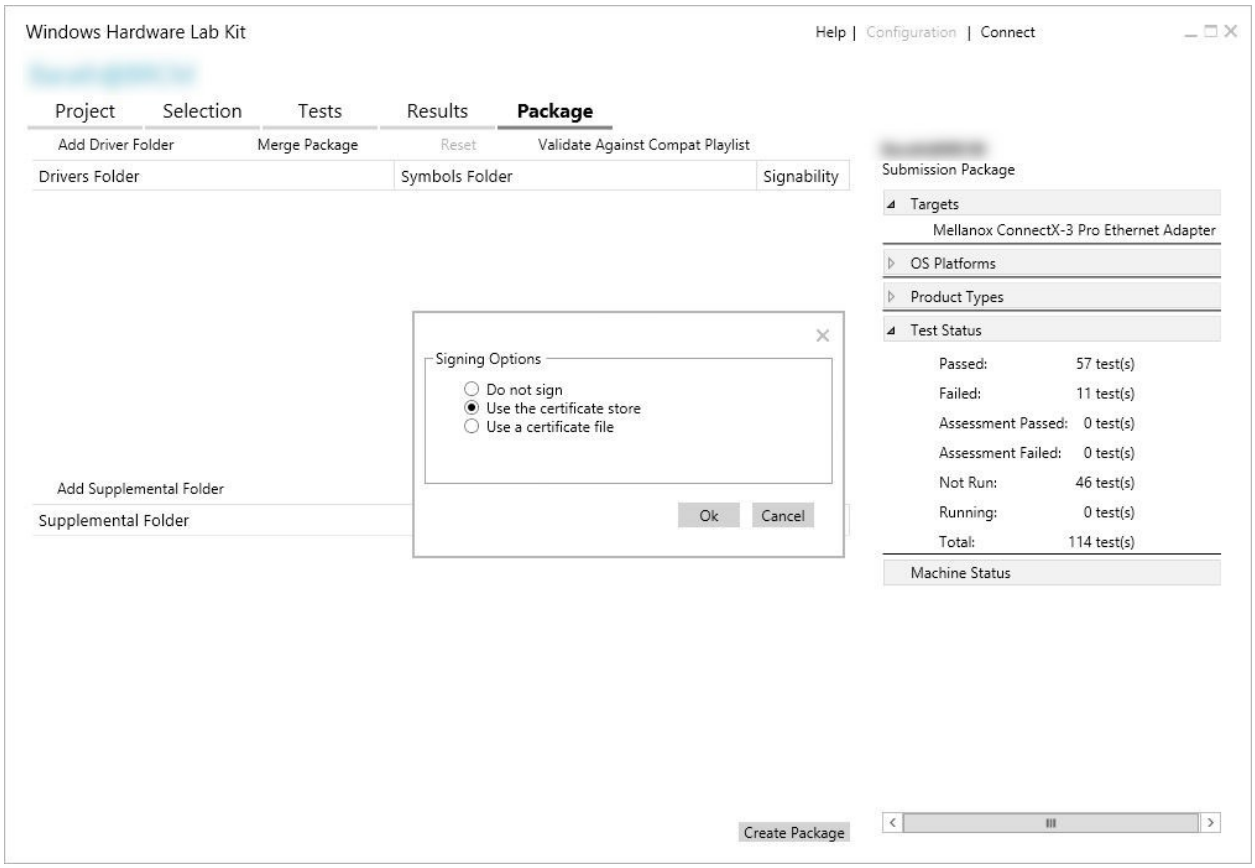

Figure 4 : Signing options

2. Next you will have to select the signing certificate. From the pop-up, select the certificate that was imported earlier on the local machines personal certificate store and click **OK**.

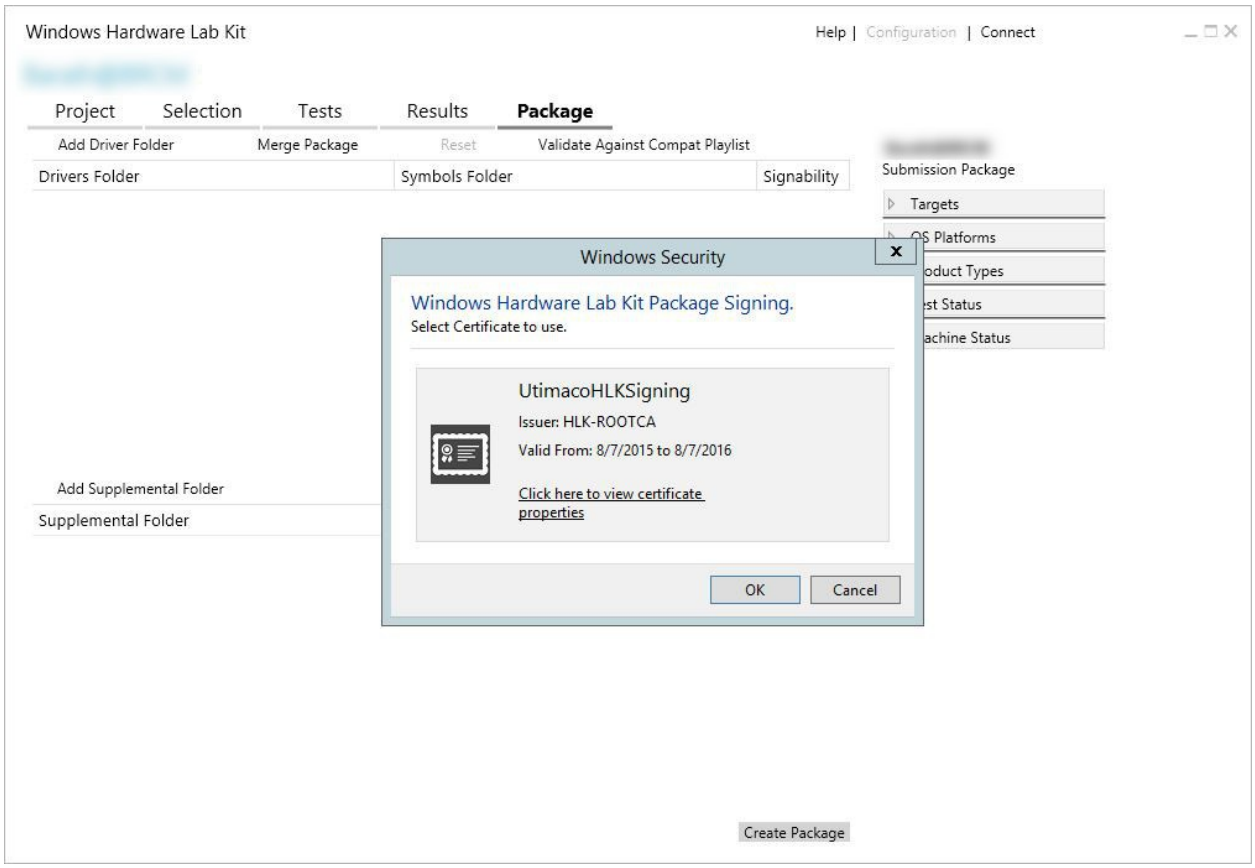

Figure 5 : Select the signing certificate

3. Select a location to save the signed package and click **Save**.
4. As soon as you click **Save**, signing will begin with a **Creating Package** window.

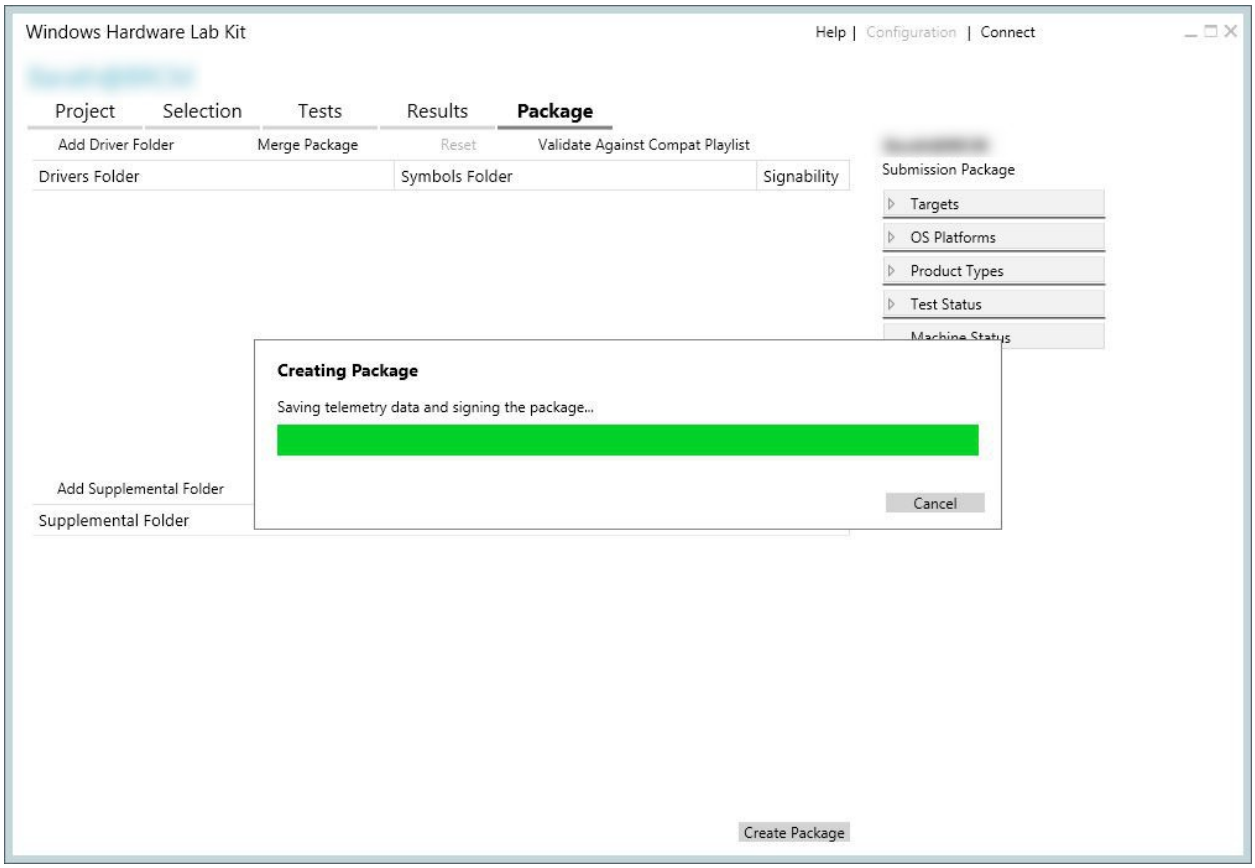

Figure 6 : Creating package

5. 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.

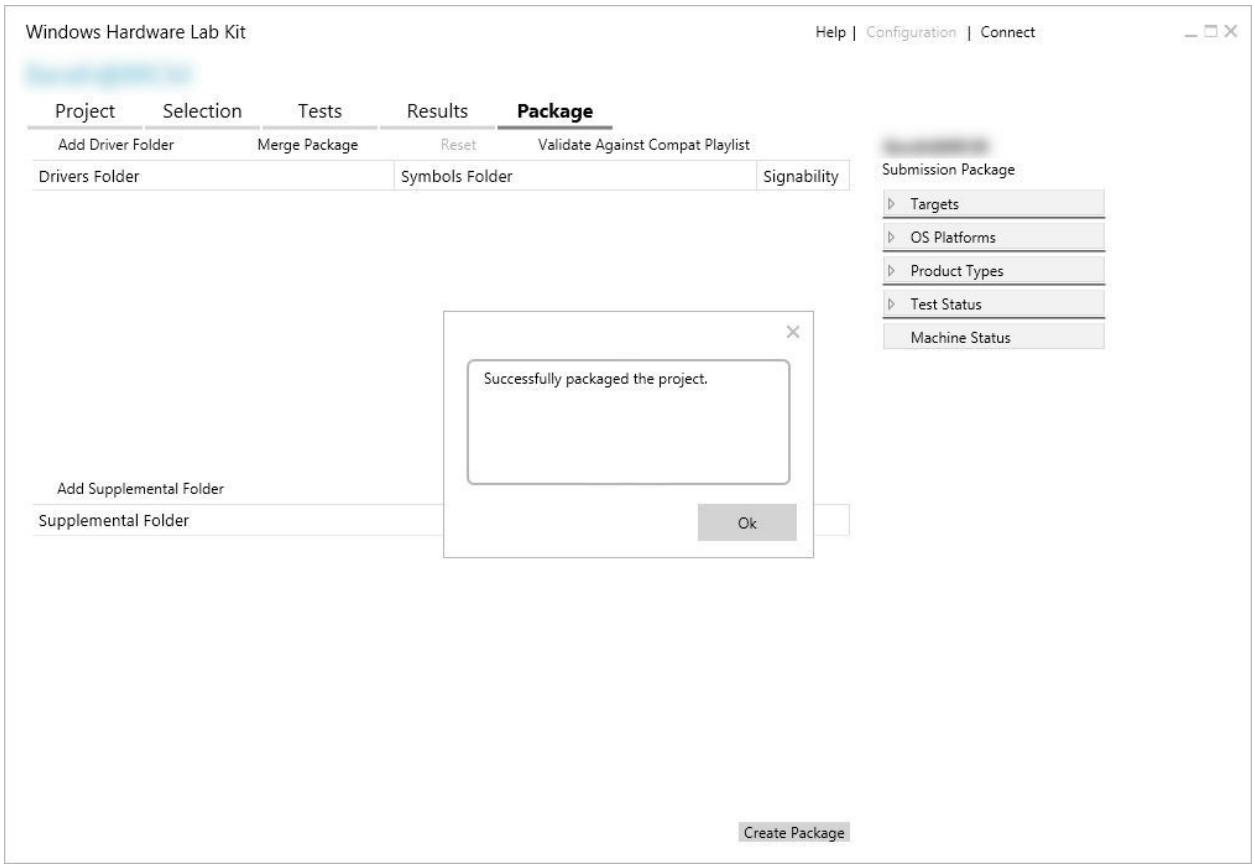

Figure 7 : Successfully packaged

5 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.