

\\tsifs01\Engineering\ThorDAQ\Software\DigiCertWindowsDriverSigning

|  |  |  |  |
| --- | --- | --- | --- |
| **WRITTEN BY**  **REVISED BY** | **Don Zimmerman** | **Software Engineer** | **TSI** |
| **REVIEWED BY** |  |  |  |
| **APPROVED BY** |  |  | **Management** |

# Contents

[Contents 2](#_Toc6204028)

[1. Purpose 3](#_Toc6204029)

[2. Scope and Applicability 3](#_Toc6204030)

[3. Definitions and Acronyms 3](#_Toc6204031)

[4. Document Conventions 3](#_Toc6204032)

[5. Solution to Failure to Load Win10 Driver with UEFI Safe Boot Active 3](#_Toc6204033)

[6. Process Overview 4](#_Toc6204034)

[7. Setup Digicert USB SafeNet 5110 USB Token 6](#_Toc6204035)

[8. Use MS Partner Center to test sign MS file with Thorlabs Token-based Certificate 12](#_Toc6204036)

[9. Build Driver, Create CAB Package, and Sign with Token 13](#_Toc6204037)

[10. DOWNLOAD/Distribute Microsoft Signed Driver 15](#_Toc6204038)

[11. References 17](#_Toc6204039)

[12. Revision History 18](#_Toc6204040)

[13. Signatures 18](#_Toc6204041)

[Appendix A. Azure Active Directory (Azure AD) Windows Hardware Developer Program 19](#_Toc6204042)

# Purpose

This document describes use of Digicert Extended Validation (EV) certificate signing of ThorDAQ’s Windows 10 kernel device driver for use with new Windows 10 security requirements including UEFI (BIOS) “Safe Mode” configuration. The same USB “token” may be used for Windows 7 signing, provided Digicert changes or affirms SHA1 (Win7) or SHA2 (Win10) certificate digest as required.

# Scope and Applicability

This document applies to all Windows 10 based computers expected to operate the ThorDAQ PCIe adapter.

# Definitions and Acronyms

# Document Conventions

All mandatory product requirements in this document are introduced by the word “shall.”

All desirable requirements, or goals, are introduced by the word “should.”

All optional requirements are introduced by the word “may.”

# Solution to Failure to Load Win10 Driver with UEFI Safe Boot Active

In Windows 10 (release 1607 and beyond), kernel device drivers must be digitally signed by Microsoft through a “Partner Center” web application portal to prevent the “Windows cannot verify the digital signature…” kernel driver installation error. Access to this web app is through Azure AD login, and the Thorlabs Azure AD Administrator (Chris Bittner as of this writing) must grant access. As of this writing, there are four companies which Microsoft has granted cross certificates to for signing kernel drivers (including Digicert and Symantec); this document provides an extensible example using Digicert. The cross signing certificate, and the Thorlabs issued certificate must be SHA2 (the Extended Validation “Root” Certificate Authority is still SHA1), and the signature must be SHA256 (i.e. flag /fd in signtool.exe). This document details the entire process of USB-token key creation, synchronizing that key with “Partner Center” certificates settings, and the “driver package” signing procedure (i.e. uploading driver .CAB package for MS signing). The end goal is a Thorlabs driver package where MS replaces the Thorlabs certificate with its own certificate, which eliminates the driver loading error with Safe Boot active. This is called “Attestation Signing”, because we do not complete the HLK (Hardware Lab Kit) suite of testing normally required of Windows kernel mode drivers. Attestation is possible because ThorDAQ is not an O/S kernel boot device.

# Process Overview

Use MS Partner Center to test sign MS file (certifies Thumbprint)

Build Driver and /or make Package Edits; Create .CAB driver package signed with Thorlabs cert.

Install correct Win10 kernel drivers for DigiKey USB token operation

Use MS Partner to UPLOAD driver package

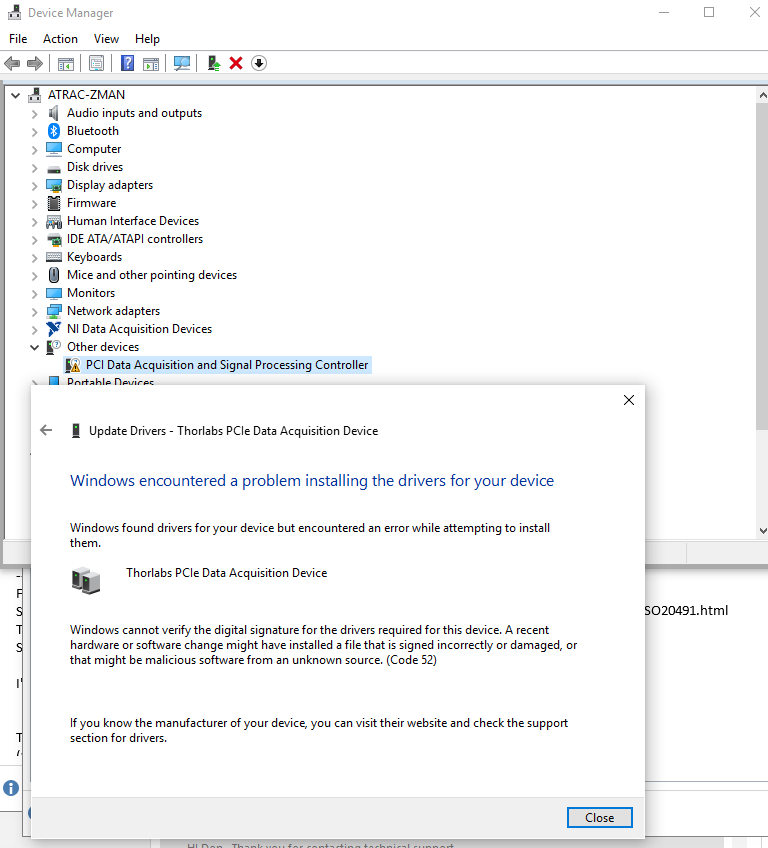
Setup Digicert USB SafeNet TOKEN-based Thorlabs SHA2 certificate and record Thumbprint

NO

Partner Center accepts & resigns Driver package?

YES

DOWNLOAD/Distribute Microsoft Signed Driver



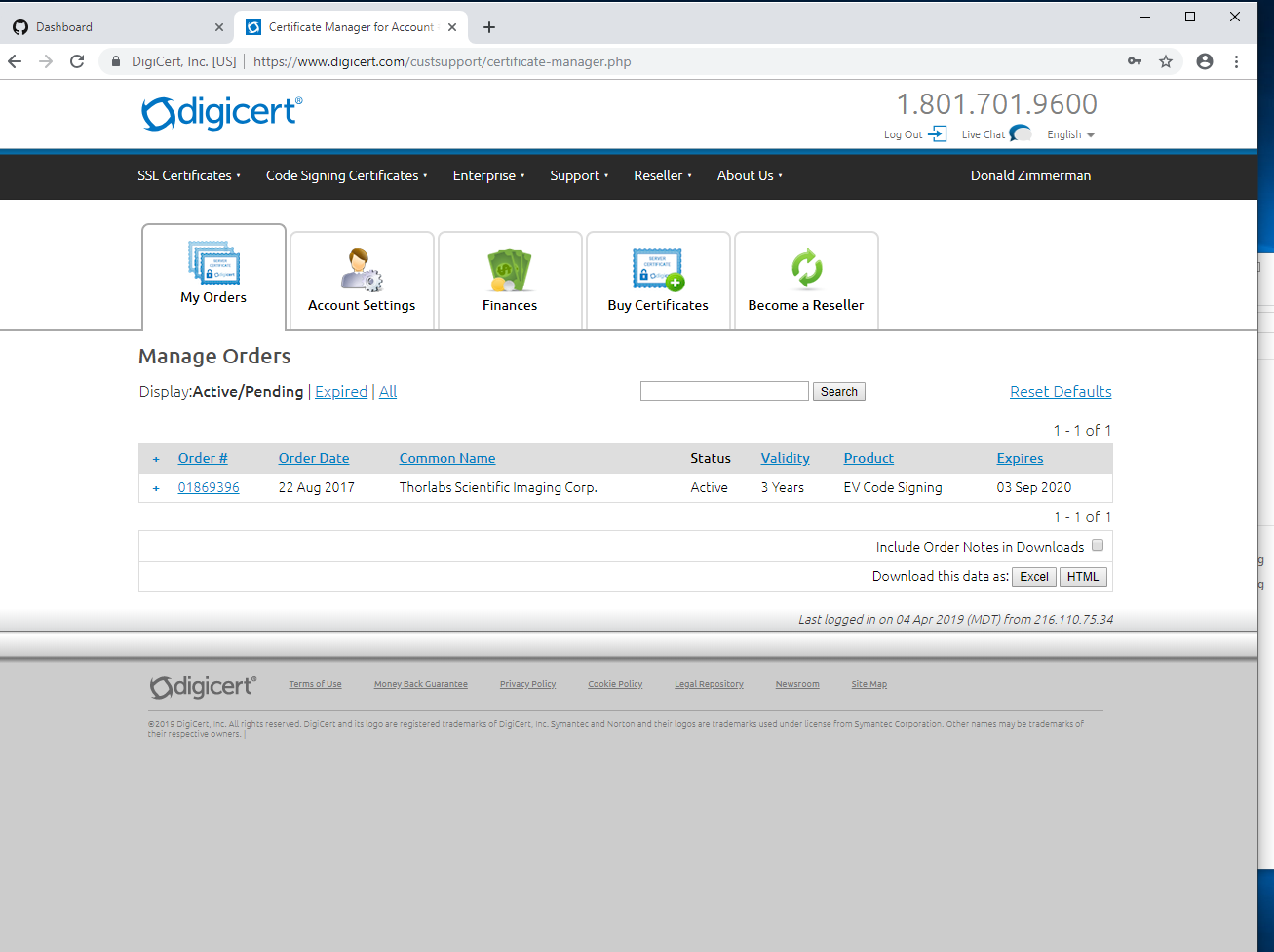
# Setup Digicert USB SafeNet 5110 USB Token

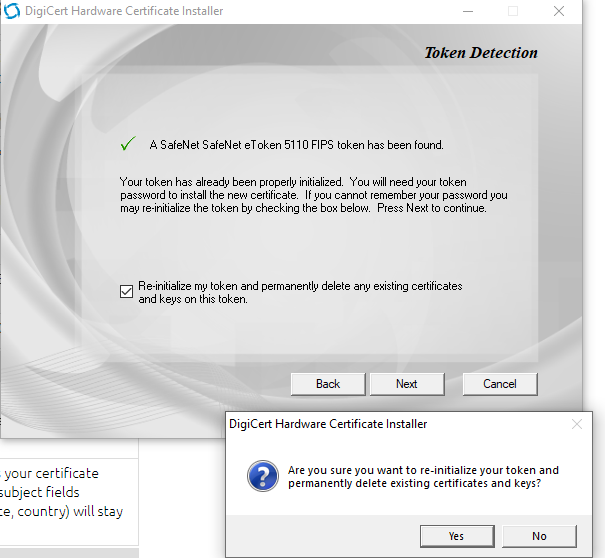


The Sentinel “SafeNet 5110” USB Token use by DigiCert

The Digicert certificate is managed by website login, with Thorlabs manager (i.e.. Martin Parker) having authority to add users to the account. In the screen shot below, a user has been successful added to the account. This permits initialization of the USB “SafeNet” key (or “token”).

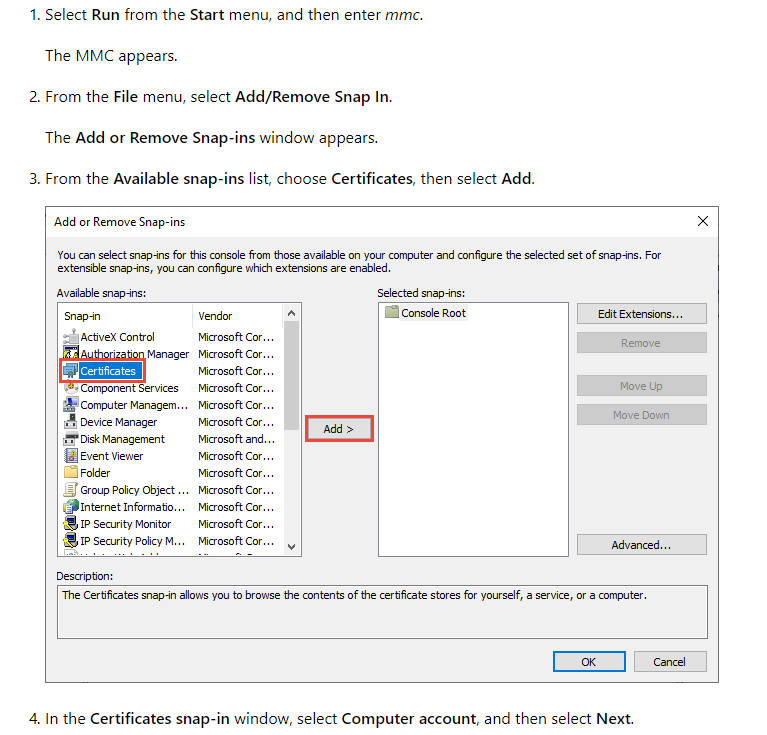
1. Plug the token into a USB port; if the correct device drivers have not been loaded, an error message will appear, identifying the Sentinel token but saying “device drivers not installed”. To fix this problem, see document <https://knowledge.digicert.com/solution/SO20491.html>, and run the executable with correct kernel device driver, e.g. DIGICERT\_SafeNetAuthenticationClient-x32-x64-10.4; when device drivers are correctly loaded, “Device Manager” settings for Smart card readers should appear as in screen shot below. See Appendix B for details.
2. To re-initialize (i.e. validate) the token, perform the “Reissue – Re-Key” process, and “Create New Initialization Code”. [Newer version of DigiCert.com instructions may say “Install Certificate” and give you ONLY one chance to set the password. Password reset not allowed unless certificate is “Reissued”.]
3. Follow instructions to download the [DigiCert Hardware Certificate Installer](https://www.digicert.com/StaticFiles/DigiCertHardwareCertificateInstaller.zip) and enter initialization code.
4. NOTE: Digicert makes continuous changes to process – e.g. as of July 2020, there is only ONE opportunity to set the password after the certificate is “issued” (or “re-issued”). If password cannot be discovered, you must re-issue. Re-issue requires approval of the original Thorlabs purchaser/admin of the certificate, typically by e-mail directly from Digicert. Contact Digicert technical support for details regarding consequence of “re-issue” on the certificate – e.g., does a re-issue invalidate the previously signed code.
5. After re-issue, this new token certificate must be used for future signing, and procedurally recorded in the web portal “Partner Center”.
6. Token Name: *ThorDAQ Windows Driver*, Passwd: (*see Thordaq engineer who inititalized*)
7. No Administrator Password
8. On success, you will see screenshot below, “…successfully installed and is ready for use”.



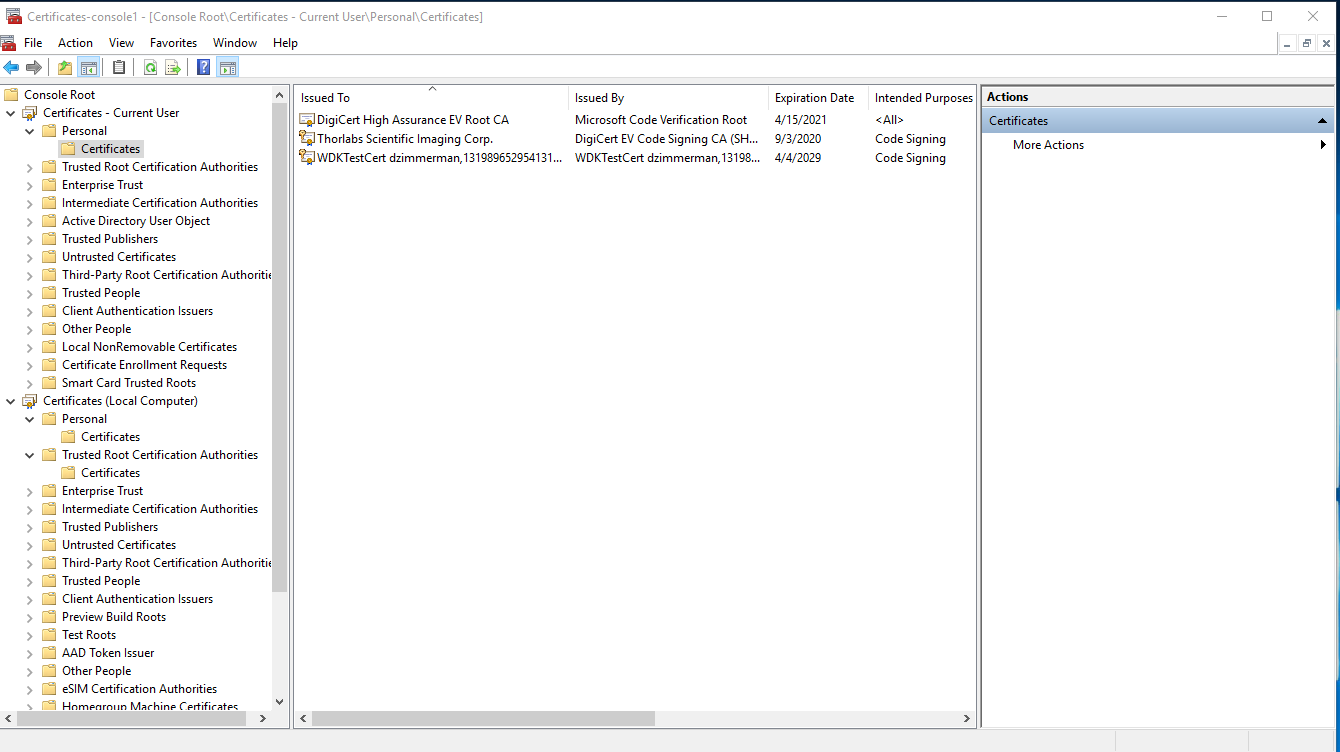


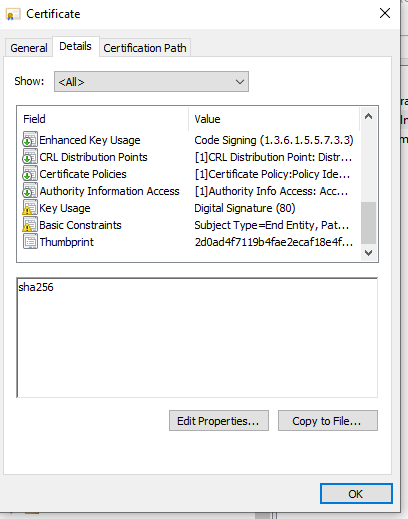


1. VERIFY that this new certificate is visible in the “Personal” certificate store, by starting the MMC for the “Local computer”:



1. Now verify that the Thorlabs token-based certificate you just re-keyed appears under *Certificate –> Current User -> Personal -> Certificates*, .e.g.; click on the Thorlabs Cert, then Details -> Signature hash algorithm, and verify it is “sha256”, then scroll down *and note the “Thumbprint”.* This Thumbprint is how you confirm, in a later step, that this certificate is recognized by the Partner Center when uploading driver packages. Also note that if you physically remove the USB token and “refresh” the Certificate list, the Thorlabs certificate disappears.

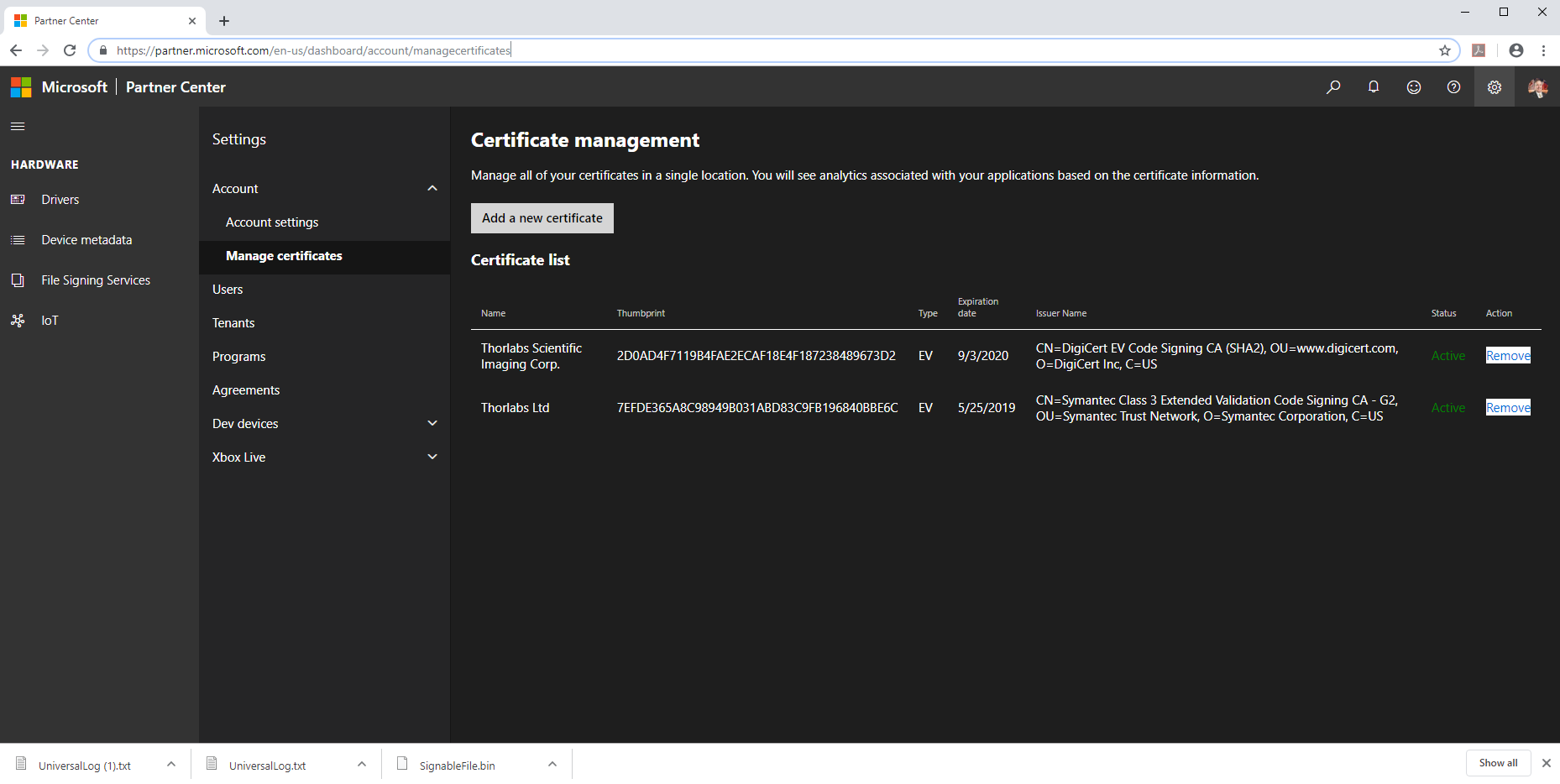




NOTE! After you re-key the token, you MUST update the Azure-AD based Partner center account to reflect the Thumprint (SHA hash) of the new certificate in order to upload kernel driver packages to Microsoft.

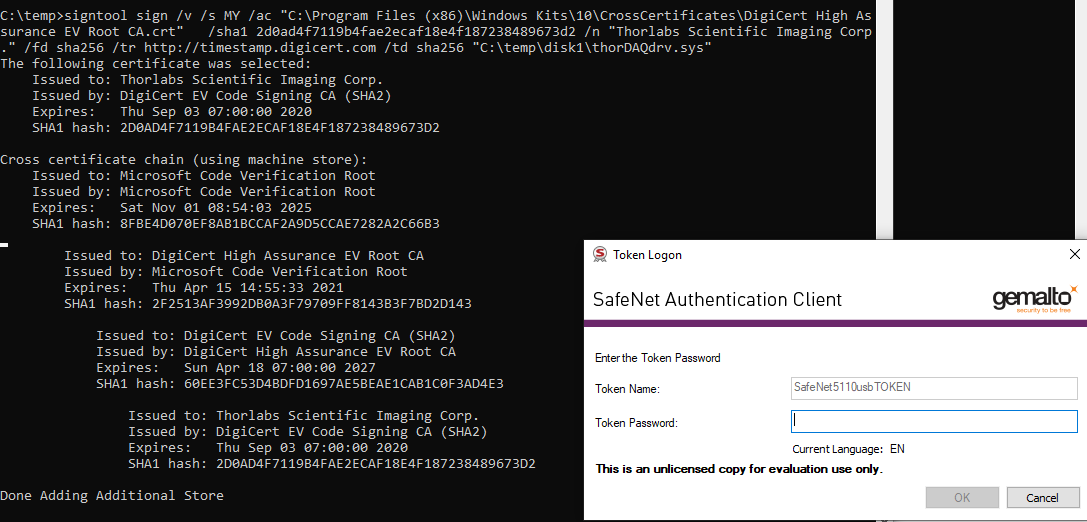
# Use MS Partner Center to test sign MS file with Thorlabs Token-based Certificate

1. Login to <https://partner.microsoft.com/en-us/dashboard>. (If you do not have a login, or lack permissions to add certificates, and/or have no idea who the Azure Active Director admin is for this login, see Appendex A.) Under Settings -> Account -> Manage certificates -> Add a new certificate, you will be able to download a MS file (e.g. “SignableFile.bin”). Download this file.
2. From Digicert.com, download the .crt file corresponding to the USB Token key creation above; as of this writing, that .crt file is here: <https://www.digicert.com/code-signing/driver-signing-in-windows-using-signtool.htm#using_kernel_mode> ([Click here to download the DigiCert Code Signing Cross-Certificate](http://download.microsoft.com/download/2/4/E/24E730E6-C012-448F-92B6-78744D3B77E1/DigiCert%20High%20Assurance%20EV%20Root%20CA.zip).)
3. Copy the downloaded file to the following filespec, for use by signtool: *C:\Program Files (x86)\Windows Kits\10\CrossCertificates\DigiCert High Assurance EV Root CA.crt*
4. Using WDK tool “signtool.exe”, sign the file with a command like: *signtool sign /v /s MY /ac "C:\Program Files (x86)\Windows Kits\10\CrossCertificates\DigiCert High Assurance EV Root CA.crt" /n "Thorlabs Scientific Imaging Corp." /fd sha256 /tr http://timestamp.digicert.com /td sha256 "C:\temp\SignableFile.bin"*
5. Upload this signed file back to partner center; under “Certificate list”, verify that the “Thumbprint” matches what you created above.

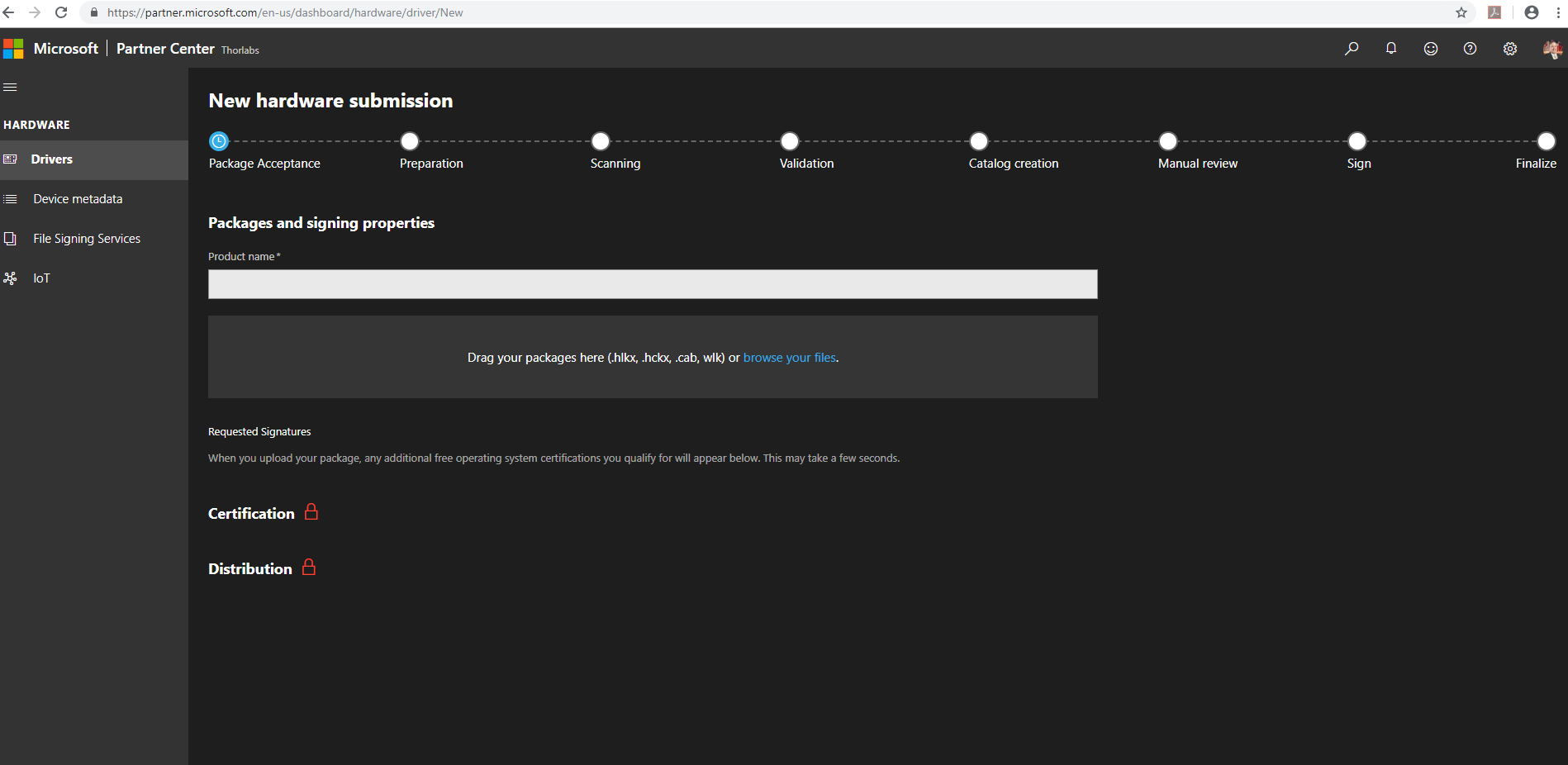


# Build Driver, Create CAB Package, and Sign with Token

1. Presuming the Visual Studio and SDK/WDK has been setup according to *2019VS\_TFS\_DevelopmentEnvironmentAddInSetup* or similar document, open a VS Command Prompt, e.g. *x86\_x64 Cross Tools Command Prompt for VS 2019*. Make sure the Digicert USB Token is plugged in
2. Execute the following script and confirm correct output; you should be prompted (twice) for the Token key password:

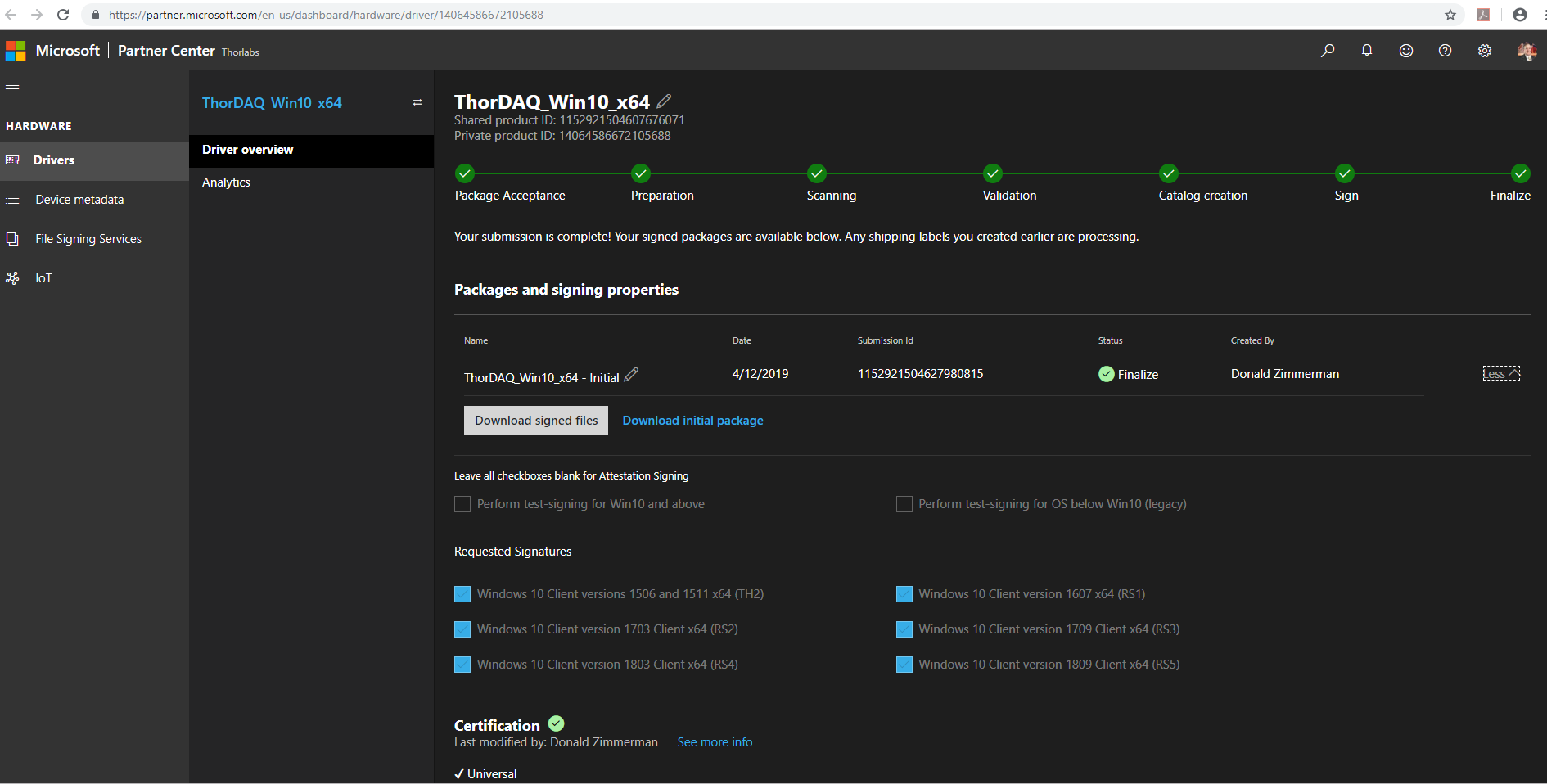


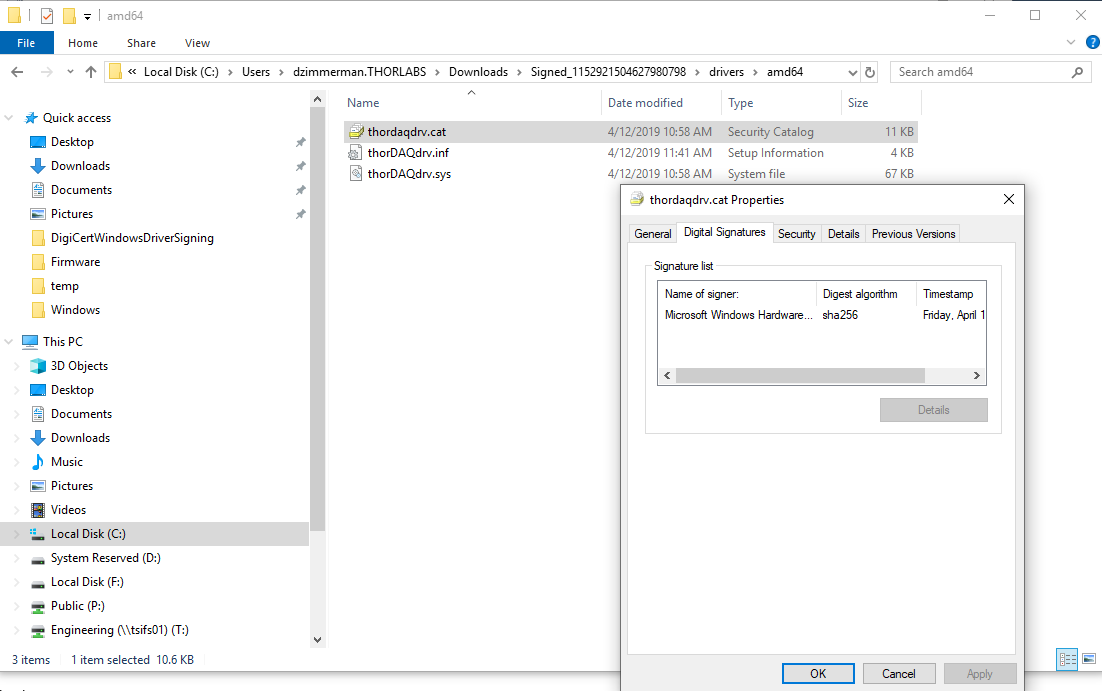
1. In this example, the “package file” to upload to Partner Center is **C:\temp\disk1\ThorDAQdriver.cab**: verify that the file has the proper signature “Thumbprint”, consistent with Partner Center certificates above. Failure to match thumbprints will result in “Preparation” stage FAILURE.
2. In Partner Center, make a “New Hardware Submission” with appropriate name, and “Browse” to upload the .CAB file, then SUBMIT; check all the Win10 x64 versions (except ARM architecture); the 7 step completion takes about 15 - 25 minutes if successful.



# DOWNLOAD/Distribute Microsoft Signed Driver

1. If successful, the Microsoft signed driver may be downloaded (“Download Signed Files”) from Partner Center as .ZIP, appearing as below:
2. Confirm that Microsoft has indeed signed these drivers by examining the “Digital Signatures” under File Explorer, as below; note that the .CAB submitted driver was signed by the Thorlabs certificate, but the download driver is signed by a Microsoft certificate.
3. Using the three file set, you may “Update” the Thorlabs driver from “Device Manager” with “Secure Boot” enabled.





# References

|  |  |
| --- | --- |
| **Document Number** | **Document Title** |
|  |  |
|  |  |
|  |  |
|  |  |

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Effective Date** | **Description of Change** | **Revision Originator** |
| 1.0 | 4-Apr-19 | Initial Draft | Don Zimmerman |
| 1.1 | 15-Apr-19 | Minor formatting and typo corrections | DZimmerman |
| 1.2 | 23-Jul-20 | Add Appendix and detail on kernel driver install for USB key | DZimmerman |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

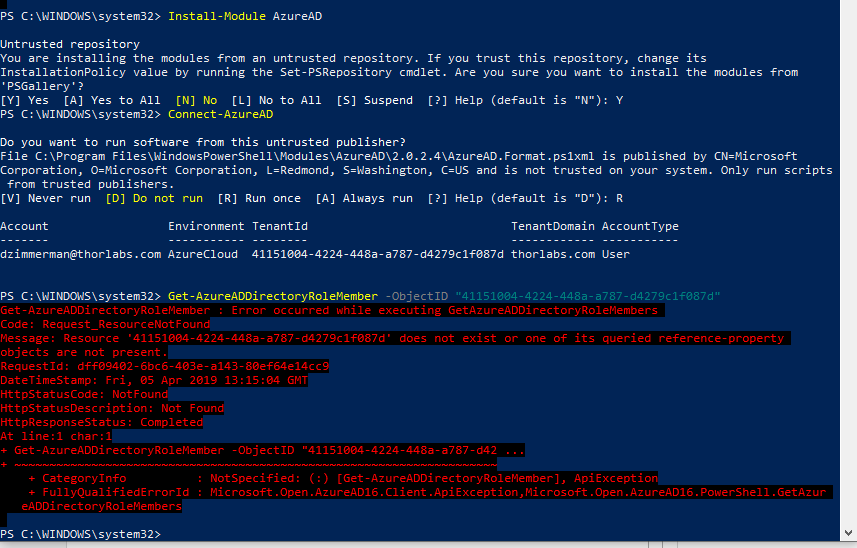
# Signatures

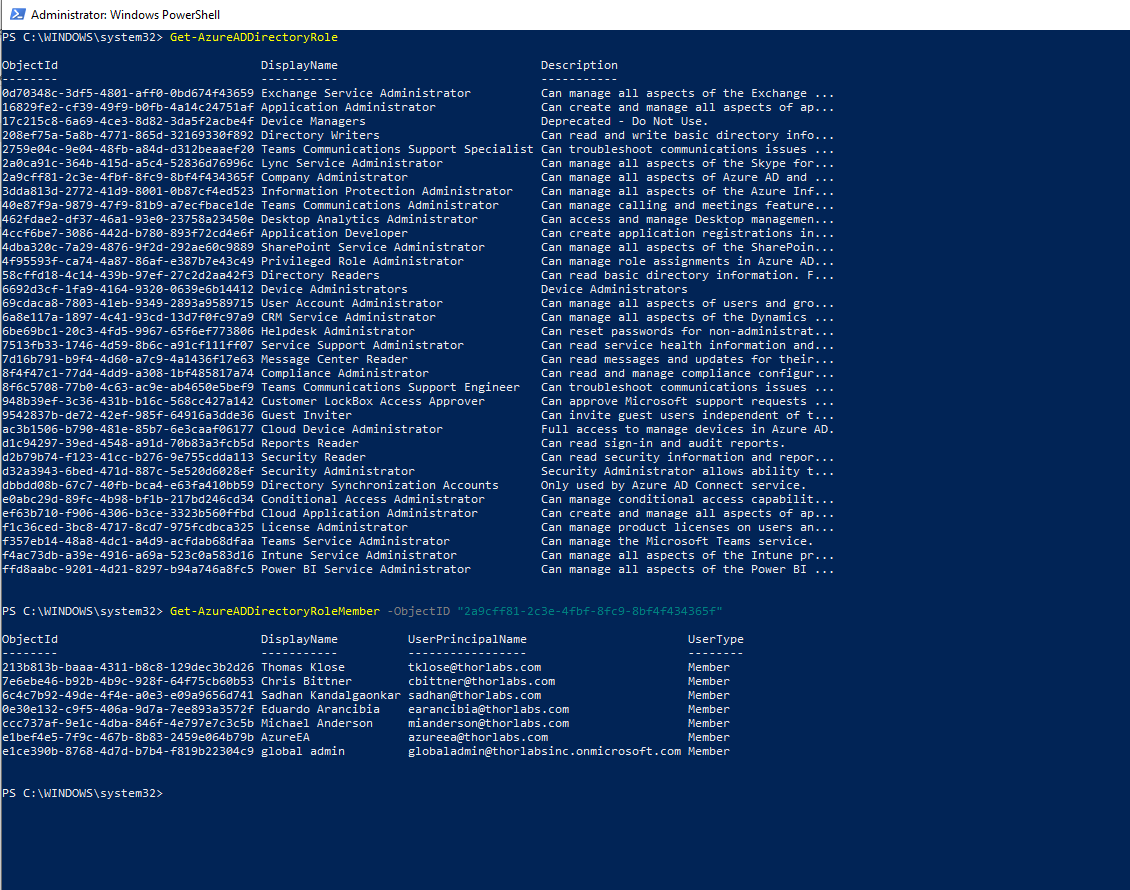
|  |  |
| --- | --- |
| **Name and Title** | **Date** |
|  |  |
|  |  |
|  |  |
|  |  |

# Appendix A. Azure Active Directory (Azure AD) Windows Hardware Developer Program

For Windows 10, kernel drivers must be submitted to and cross signed by Microsoft through the AzureAD Hardware Developer Partner portal, which requires access to the *Windows Hardware Developer Program* account. To discover who at Thorlabs can grant access, use an *administrator* privilege Power Shell to install AzureAD module (below), then find the Thorlabs company administrator e-mails, as illustrated below.

As of April 2019, the Thorlabs AzureAD admin was Chris Bittner (cbittner); you must have MS Partner Center login access to proceed





# Appendix B. Digicert USB Key Windows 10 Device Driver Install

A typical insertion of the Digicert USB Key (a.k.a. Token) on Windows 10 without the required device drivers is illustrated in *Figure 1: USB Key in Device Manager Prior to kernel driver install*, and after correct device drivers in *Figure 2: Digicert USB Key in Device Manager with correct drivers*.

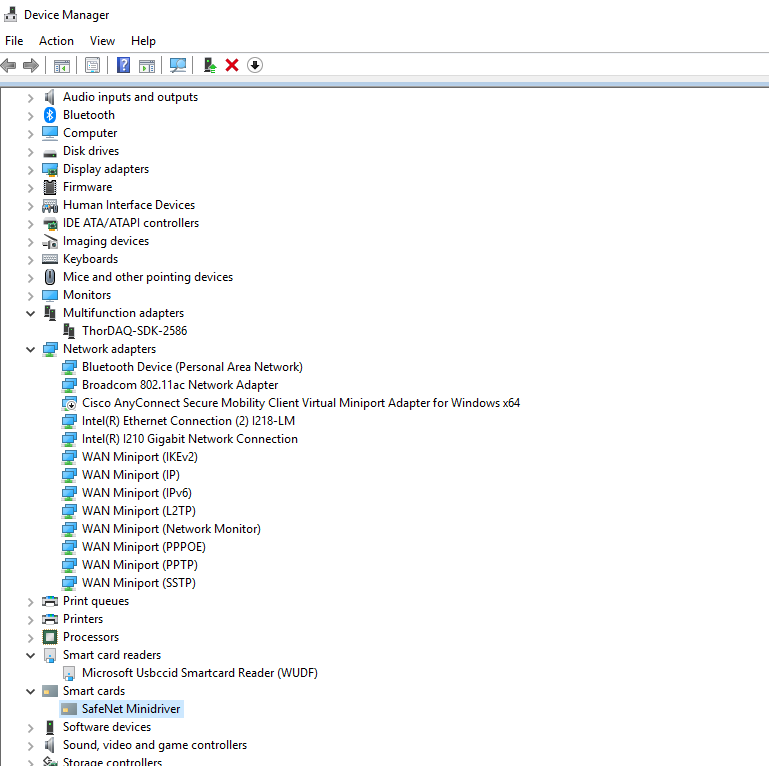


Figure : USB Key in Device Manager Prior to kernel driver install

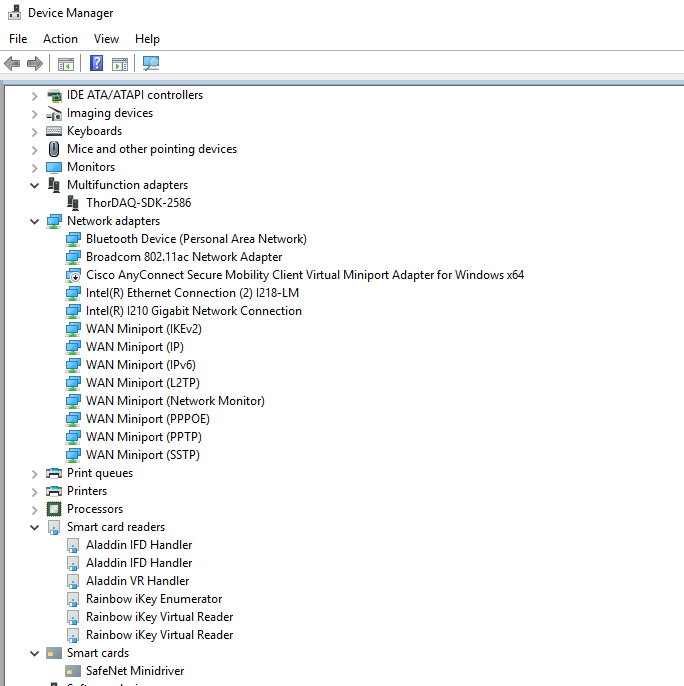


Figure : Digicert USB Key in Device Manager with correct drivers