Microsoft Authenticode

Integration Guide

u.trust GP HSM

SecurityServer 6.4.0

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	2026-06-11
Status	PUBLISHED
Document No.	IG-2026-0058

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle. All Utimaco SecurityServer product documentation is available from Utimaco's website at: https://utimaco.com/.

1.1 About This Guide

This guide describes how to enable u.trust GP HSM integration with Microsoft Authenticode.

1.1.1 Target Audience for This Guide

This guide is intended for Microsoft Authenticode and GP HSM administrators.

1.1.2 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

Table 1: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message indicates the expected result after the successful execution of an instruction.

1.1.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
CA	Certificate Authority
CLI	Command Line Interface
CNG	Cryptography API Next Generation
CSAR	Cloud Service Architecture
CSP	Cryptographic Service Provider
CXI	Cryptographic eXtended Services Interface
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface

Abbreviation	Meaning
HMAC	Hash-based message authentication code
HSM	Hardware Security Module
LAN	Local Area Network
MBK	Master Backup Key
PKI	Public Key Infrastructure
PS	PowerShell
RSA	Rivest-Shamir-Adleman
SDK	Software Development Kit
TSS	Time Stamp Server
URL	Uniform Resource Locator
ACS	Azure Code Signing
ADCS	Active Directory Certificate Services
CSR	Certificate Signing Request
KSP	Key Storage Provider
PEM	Privacy Enhanced Mail

Abbreviation	Meaning
DER	Distinguished Encoding Rules
EKU	Extended Key Usage
CN	Common Name
INF	Setup Information File
PE	Portable Executable

Table 2: List of abbreviations

2 Overview

2.1 Microsoft Authenticode

Microsoft Authenticode is a code-signing technology that identifies the publisher of Authenticode-signed software. It also verifies that the software has not been tampered with since it was signed and published. Authenticode uses cryptographic techniques to verify publisher identity and code integrity.

Authenticode relies on proven cryptographic techniques from Microsoft and the use of one or more private keys to sign and timestamp published software. From a security point of view, it is important to maintain the confidentiality of these code-signing keys. The u.trust GP Hardware Security Module (HSM) integrates with Microsoft Authenticode to provide a trusted system for protecting the organizational credentials of a software publisher. The u.trust GP HSM secures the code-signing keys on a certified industry standard FIPS 140-2.

This integration guide covers all the necessary information to install, configure and integrate Microsoft Authenticode with Utimaco u.trust GP HSM.

The benefits of using an HSM with Microsoft Authenticode include:

- The private key will be securely stored on the HSM.
- The hardware is FIPS 140-2 level 3 validated.
- Trusted timestamp (TSS) for Authenticode.

Refer to the Microsoft documentation for more information about installing Microsoft Authenticode.

2.2 Utimaco u.trust GP HSM

u.trust GP HSM is a hardware security module developed by Utimaco IS GmbH. u.trust GP HSM is a physically protected, specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage, as well as store, cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Integration Requirements and Prerequisites

Ensure that the system environment you will be using meets the following hardware and software requirements.

This guide assumes that the user has already installed and configured the required software.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with Microsoft Authenticode.

Operating System	Microsoft .NET Framework	Windows SDK	Utimaco Security Server Version	Utimaco HSM
Windows Server 2022 Windows 11	6/8	10.0.22621	SecurityServer 6.4.0	GP HSM CSeSeries/Se-Series

Table 3: List of tested versions

3.2 Software Requirements

Software	Software Requirements
HSM Interfaces	u.trust HSM CSP/CNG Provider
Microsoft .NET Framework	6/8
Windows SDK	10.0.22621

Table 4: List of software requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM CSe-Series/Se-Series LAN with firmware SecurityServer 6.4.0 or higher
Utimaco PCI-e HSM	u.trust GP HSM CSe-Series/Se-Series PCI-e with firmware SecurityServer 6.4.0 or higher

Table 5: List of hardware requirements

Set up an account on the Utimaco support portal and request download access at the following URL: https://support.hsm.utimaco.com/.

3.4 Prerequisites

Before you begin, please ensure:

- You installed/set up the operating system listed in Tested Versions.
- You installed/set up the SecurityServer version listed in Tested Versions.
- You replaced the GP HSM Default Admin with a new admin user.
- You created and stored the MBK onto each HSM. Refer to the u.trust GP HSM documentation to set up the MBK.
- You set up and configured the u.trust GP HSM. Refer to the u.trust GP HSM documentation to set up the HSM.
- You installed and configured Microsoft SDK as listed in Tested Versions.

4 Configuring the CSP-CNG Provider

4.1 Introduction and Prerequisites

A CSP (Cryptographic Service Provider) is a general-purpose cryptography standard, developed by Microsoft. On one side, it defines a cryptographic interface to be used by applications (CryptoAPI). On the other side, it defines an interface to be used by manufacturers to integrate their cryptographic hardware.

A CNG (Cryptography API Next Generation) is a second-generation cryptographic interface, developed by Microsoft. It offers updated cryptographic algorithms and is intended as a long-term replacement for CSP.

When installing the CryptoServer setup, make sure to select the CPS/CNG - Cryptographic Service Provider (Microsoft) interface. A Cryptographic User should be created, and an MBK should be generated.

Generating the MBK is necessary for the HSM to become operational. Without the MBK, one cannot run any cryptographic operations.

4.2 Creating HSM Users

Start the CryptoServer Administration Tool and log in a user with the permission level of at least 02000000.

4.2.1 Creating a Key Manager User

If the Key Manager and Crypto User roles are separated, a Key Manager User might need to be created.

More users with the permission level **00000010** might be needed (**Group 1**) to enforce "m of n" security policy for the key management, and smart card authentication might need to be used.

For this guide, only one Key Manager User will be created.

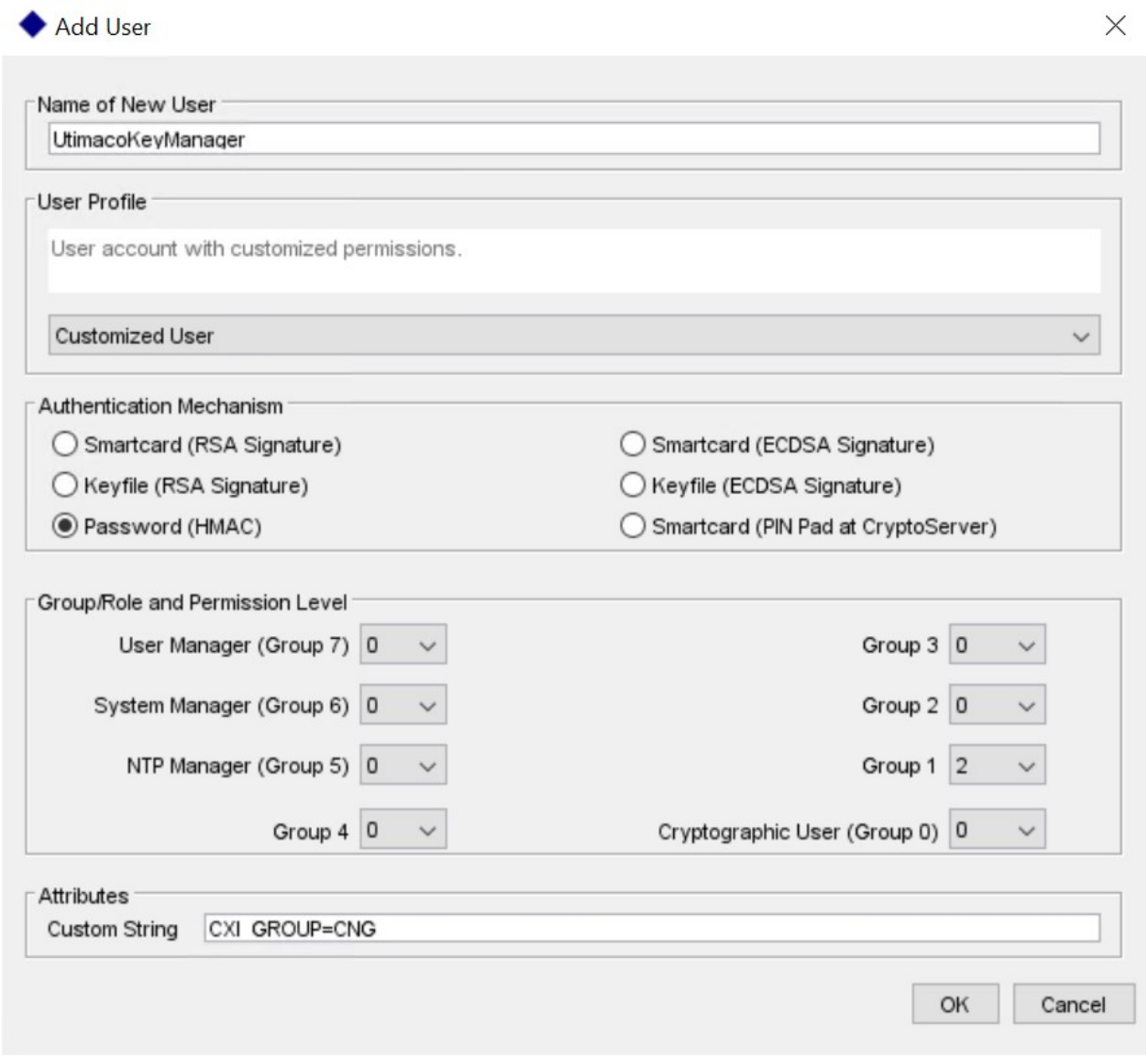

Figure 1 : Creating Key Manager User

4.2.2 Creating a Crypto User

Crypto Users with permission level of **00000222** will have to be created. Use encrypted passwords. For this guide, a user with permission level of 00000222, **CXI Group "CNG"** and **HMAC** password will be created.

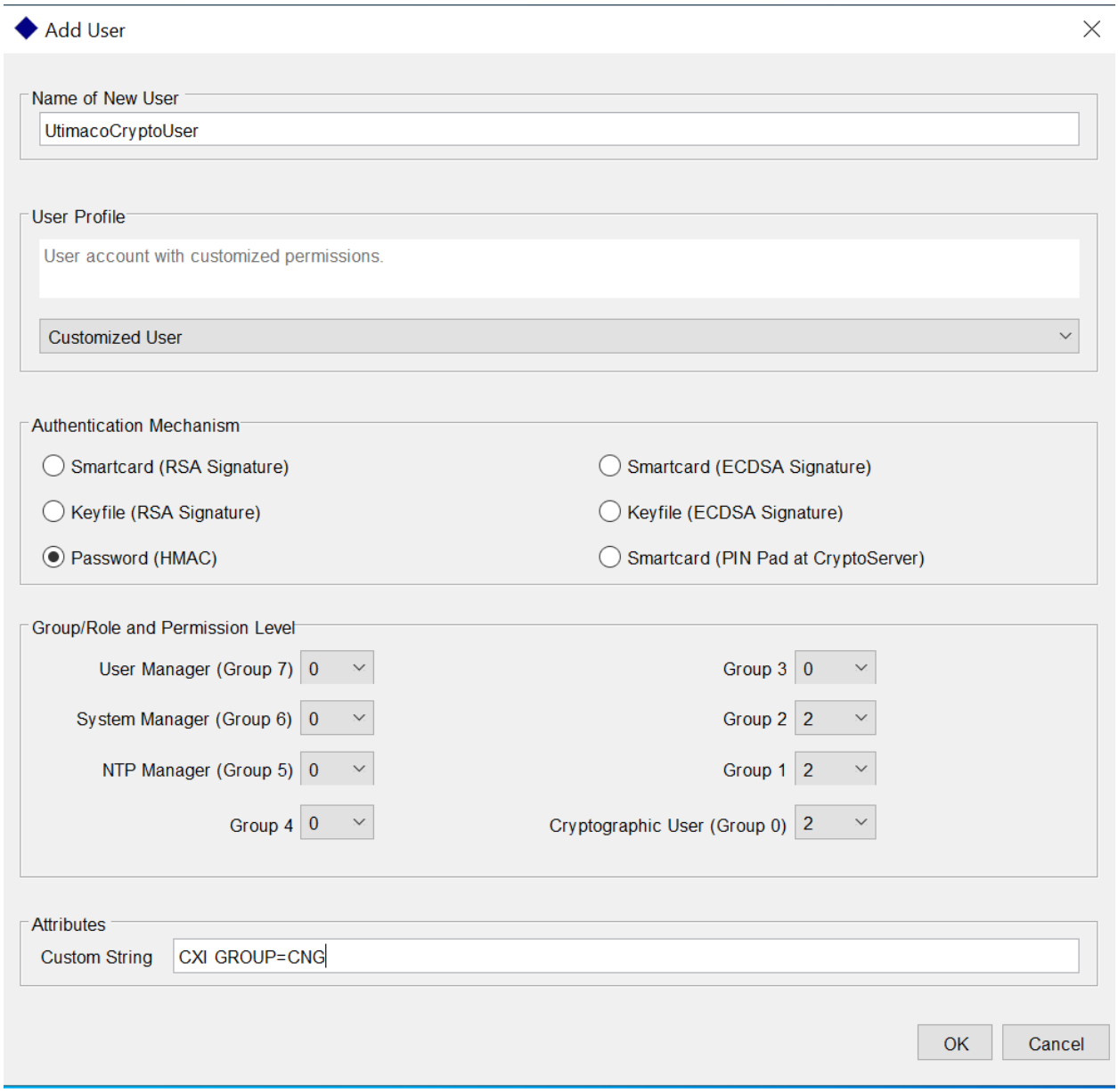

Figure 2 : Creating a Crypto user

Based on your requirements, the user can use Password (HMAC), Smartcard or Keyfile protection type. If you are using Smartcard Authentication, the PIN Pad device will prompt to insert the Smartcard and enter the PIN. Then press the OK button on the PIN Pad.

4.3 Setting up the CSP/CNG Provider

The `CS_CNG_CFG` environment variable contains the path and name of the configuration file.

By default, it is located at `C:\ProgramData\Utimaco\CNG\cs_cng.cfg`.

For more advanced configuration, refer to [CspCng];

1. Open the `cs_cng.cfg` file with an appropriate text editor.

```
notepad %CS_CNG_CFG%
```

2. For this installation, set the path to the log file and set the log level to **ERROR**.

```
# Path to the logfile (name of logfile is attached by the API)

Logpath = C:\ProgramData\Utimaco\CNG\log

# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)  Logging = 1
```

To make your testing easier, it would be good to enable the CNG log file. That can be enabled by editing the Logging Loglevel. Set the LogPath and Logging Loglevel to 1. For testing you may want to increase it to 4.

The added LogPath points to a writable directory, not to a file.

If you encounter problems, check the log file named `cs_cng.log` in the LogPath defined directory. When you are done testing, you should change Logging to 1 or 2. This will limit the logging to only critical and important messages.

3. Set the **Login**. In this case, the name of the Cryptographic User is **UtimacoCryptoUser** with an HMAC password.

```
Login = UtimacoCryptoUser,HMACPwd=<password>
```

If using Smartcard or KeyFile protection, make the appropriate change in the Login Section as shown below:

Login = username,RSASign=filename#password

Login = "SmartCardUser,RSASign=:cs2:auto:USB0@<HSM-IP>"

For additional information refer to the CryptoServer_csadm_Manual_Systemadministrators.pdf document, found on the product CD in the Documentation directory.

4. Set the IP address of the HSM.

```
# default device and fallback devices
Device = 3001@<IP>
```

For more information regarding the commands and command parameters, please check the Utimaco documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

Device = 288@<HSM IP address> Hardware (LAN) HSM

OR

Device = /dev/cs2.0 Hardware (PCIe) HSM

4.3.1 Testing Connection

To enumerate providers, use the following command:

```
cngtool EnumProvider
```

```
C:\Program Files\Utimaco\SecurityServer\Administration>cngtool EnumProvider
Microsoft Key Protection Provider
Microsoft Passport Key Storage Provider
Microsoft Platform Crypto Provider
Microsoft Primitive Provider
Microsoft Smart Card Key Storage Provider
Microsoft Software Key Storage Provider
Microsoft SSL Protocol Provider
Windows Client Key Protection Provider
Utimaco CryptoServer Key Storage Provider
```

Figure 3 : Enumerate providers

To get the provider information, use the following command:

```
cngtool ProviderInfo
```

```
C:\ProgramData\Utimaco\CNG>cngtool ProviderInfo

------------------------------------------------------------

Provider          : Utimaco CryptoServer Key Storage Provider
Device            : 3001@172.31.1.130
Group             : CNG
Mode              : Internal Key Storage

------------------------------------------------------------
Name              : Utimaco CryptoServer Key Storage Provider
Version           : 0x06040000
Impl.-Type        : 0x00000011
MaxNameLength     : 0x00000104
Device            : 3001@172.31.1.130
Group             : CNG
Mode              : Internal Key Storage
```

Figure 4 : Provider details

5 Generate the Authenticode Key using PowerShell

The following procedure demonstrates the key and certificate generation for the Authenticode and signing executables using the PowerShell script.

5.1 Install the PowerShell PKI Module

PKI Module is intended to simplify various PKI management tasks by using automation with Windows PowerShell. It is intended for Certification Authority (CA) management.

Using the below command in PowerShell, the user will get all the PKI modules installed.

```
C:\> Install-Module -Name PSPKI
```

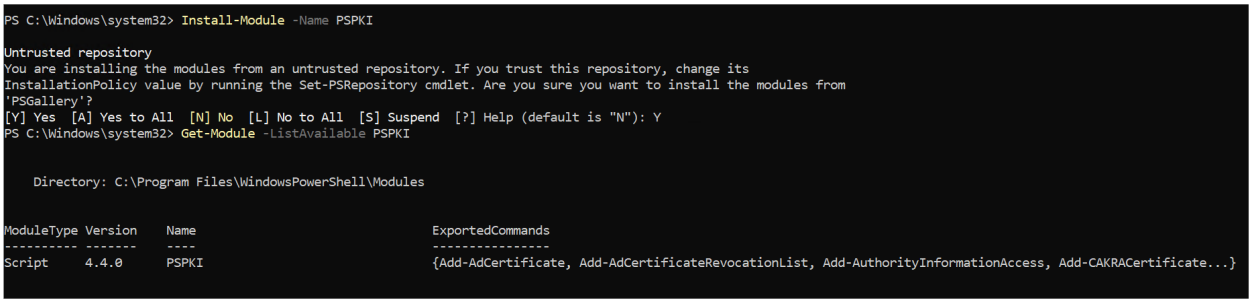

Figure 5 : PKI Module installation window

Verify the following PKI modules are installed correctly by running the following command.

```
Get-Command -Module PKI
```

```
PS C:\Windows\system32> Get-Command -Module PKI

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Cmdlet          Add-CertificateEnrollmentPolicyServer              1.0.0.0    PKI
Cmdlet          Export-Certificate                                 1.0.0.0    PKI
Cmdlet          Export-PfxCertificate                              1.0.0.0    PKI
Cmdlet          Get-Certificate                                    1.0.0.0    PKI
Cmdlet          Get-CertificateAutoEnrollmentPolicy                1.0.0.0    PKI
Cmdlet          Get-CertificateEnrollmentPolicyServer              1.0.0.0    PKI
Cmdlet          Get-CertificateNotificationTask                    1.0.0.0    PKI
Cmdlet          Get-PfxData                                        1.0.0.0    PKI
Cmdlet          Import-Certificate                                 1.0.0.0    PKI
Cmdlet          Import-PfxCertificate                              1.0.0.0    PKI
Cmdlet          New-CertificateNotificationTask                    1.0.0.0    PKI
Cmdlet          New-SelfSignedCertificate                          1.0.0.0    PKI
Cmdlet          Remove-CertificateEnrollmentPolicyServer           1.0.0.0    PKI
Cmdlet          Remove-CertificateNotificationTask                 1.0.0.0    PKI
Cmdlet          Set-CertificateAutoEnrollmentPolicy                1.0.0.0    PKI
Cmdlet          Switch-Certificate                                 1.0.0.0    PKI
Cmdlet          Test-Certificate                                   1.0.0.0    PKI
```

Figure 6 : PKI Module list

5.2 Generate the Authenticode Key

To generate the Authenticode Key, follow the steps below.

1. Create a PowerShell script file with the name `Generate_AuthenticodeKey.ps1` at the appropriate location, and add the following content into the script file.

```
#Define Utimaco Provider

$UtimacoProviderName = "Utimaco CryptoServer Key Storage Provider"

#Define Algorithm

$AlgorithmName = "RSA"

#Define Key Size

$KeySize = 2048

# Provide the Key Name

$KeyName = "Authenticode_TestKey"

$KeyParams = New-Object

System.Security.Cryptography.CngKeyCreationParameters

$KeyParams.provider = New-Object
```

```
System.Security.Cryptography.CngProvider($UtimacoProviderName)

$KeyParams.KeyCreationOptions =

[System.Security.Cryptography.CngKeyCreationOptions]::OverwriteExistingKe y

$keySizeProperty = New-Object

System.Security.Cryptography.CngProperty("Length",[System.BitConverter]::

GetBytes($KeySize),

[System.Security.Cryptography.CngPropertyOptions]::None);

$KeyParams.Parameters.Add($keySizeProperty)

$Algorithm = New-Object

System.Security.Cryptography.CngAlgorithm($AlgorithmName)

$Key = [System.Security.Cryptography.CngKey]::Create($Algorithm, $KeyName,
$KeyParams)
```

2. Launch PowerShell as Administrator, and run `Generate_AuthenticodeKey.ps1`.

```
.\Generate_AuthenticodeKey.ps1
```

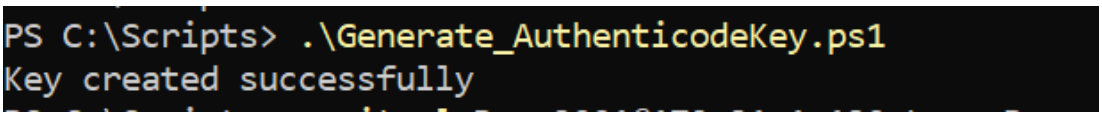

Figure 7 : Key created successfully

If you are using Smartcard Authentication, the PIN Pad device will prompt to insert the Smartcard and enter the PIN. Then, press the OK button on the PIN Pad.

3. The generated keys will be protected by the HSM and can be verified using the command below.

```
cngtool ListKeys
```

```
PS C:\Scripts> cngtool ListKeys

------------------------------------------------------------

Provider          : Utimaco CryptoServer Key Storage Provider
Device            : 3001@172.31.1.130
Group             : CNG
Mode              : Internal Key Storage

------------------------------------------------------------

Index  AlgId        Size   Group           Name                                Spec
-------------------------------------------------------------------------------
1      RSA          2048   CNG             Authenticode_CLI_Key                0
2      RSA          2048   CNG             tq-98f02315-592d-451a-a685-4d825ab34fc8 0
3      RSA          2048   CNG             tq-714a99bd-6e3d-44c7-a3ab-9d78db4af549 0
4      RSA          2048   CNG             Authenticode_TestKey                0
```

Figure 8 : List keys

If you are using Smartcard Authentication, the PIN Pad device will prompt to insert the Smartcard and enter the PIN. Then, press the OK button on the PIN Pad.

5.3 Generate the Authenticode Signing Certificate

To generate a self-signed code signing certificate, follow the steps below.

1. Create a PowerShell script file with the name `Generate_Authenticode_SelfCert.ps1` at the appropriate location, and add the following content into the script file.

```
# Define Utimaco Provider
$UtimacoProviderName = "Utimaco CryptoServer Key Storage Provider"

# Define Subject Name of the Self Signed Certificate
$SubjectName = "Authenticode Certificate"

# Define Friendly Name
$FriendlyName = "Authenticode_SelfCert"

# Based on the Key Store (Local Machine or Current user) make appropriate changes
# in location name parameter
 $LocationName = "Cert:\LocalMachine\My"
#$LocationName = "Cert:\CurrentUser\My"

# Container name should match with Keyname parameter in 5.2 section
```

```
$ContainerName = "Authenticode_TestKey"

# Generate Self Signed Certificate
New-SelfSignedCertificate `
  -Subject $SubjectName `
  -FriendlyName $FriendlyName `
  -Type CodeSigningCert `
  -CertStoreLocation $LocationName `
  -Provider $UtimacoProviderName `
  -ExistingKey `
  -Container $ContainerName
```

2. Launch PowerShell as Administrator, and run `Generate_Authenticode_SelfCert.ps1`.

```
.\Generate_Authenticode_SelfCert.ps1
```

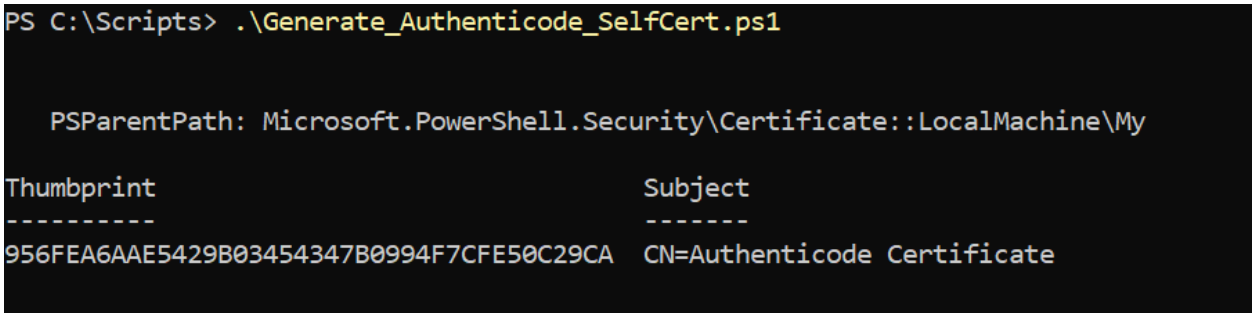

Figure 9 : Generate certificate

If you are using Smartcard Authentication, the PIN Pad device will prompt to insert the Smartcard and enter the PIN. Then, press the OK button on the PIN Pad.

3. The self-signed certificate can be viewed in a PowerShell window, as seen below.

```
Get-ChildItem -Path Cert:\CurrentUser\My -CodeSigningCert -Recurse
```

```
PS C:\Scripts> Get-ChildItem -Path Cert:\CurrentUser\My -CodeSigningCert -Recurse


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
6677BE59A0C0E6479589B17F8EC2CA94BEEFB4F0  CN=Authenticode Certificate
```

Figure 10 : Self-signed certificate details

5.4 Sign and Time-Stamp the Code with Microsoft SDK

Sign Tool is a command-line tool used for verifying signatures in files, signing files digitally, and time-stamping files. To time-stamp an `.exe` file, the user must use an online Time Stamp Server (TSS).

5.4.1 Exporting a Certificate

1. Create a PowerShell script file with the name `Export_Certificate.ps1` at the appropriate location, and add the following content into the script file.

```
# Get the certificate
#$SelfCertificate = Get-ChildItem -Path Cert:\CurrentUser\My\ |
$SelfCertificate = Get-ChildItem -Path Cert:\LocalMachine\My\ |
Where-Object { $_.Subject -eq "CN=Authenticode Certificate" }

# Export the Self Signed Certificate
Export-Certificate `
  -FilePath "C:\Authenticode\Authenticode_Certificate.cer" `
  -Cert $SelfCertificate
```

2. Launch PowerShell as Administrator, and run `Export_Certificate.ps1`.

```
.\Export_Certificate.ps1
```

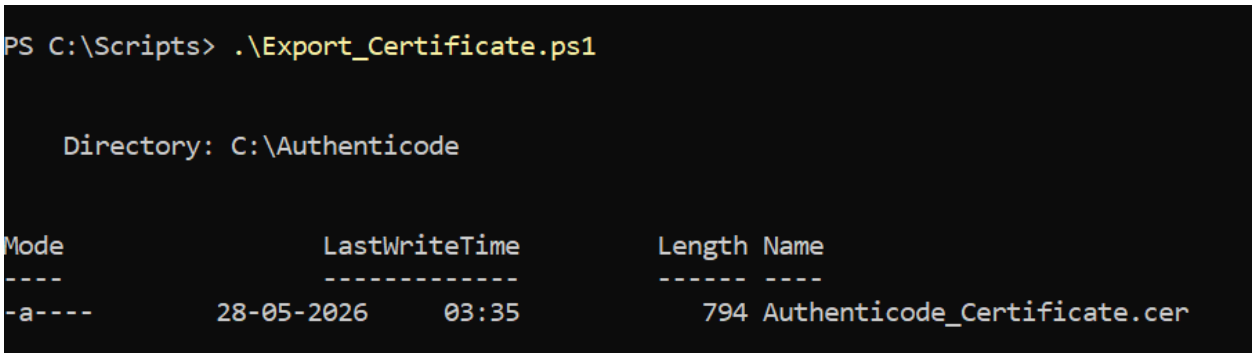

Figure 11 : Exporting the certificate

3. To view the Properties, double-click on the exported certificate.

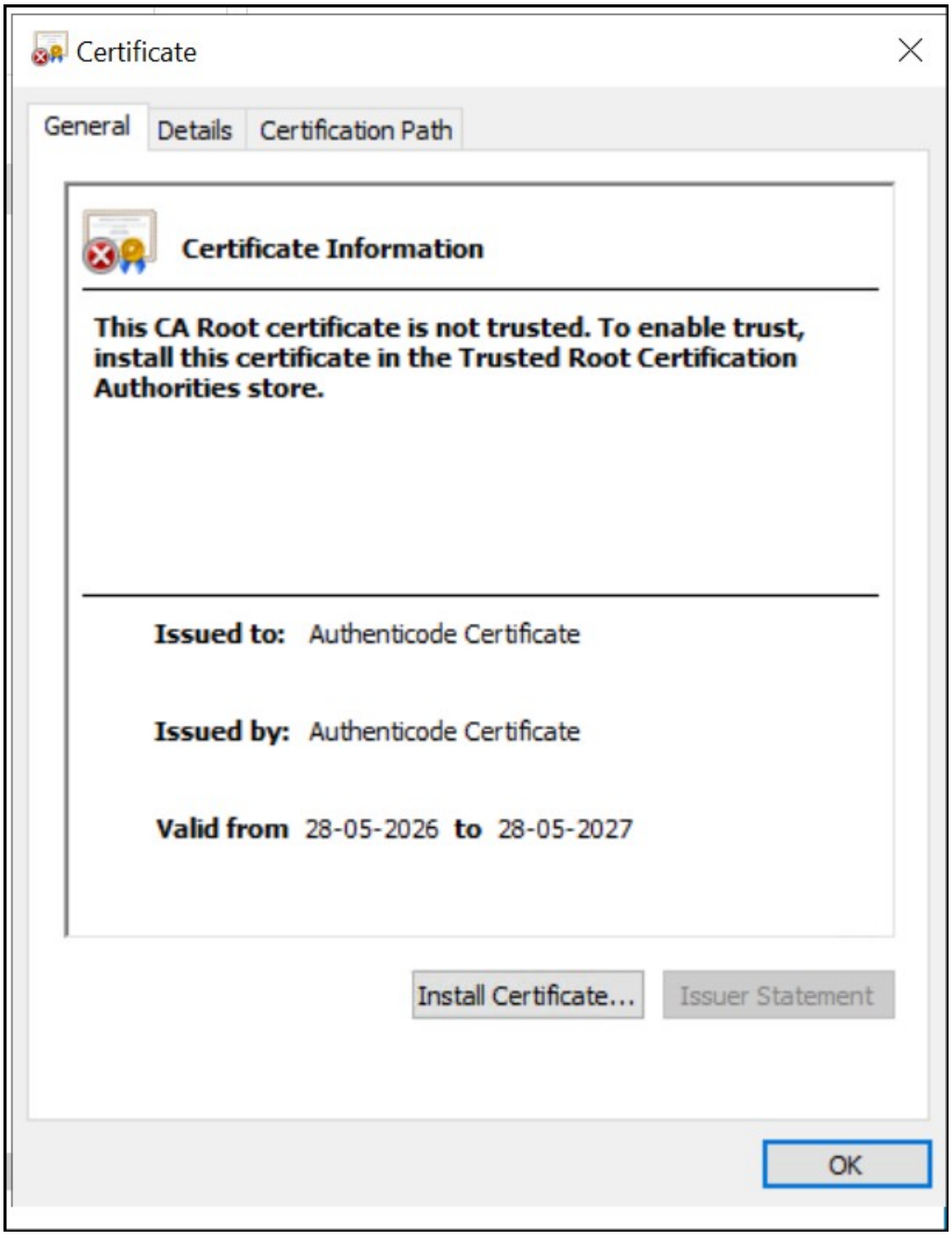

Figure 12 : Exported certificate details

5.4.2 Sign and Time-Stamp the Executable

There are different ways to access the code-signing certificate using Signtool.

- The preferred method to do this is directly from the certificate stored with the thumbprint.
- The second method is by using the key name.
- The third method is by pointing to a `.cer` file that was created by exporting the certificate.

In this guide, an executable file called `MyApplication.exe` was created, signed, and time-stamped.

1. Create a PowerShell script file with the name `Sign_Timestamp_Executable.ps1` and add the following content into the script file.

```
#The first method using the certificate hash value
#Get the certHash Value from Step 3 in section 5.3
$certHash = "956FEA6AAE5429B03454347B0994F7CFE50C29CA"
#The second method is name of the key
#Key name generated in section 5.2
$ContainerName = "Authenticode_TestKey"
#The third method is by using an exported certificate path
#Self Signed Certificate name generated in section 5.3
$SelfCertName = "Authenticode Certificate"
$SelfSignedCertificatePath = "C:\Authenticode\Authenticode_Certificate.cer"
# Certificate Services Time Stamp Server
$timestampServer = "http://timestamp.digicert.com”
# File to be Signed
$fileName = "C:\Authenticode\MyApplication.exe"
# signtool path (recommended)
$signtoolPath = "C:\Program Files (x86)\Windows
Kits\10\bin\10.0.22621.0\x64\signtool.exe"
&$signtoolPath sign `
  /debug `
  /tr $timestampServer `
  /td sha256 `
  /fd sha256 `
  /a `
  $fileName
```

2. Launch PowerShell as Administrator and run `Sign_Timestamp_Executable.ps1`. Enter the passphrase when prompted.

```
.\Sign_Timestamp_Executable.ps1
```

›_ PowerShell

```
> .\Sign_Timestamp_Executable.ps1

The following certificates were considered:

    Issued to: Authenticode Certificate

    Issued by: Authenticode Certificate

    Expires:   Fri Mar 17 09:57:01 2023

    SHA1 hash: 1974f986d9b8bf32f47fc2af33d6271dd905c44f

After EKU filter, 1 certs were left.

After expiry filter, 1 certs were left.

After Subject Name filter, 1 certs were left. After Private Key filter, 1 certs
were left. The following certificate was selected:

    Issued to: Authenticode Certificate

    Issued by: Authenticode Certificate

    Expires:   Fri Mar 17 09:57:01 2023

    SHA1 hash: 1974f986d9b8bf32f47fc2af33d6271dd905c44f

Done Adding Additional Store

Successfully signed: C:\Authenticode\MyApplication.exe

Number of files successfully Signed: 1

Number of warnings: 0

Number of errors: 0
```

If you are using Smartcard Authentication, the PIN Pad device will prompt to insert the Smartcard and enter the PIN. Then, press the OK button on the PIN Pad.

3. You can verify that your application is now signed by right-clicking on it and selecting **Properties**. On the **Digital Signatures** tab (if it exists), you can view the signing certificate and time-stamp.

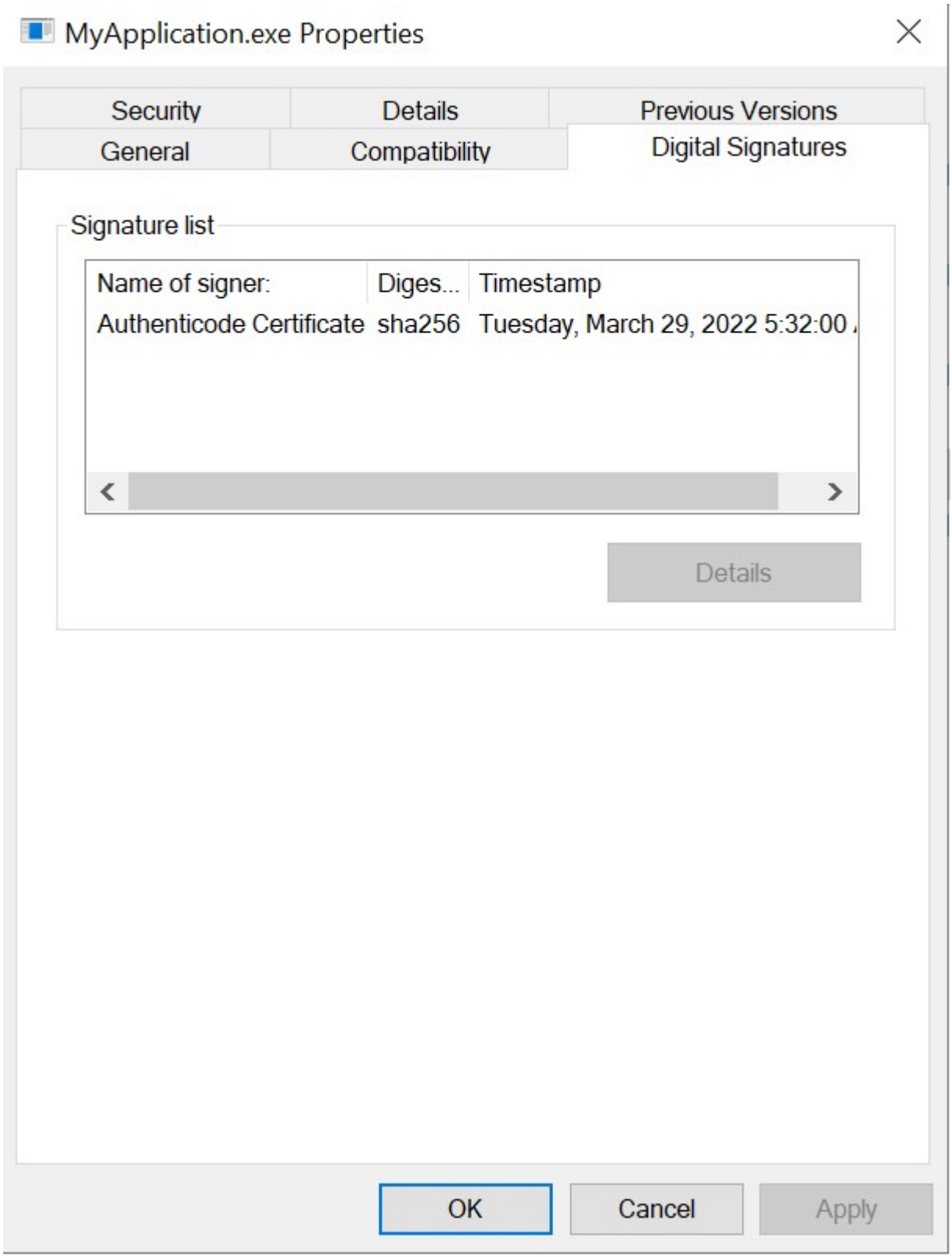

Figure 13 : Digital signature details

6 Generate the Authenticode Key using CLI

6.1 Create Certificate Request

It is necessary to create a specific certificate for the code-signing purposes. This certificate is installed in the local Windows certificate store (e.g., personal store). To retrieve an official code signing certificate issued by a certification authority, you have to create a certificate request (CSR) first. Normally, an official certificate authority (e.g., VeriSign, Thawte, DigiCert) will create and sign a certificate based on your certificate request. If you don't need an officially signed certificate, you can use an in-house certificate authority (e.g., Microsoft Windows Server Certification Authority).

To create a code-signing certificate request, you first need to create a template file `.inf`. You will then issue the certificate request based on this template file using Microsoft's utility `certreq.exe`.

Create a file called `request.inf`, which should include, amongst others, the following information:

- The subject details must include a 2-letter country code (**C**) and a common name (**CN**), which may be your company name.
- **KeyAlgorithm** and **KeyLength** as required (e.g., RSA, 2048 bit key).
- The Cryptographic Service **ProviderName**. For use with CryptoServer, this needs to be Utimaco CryptoServer Key Storage Provider.
- You can add a **KeyContainer** parameter to set the key name in the CryptoServer. This helps to distinguish several code-signing keys from each other. If no **KeyContainer** is specified, a random string is generated, starting with "CertReq".

```
[Version]

Signature = "$Windows NT$"

[NewRequest]

Subject = "CN=Utimaco Code Signing,O=Utimaco,L=Aachen,C=DE"

KeyAlgorithm = RSA

KeyLength = 2048

Exportable = FALSE
```

```
MachineKeySet = FALSE

ProviderName = "Utimaco CryptoServer Key Storage Provider"

KeyUsage = CERT_DIGITAL_SIGNATURE_KEY_USAGE

KeyUsageProperty = NCRYPT_ALLOW_SIGNING_FLAG

HashAlgorithm = SHA256

KeyContainer = Authenticode_CLI_Key

[EnhancedKeyUsageExtension]

OID = 1.3.6.1.5.5.7.3.3 ; Code Signing
```

It is important that the **ProviderName** is given as Utimaco CryptoServer Key Storage Provider. This links the code-signing certificate with the private key which is stored in the CryptoServer.

1. Open a command prompt.
2. Change to the directory where you have saved the `request.inf` file.
3. Execute the following command. If you would like to review the actions of the command on the CryptoServer for debug purposes, enable logging in the CNG configuration file.

```
certreg -new request.int requestcert.reg
```

```
PS C:\Authenticode> certreq -new request.inf requestcert.req

CertReq: Request Created
```

Figure 14 : Certificate request created

`certreq` creates a certificate request file `request.req` that can either be sent to an official certificate authority or be signed with your in-house certificate authority.

If you are using Smartcard Authentication, the PIN Pad device will prompt to insert the Smartcard and enter the PIN. Then, press the OK button on the PIN Pad.

6.2 Install the Code Signing Certificate

After creating a certificate request, you obtain the certificate from a certificate authority or from your own certificate authority. In the following, we name that file `codesign.crt`. To use your code signing certificate, you need to install this in your local Windows certificate store. This can be achieved by the GUI or the command line.

6.2.1 Command Line Procedure

If you have created the certificate request on the same computer using `certreq`, Windows has "remembered" this open request. To install the certificate now, simply run:

›_ Console

```
C:\>certreq -accept -user codesign.crt

Installed Certificate:

  Serial Number: 2d0000002ba56ec00d8b611e4a00000000002b

  Subject: CN=YourCompany Code Signing, O=YourCompany, L=Aachen, C=DE

  NotBefore: 3/25/2022 8:31 AM

  NotAfter: 3/25/2023 8:31 AM

  Thumbprint: f61f71e40bcb5d14452d7edd2a034d22801fb547
```

Since Windows has also remembered that the key for this certificate was created with the Utimaco CryptoServer Key Storage Provider, it has already associated the certificate with that key provider and container. Thus, you can directly move on to sign code.

However, if the request was created on another computer or if you need to reinstall the certificate, an error will be shown:

›_ Console

```
C:\>certreq -accept -user codesign.crt

Certificate Request Processor: Cannot find object or property. 0x80092004
(-2146885628)
```

In that case, you first have to import the certificate and then manually associate it with the key provider and container.

1. Run the following command to import the certificate:

›_ Console

```
C:\>certutil -addstore -user My codesign.crt

My "Personal"

Related Certificates:


Exact match:

Element 0:

Serial Number: 2d0000002ba56ec00d8b611e4a00000000002b

Issuer: CN=Utimaco-RootCA, DC=utimaco, DC=local

 NotBefore: 3/25/2022 8:31 AM

 NotAfter: 3/25/2023 8:31 AM

Subject: CN=YourCompany Code Signing, O=YourCompany, L=Aachen, C=DE

Non-root Certificate

Template:

1.3.6.1.4.1.311.21.8.16593323.14862581.6636168.15641503.12204691.200.1114
8576.10529166

Cert Hash(sha1): f61f71e40bcb5d14452d7edd2a034d22801fb547

CertUtil: -addstore command completed successfully.
```

2. Then, run the following command to obtain the serial number. Replace “YourCompany Code Signing” with the common name (**CN** field) of your certificate.

›_ Console

```
C:\>certutil -store -user My "YourCompany Code Signing" | findstr Serial

Serial Number: f61f71e40bcb5d14452d7edd2a034d22801fb547
```

3. Use the `certutil` tool to link the private key on the CryptoServer with the code-signing certificate:

›_ Console

```
C:\>certutil -repairstore -user My <SerialNumber>

My "Personal"

================ Certificate 0 ================

Serial Number: f61f71e40bcb5d14452d7edd2a034d22801fb547

Issuer: CN=Utimaco-RootCA, DC=utimaco, DC=local

NotBefore: 3/25/2022 8:31 AM

NotAfter: 3/25/2023 8:31 AM

Subject: CN=YourCompany Code Signing, O=YourCompany, L=Aachen, C=DE

Non-root Certificate

Template:

1.3.6.1.4.1.311.21.8.16593323.14862581.6636168.15641503.12204691.200.1114
8576.10529166

Cert Hash(sha1): f61f71e40bcb5d14452d7edd2a034d22801fb547

  Key Container = tq-e5742d68-a308-4768-969c-dc11f7c3ed63

  Unique container name: D5A46CE713A51CA294D36197C327E614   Provider = Utimaco
CryptoServer Key Storage Provider

Private key is NOT exportable

Signature test passed

CertUtil: -repairstore command completed successfully.
```

6.2.2 GUI Procedure

Using the GUI, the procedure is as follows:

1. Run `certmgr.msc`, either by pressing Windows-R or opening a console and entering this command.
2. Right-click on **Certificates - Current User > Personal** and then click on **All Task > Import** and follow the instructions to import the signed certificate. Verify the certificate is successfully imported in **Certificates - Current User > Personal > Certificates**.

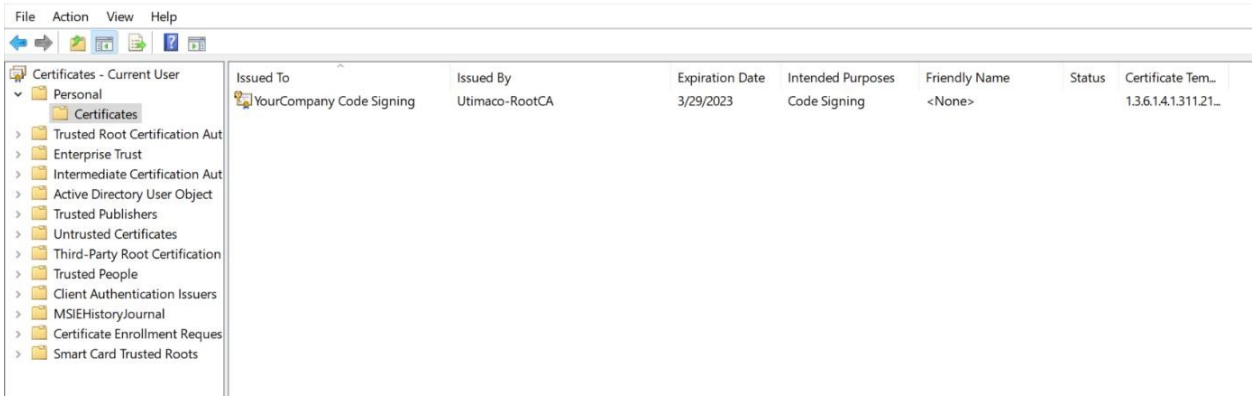

Figure 15 : Code-signing certificate

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

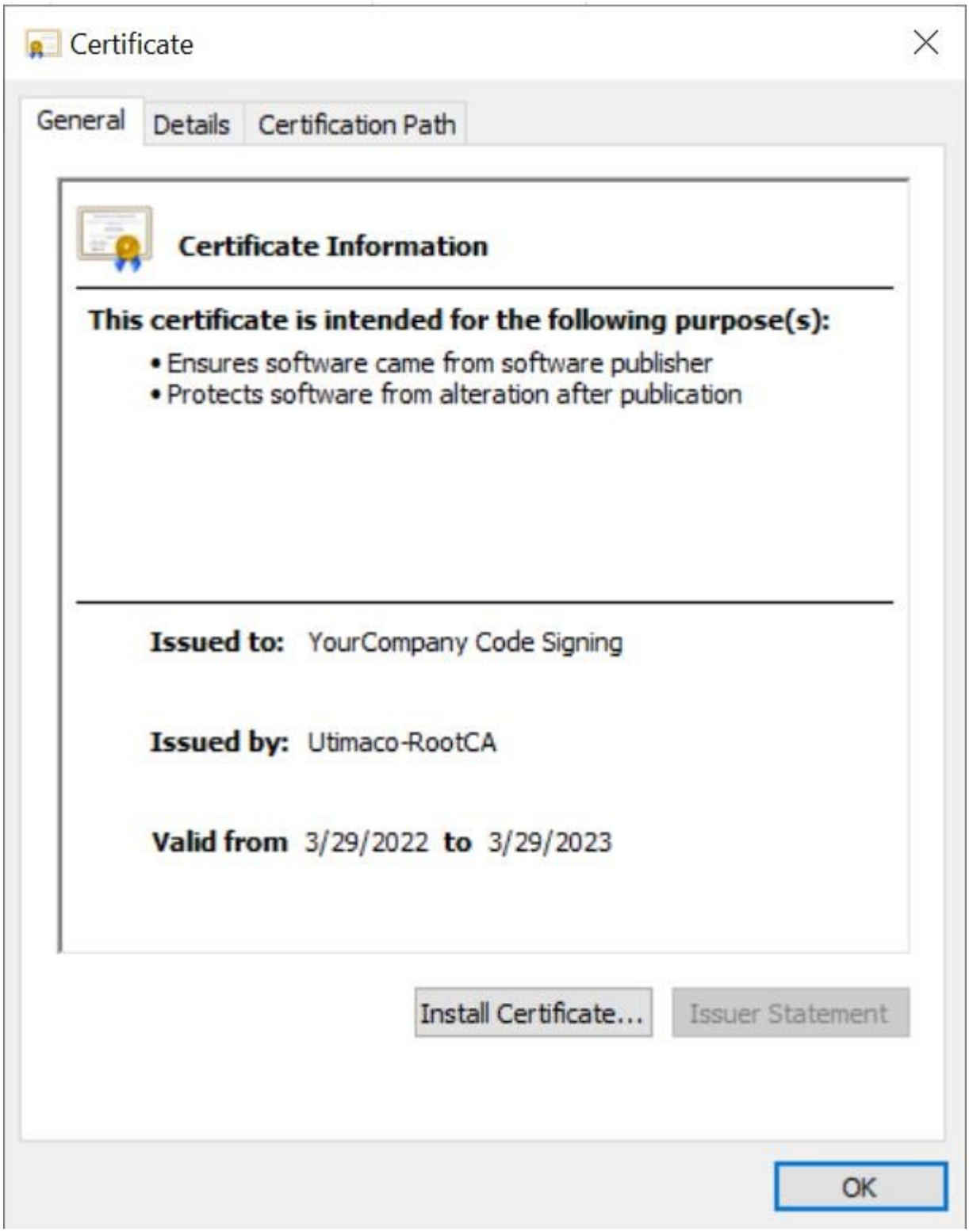

Figure 16 : Certificate properties

4. In case the private key is not mapped with private in the CryptoServer, repair the code-signing certificate using the `certutil repairstore` utility.

- Browse to the details tab.
- Select the serial number or thumb print field.
- Copy the data.
- Use the `certutil` tool to link the private key on the CryptoServer with the code-signing certificate. Don't forget the double quotes since the serial number or thumb print copied before usually contains spaces.

›_ Console

```
C:\>certutil -repairstore -user My <SerialNumber>

My "Personal"

================ Certificate 0 ================

Serial Number: f61f71e40bcb5d14452d7edd2a034d22801fb547

Issuer: CN=Utimaco-RootCA, DC=utimaco, DC=local

 NotBefore: 3/25/2022 8:31 AM

 NotAfter: 3/25/2023 8:31 AM

Subject: CN=YourCompany Code Signing, O=YourCompany, L=Aachen, C=DE

Non-root Certificate

Template:

1.3.6.1.4.1.311.21.8.16593323.14862581.6636168.15641503.12204691.200.1114
8576.10529166

Cert Hash(sha1): f61f71e40bcb5d14452d7edd2a034d22801fb547

  Key Container = tq-e5742d68-a308-4768-969c-dc11f7c3ed63

  Unique container name: D5A46CE713A51CA294D36197C327E614   Provider = Utimaco
CryptoServer Key Storage Provider

Private key is NOT exportable

Signature test passed

CertUtil: -repairstore command completed successfully.
```

5. After the `repairstore` command has been successfully executed, refresh the certificate manager snap in, open the certificate and make sure you see the message "You have a private key that corresponds to this certificate".

7 Code Signing

Once the code-signing certificate has been installed in the local personal Windows certificate store, it is possible to sign your executables, dynamic link libraries or cabinet files. Depending on how you have installed `signtool`, you might have to open a developer console in order to include `signtool` in your local Windows search path.

For the purpose of integration and verification, a self-signed certificate was generated and used for code signing. The certificate was created using the private key that was generated as part of the certificate request process.

To create a self-signed certificate, use the following command.

```
PS C:\Authenticode> New-SelfSignedCertificate `
>>   -Subject "CN=Utimaco Code Signing,O=Utimaco,L=Aachen,C=DE" `
>>   -Type CodeSigningCert `
>>   -CertStoreLocation "Cert:\LocalMachine\My" `
>>   -Provider "Utimaco CryptoServer Key Storage Provider" `
>>   -ExistingKey `
>>   -Container "Authenticode_CLI_Key"
```

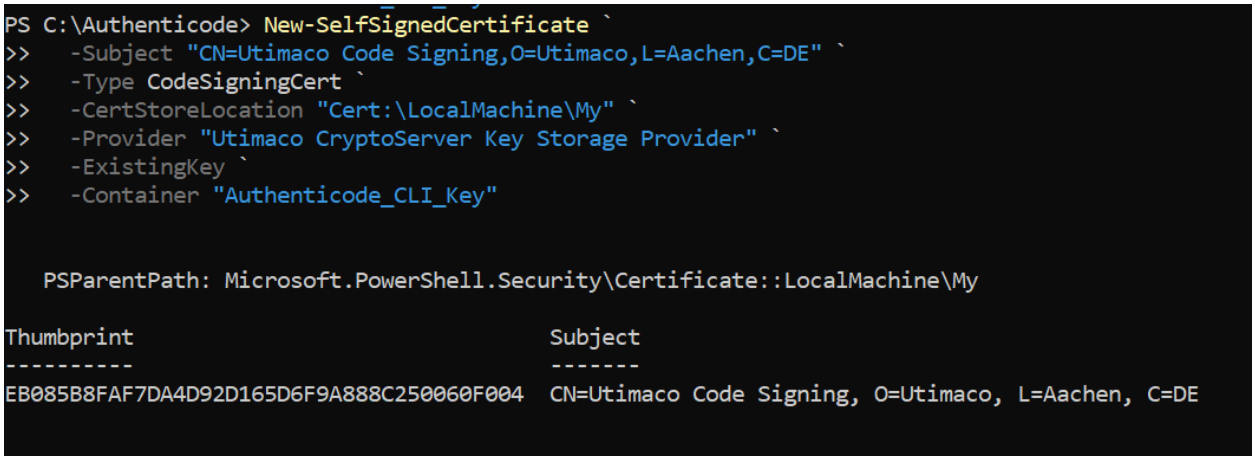

Figure 17 : Self-signed certificate created

Use the following basic command to sign your executable. Replace "YourCompany Code Signing" with the common name (**CN** field) of your certificate. You can also add the `/fd sha256` parameter to use the more secure SHA256 digest algorithm.

```
signtool sign /v /fd sha256 /sm /n "YourCompany Code Signing" sample.exe
```

```
PS C:\Authenticode> & "C:\Program Files (x86)\Windows Kits\10\bin\10.0.22621.0\x64\signtool.exe" sign `
>>   /v `
>>   /fd sha256 `
>>   /sm `
>>   /n "Utimaco Code Signing" `
>>   sample.exe
The following certificate was selected:
    Issued to: Utimaco Code Signing
    Issued by: Utimaco Code Signing
    Expires:   Fri May 28 19:36:29 2027
    SHA1 hash: EB085B8FAF7DA4D92D165D6F9A888C250060F004

Done Adding Additional Store
Successfully signed: sample.exe

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

Figure 18 : Code-signed the exe

If you are using Smartcard Authentication, the PIN Pad device will prompt to insert the Smartcard and enter the pin. Then, press the OK button on the PIN Pad.

It is advisable to also include a time stamp in your code signature. With a time stamp, the signature usually stays valid even after the expiry date of the code-signing certificate. Add a timestamping authority like DigiCert as an extra parameter to `signtool`, as shown next.

```
signtool sign /v /fd sha256 /n "YourCompany Code Signing" /t http://
timestamp.digicert.com /td sha256 /sm /a sample.exe
```

```
PS C:\Authenticode> & "C:\Program Files (x86)\Windows Kits\10\bin\10.0.22621.0\x64\signtool.exe" sign `
>>   /v `
>>   /fd sha256 `
>>   /sm `
>>   /n "Utimaco Code Signing" `
>>   /tr http://timestamp.digicert.com `
>>   /td sha256 `
>>   sample.exe
The following certificate was selected:
    Issued to: Utimaco Code Signing
    Issued by: Utimaco Code Signing
    Expires:   Fri May 28 19:36:29 2027
    SHA1 hash: EB085B8FAF7DA4D92D165D6F9A888C250060F004

Done Adding Additional Store
Successfully signed: sample.exe

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

Figure 19 : Code-sign with time-stamp

8 Troubleshooting

Error	Diagnosis
Error B91D0003 Pin Pad API no device found	Check the connectivity between the PIN pad device and the remote server by using the below command `csadm GetCardInfo=:cs2:cjo:USB0@<ip-address>` where the PIN pad device is connected
SmartCard LoginUser= failed:	Enter the correct PIN on PIN pad device
Error related to timestampServer while running the script	Check the entry for the timestamp server in the script

PPD installation error	Check the logs for the error and reinstall it using below command:
	
	`ppd –`
	
	`config=C:ProgramData\Utimaco\PPD\ppd.cfg – install`

Cngtool command not working	Check the Environment Variable

Table 6: List of errors and their diagnoses

9 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.

10 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website: https://utimaco.com/.

11 Appendices

11.1 References

Reference	Title/Company	Document No.
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSLAN]	CryptoServerLAN_V5_Manual_Systemadministrators.pdf	2018-0010
[CSP-CNG]	CryptoServer_Manual_CSP_CNG.pdf	2008-0002

Table 7: References

11.2 Command Summary

Commands Used	Purpose
`Install-Module -Name PSPKI`	Install PKI PowerShell module
`Get-Command -Module PKI`	Verify PKI modules
`cngtool EnumProvider`	List available CNG providers
`cngtool ProviderInfo`	Display provider details
`cngtool ListKeys`	List keys stored in HSM
`certreq -new request.inf request.req`	Generate CSR and HSM key

Commands Used	Purpose
`certreq -accept codesign.crt`	Install certificate
`certutil -addstore my codesign.crt`	Import certificate into store
`certutil -store my`	View certificate details
`certutil -repairstore my <serial>`	Repair certificate-key mapping
`New-SelfSignedCertificate`	Create self-signed certificate using HSM key
`Export-Certificate`	Export certificate to file
`Get-ChildItem Cert:\LocalMachine\My`	List certificates
`signtool sign /fd sha256 /sm /a <file>`	Sign executable
`signtool verify /pa /v <file>`	Verify signature
`notepad %CS_CNG_CFG%`	Open CNG configuration file
`setx CS_CNG_CFG <path>`	Set CNG config environment variable

Table 8: List of commands used