Instruction

for activation and installation

Certum Code Signing

Table of content

1 Product description

The **Code Signing** certificate is used for digital signing of code as well as already developed and installed applications. The certificate is stored on a cryptographic card so both the code as well as already developed applications can be signed using common tools, such as ***signtool.exe*** and ***jarsigner***.

The instruction provides description of the path for activation and installation of the necessary software and show how a code or application that has already been signed - can be **signed** or **verified** using common tools.

2 Software installation

You will need the **proCertum CardManager** application, version **3.2.0.151** or higher for proper running of the Code Sign. You can download it from the website: **http://certum.eu/certum/cert,offer_software_and_libraries.xml#**

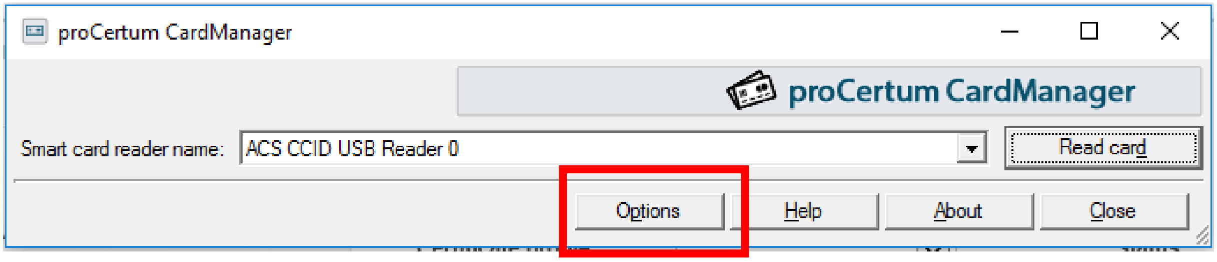
The procedure for installation of **proCertum CardManager** is as follows:

1. Download the latest version of the application from Certum website.
2. Activate the downloaded installation wizard.
3. Activate the installation wizard and click the button **Next**.
4. On the screen that will follow select "**I accept the terms of licence agreement**" and then click Next.
5. On the next screen select the path for installation of the application and then click **Next**.
6. On the screen that will follow click the **Install** button.
7. Restart your computer when the installation is finished.

3 Software configuration

1. Activate the proCertum CardManager application, version 3.2.0.151 or higher.

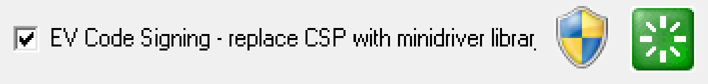
   A screen should appear with the name of your reader as shown in the screenshot below:



Smart card reader name: ACS CCID USB Reader 0

2. Click the **Options** button.

3. On the option screen select option:

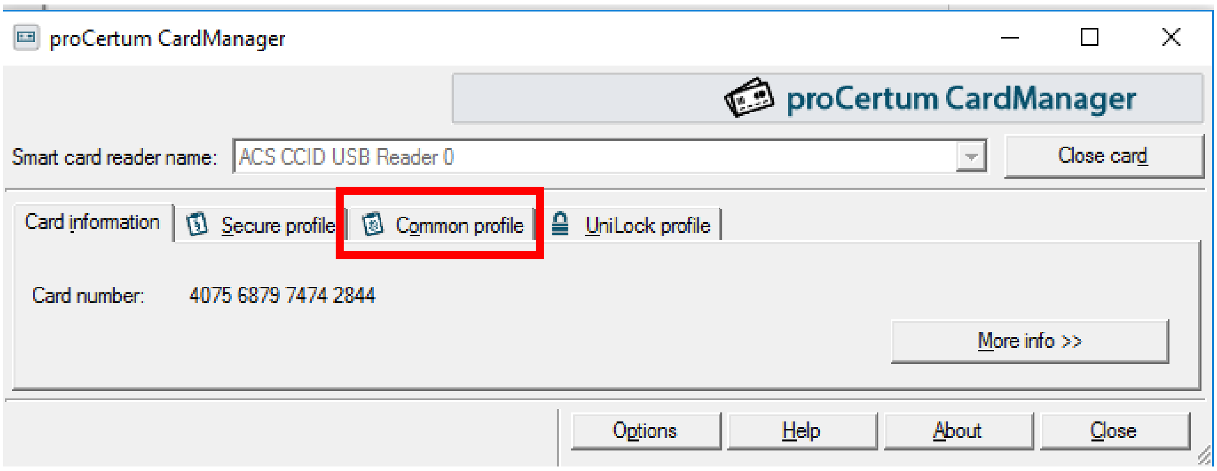


☑ EV Code Signing - replace CSP with minidriver librar

4. Restart the system. After rebooting insert the reader with the cryptographic card on which the certificate and the keys are stored.

5. To make sure that the certificate is stored on card, activate the proCertum CardManager application, select the right reader from the list (if more readers than one are configured) and click the **Read card** button.

6. Upon successful reading of the card a screen should appear as shown in the screenshot below:



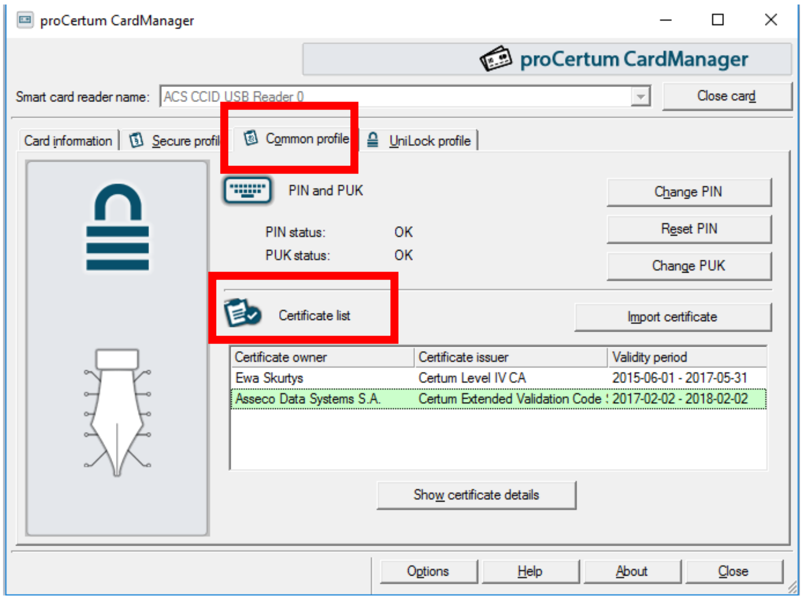
proCertum CardManager

Smart card reader name: ACS CCID USB Reader 0

Card number: 4075 6879 7474 2844

7. Go to **Common profile**.

8. Check if Common profile is active - the software should displays information about the selected profile and a list of certificates. If it is not active please go to the step 9.



proCertum CardManager

Smart card reader name: ACS CCID USB Reader 0

PIN and PUK

PIN status: OK

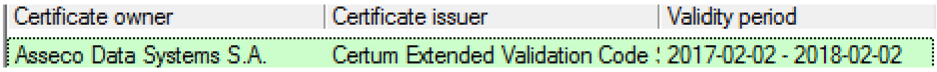
PUK status: OK

Certificate list

Certificate owner	Certificate issuer	Validity period
Ewa Skurtys	Certum Level IV CA	2015-06-01 - 2017-05-31
Asseco Data Systems S.A.	Certum Extended Validation Code :	2017-02-02 - 2018-02-02

Please note: Profile re-activation is not possible. You also cannot restore the state before activation.

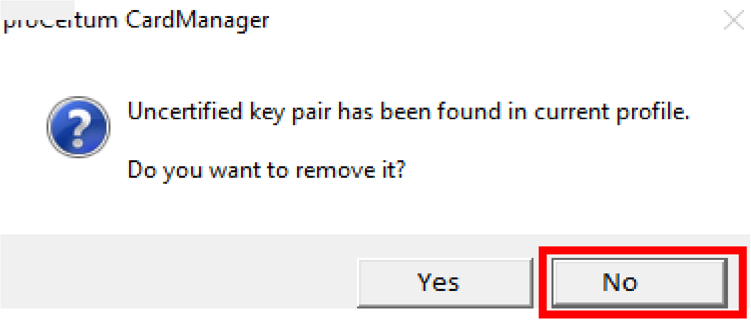
The list should include the certificate:



Certificate owner	Certificate issuer	Validity period
Asseco Data Systems S.A.	Certum Extended Validation Code :	2017-02-02 - 2018-02-02

The field "Certificate owner" will be needed at a later stage when signing the code or application.

Please note: Below message means that private key was installed on cryptographic card but certificate installation wasn't completed because certificate was not installed properly. It is recommended to click button NO and complete the installation process.

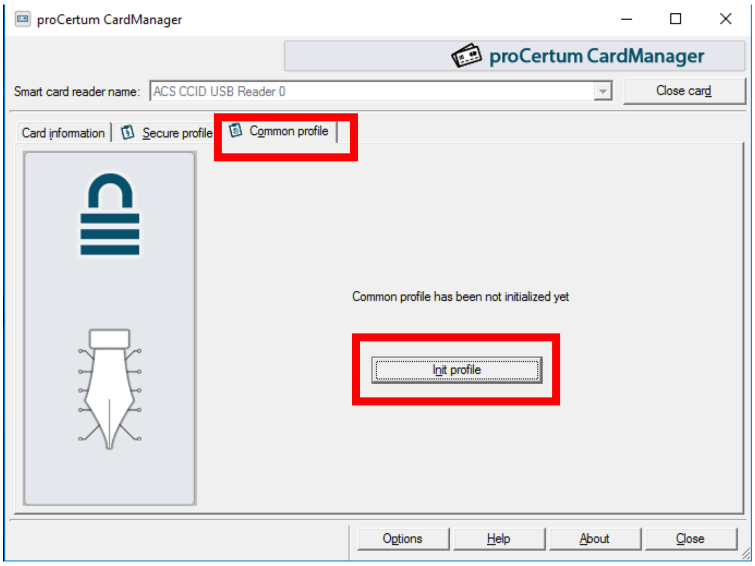


proCertum CardManager

Uncertified key pair has been found in current profile.

Do you want to remove it?

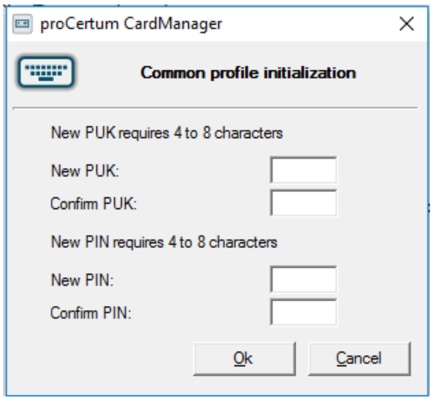
9. If the Common profile is not active, press the button **Init profile**. Then please define your new **PUK and PIN**. Each time the provided code needs to be confirmed. Press the **OK** button.



proCertum CardManager

Smart card reader name: ACS CCID USB Reader 0

Common profile has been not initialized yet



proCertum CardManager

Common profile initialization

New PUK requires 4 to 8 characters

New PUK:

Confirm PUK:

New PIN requires 4 to 8 characters

New PIN:

Confirm PIN:

After activating the common profile your cryptographic card is ready to install the Code Signing certificate.

4 Installation of certificate

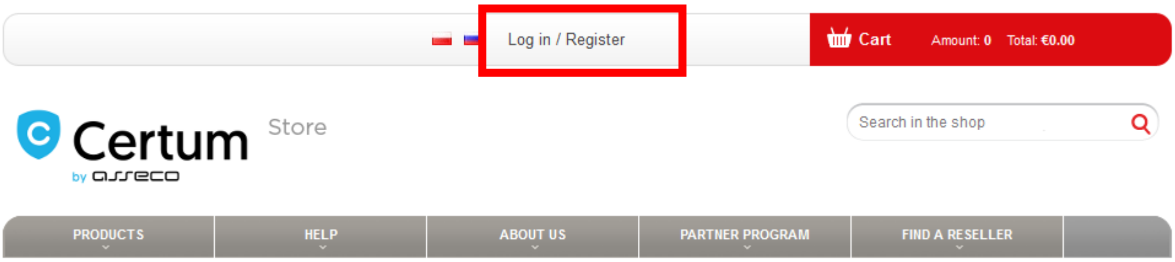
4.1 Requirements

Install the certificate using the proCertum CardManager application (Find below the installation and configuration instruction), **Internet Explorer 8**,**9**,**10 11** or Chrome browser as well as **card reader with cryptographic card** with a **normal profile** linked to the computer, stored on the card.

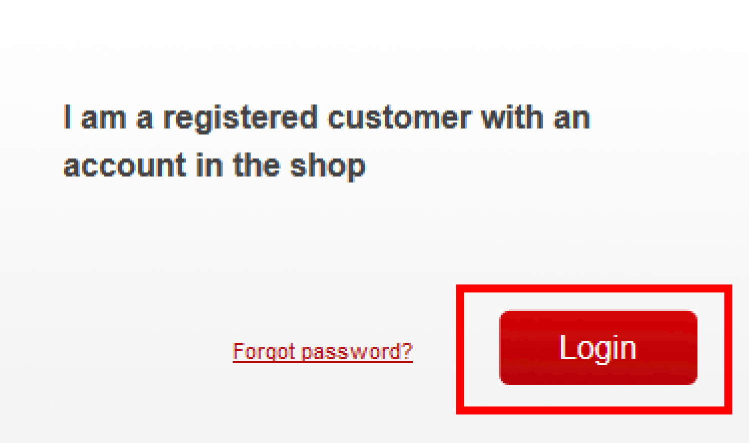
4.2 Activation of certificate

1. Having received the scratchcard or activation code please enter the **Certum store** at: https://en.sklep.certum.pl/

2. Click the **Log in/Register** button

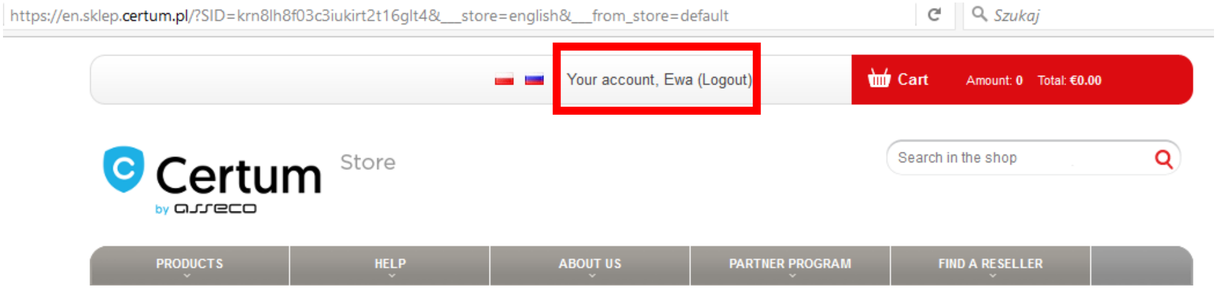


1. Log in to the **Certum account** (please create an account if you do not have one yet)



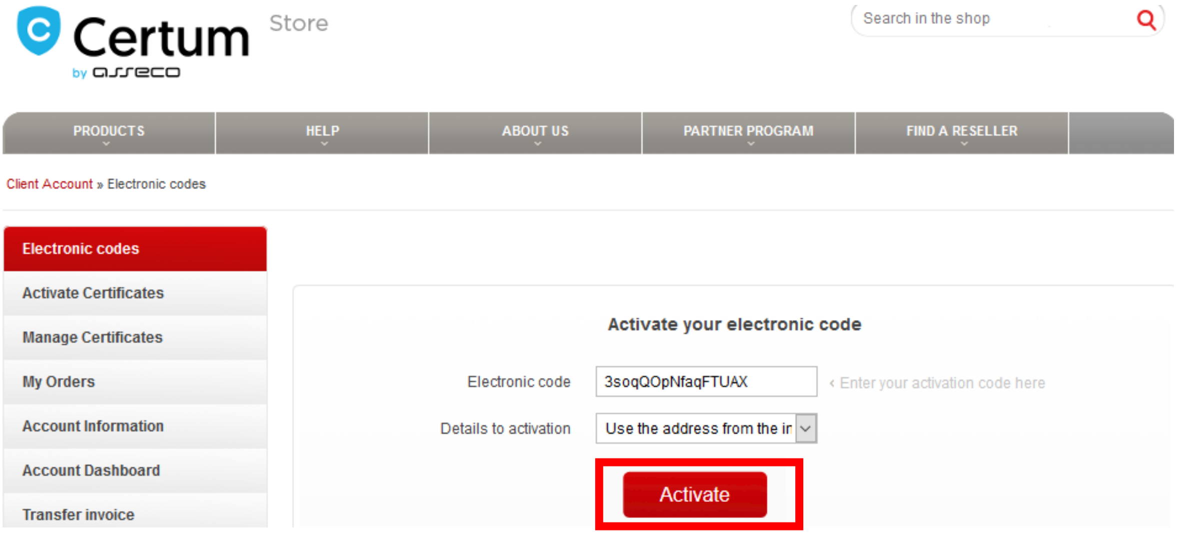
I am a registered customer with an account in the shop

4. Click the **"Your account"** button.



https://en.sklep.certum.pl/?SID=krn8lh8f03c3iukirt2t16glt4&___store=english&___from_store=default

5. If you have already received your activation code. Go to the **"Electronic codes"** section and activate the code. If you do not receive activation code please go to point 6.



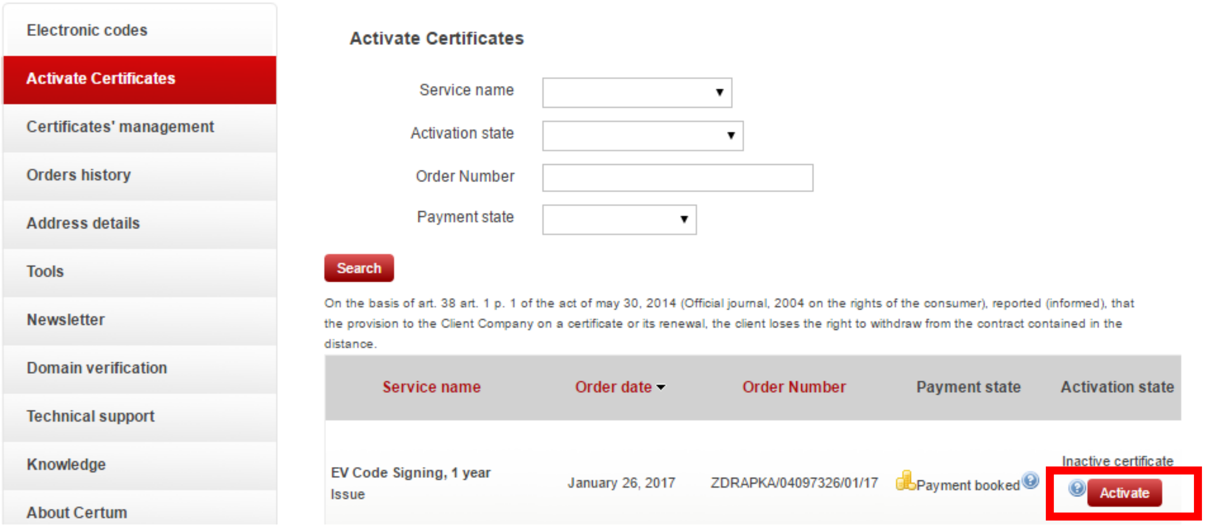
Client Account » Electronic codes

Activate your electronic code

Electronic code: 3soqQOpNfaqFTUAX ‹ Enter your activation code here

Details to activation: Use the address from the ir

6. If you have not received your code or have already successfully activated your code, go to the **"Activate Certificates"** tab. Find the **certificate** you want to activate in the list below and click **"Activate"**.



Activate Certificates

Service name ▾

Activation state ▾

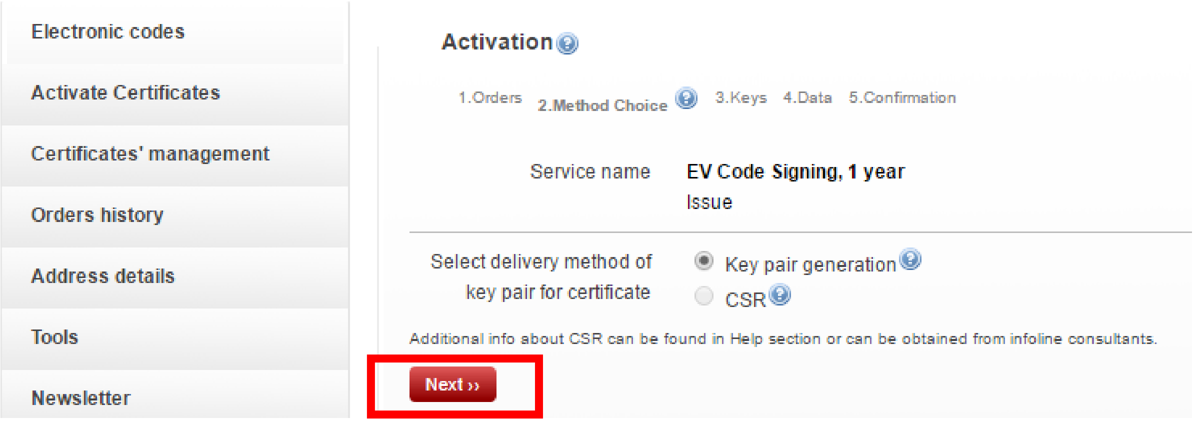
Order Number

Payment state ▾

On the basis of art. 38 art. 1 p. 1 of the act of may 30, 2014 (Official journal, 2004 on the rights of the consumer), reported (informed), that the provision to the Client Company on a certificate or its renewal, the client loses the right to withdraw from the contract contained in the distance.

Service name	Order date ▾	Order Number	Payment state	Activation state
EV Code Signing, 1 year Issue	January 26, 2017	ZDRAPKA/04097326/01/17	Payment booked	Inactive certificate Activate

8. Select the **“Generate key pair”** option and then click **“Next”**



Activation

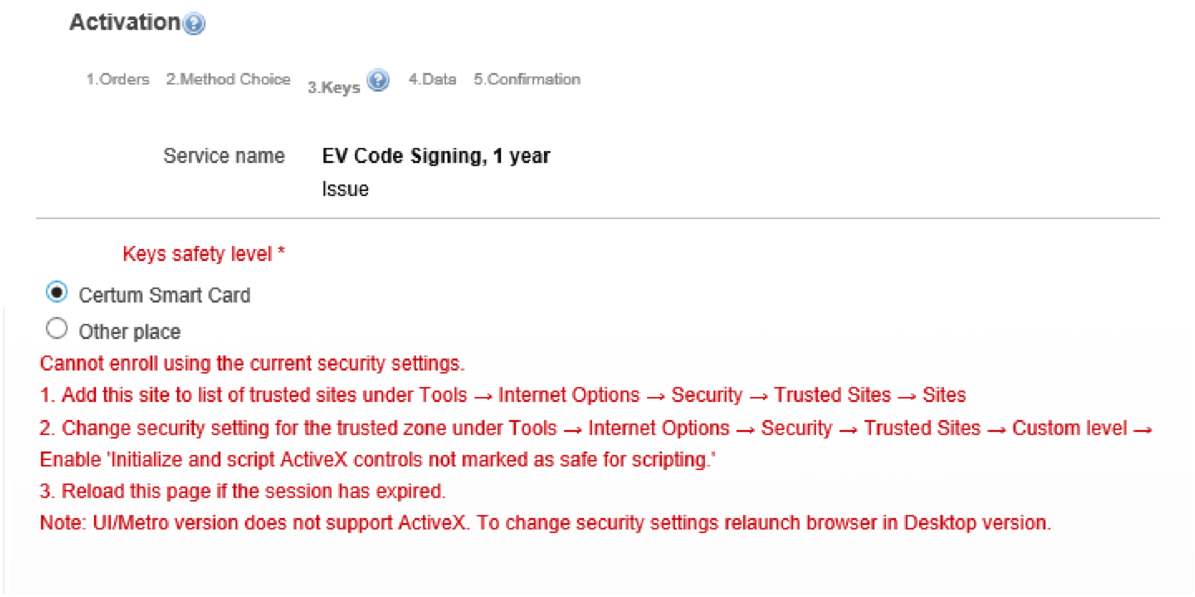
1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name EV Code Signing, 1 year
Issue

Select delivery method of key pair for certificate
● Key pair generation
○ CSR

Additional info about CSR can be found in Help section or can be obtained from infoline consultants.

9. 1. **Procedure for Internet Explorer browser.** Confirm access to www by clicking **“Yes”**



Activation

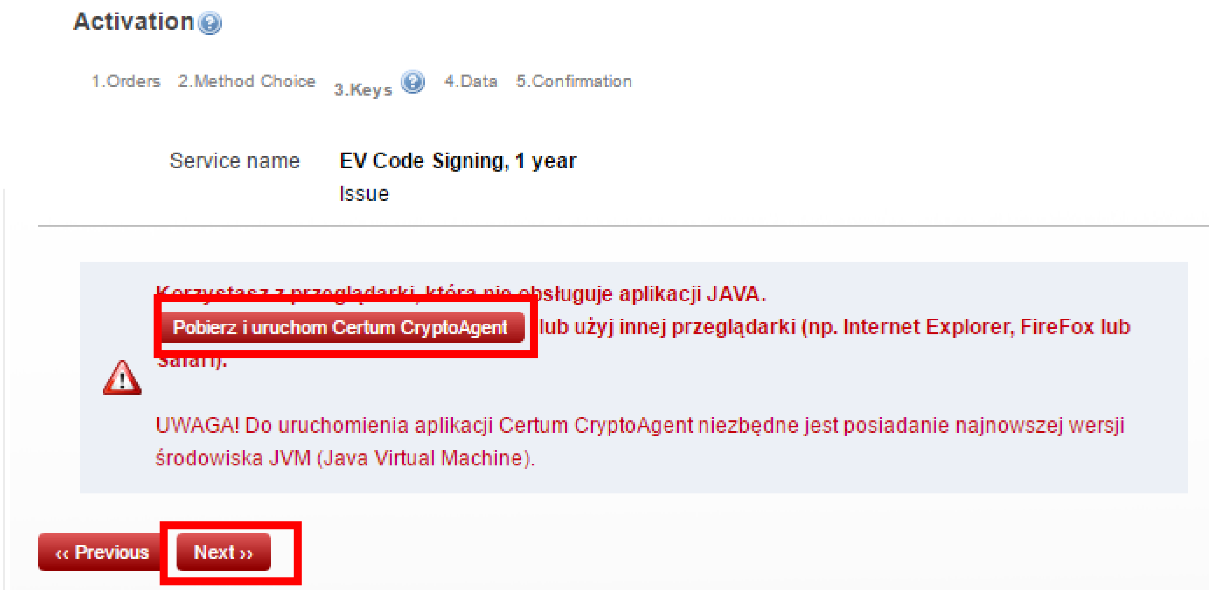
Service name EV Code Signing, 1 year
Issue

Keys safety level *

● Certum Smart Card
○ Other place

Cannot enroll using the current security settings.
1. Add this site to list of trusted sites under Tools → Internet Options → Security → Trusted Sites → Sites
2. Change security setting for the trusted zone under Tools → Internet Options → Security → Trusted Sites → Custom level → Enable 'Initialize and script ActiveX controls not marked as safe for scripting.'
3. Reload this page if the session has expired.
Note: UI/Metro version does not support ActiveX. To change security settings relaunch browser in Desktop version.

9.2. **Procedure for Chrome browser.** Download the CertumCryptoAgent application and keep it running when installing the keys on the card.



Activation

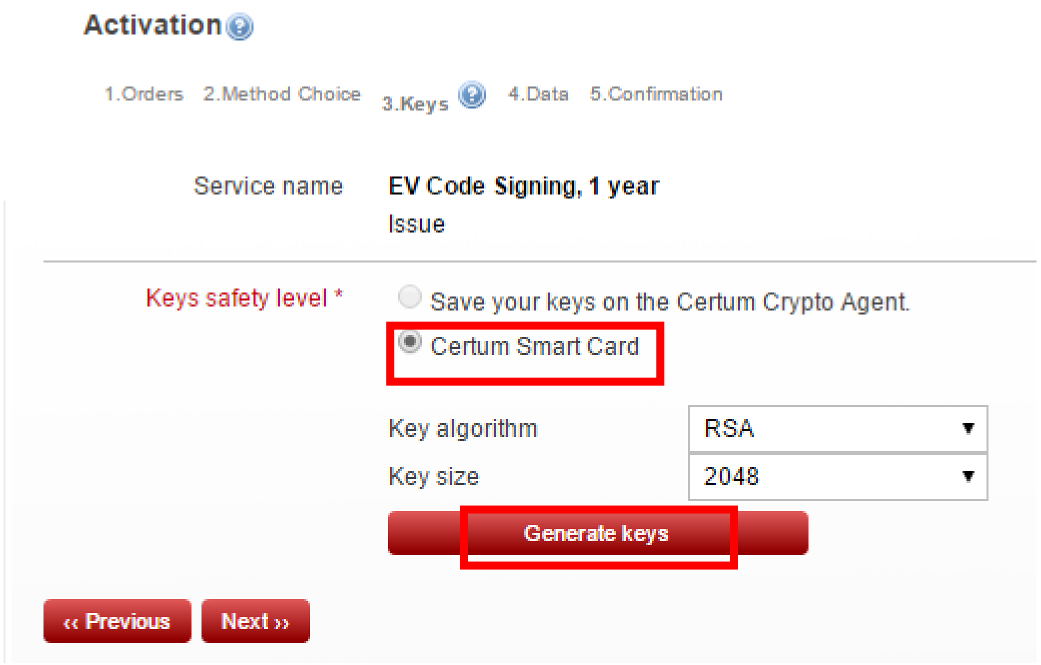
Service name EV Code Signing, 1 year
Issue

Korzystasz z przeglądarki, która nie obsługuje aplikacji JAVA. Pobierz i uruchom Certum CryptoAgent lub użyj innej przeglądarki (np. Internet Explorer, FireFox lub Safari).

UWAGA! Do uruchomienia aplikacji Certum CryptoAgent niezbędne jest posiadanie najnowszej wersji środowiska JVM (Java Virtual Machine).

Keep the CertumCryptoAgent application running when installing the keys on the card. If the application window is closed, the process of installing the keys on the card will be interrupted.

10. Select the **" Certum Smart card"** option and then click **"Generate keys"**. When prompted to provide PIN, enter the card PIN and click "**OK**".

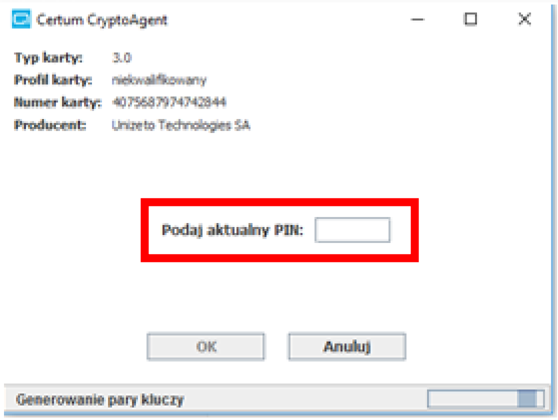


Activation

Service name: **EV Code Signing, 1 year**
Issue

Keys safety level *
○ Save your keys on the Certum Crypto Agent.
● Certum Smart Card

Key algorithm: RSA
Key size: 2048



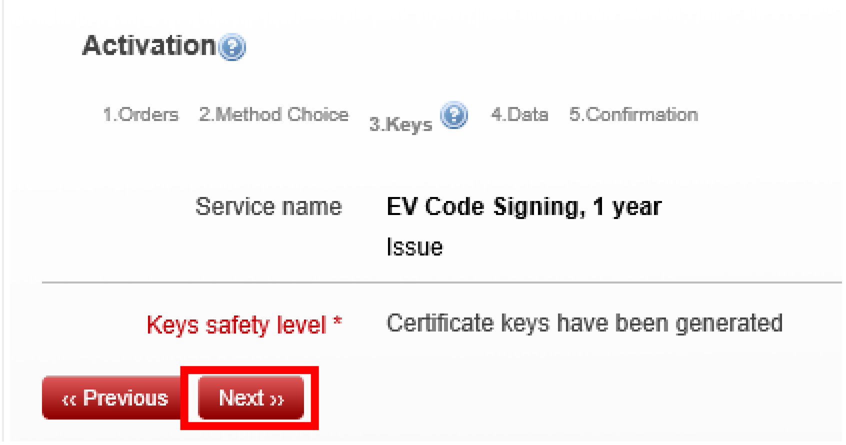
Certum CryptoAgent

Typ karty: 3.0
Profil karty: niekwalifikowany
Numer karty: 4075687974742844
Producent: Unizeto Technologies SA

Podaj aktualny PIN:

Generowanie pary kluczy

11. On the next screen with a message on successful generation of keys on the card click the **"Next"** button.

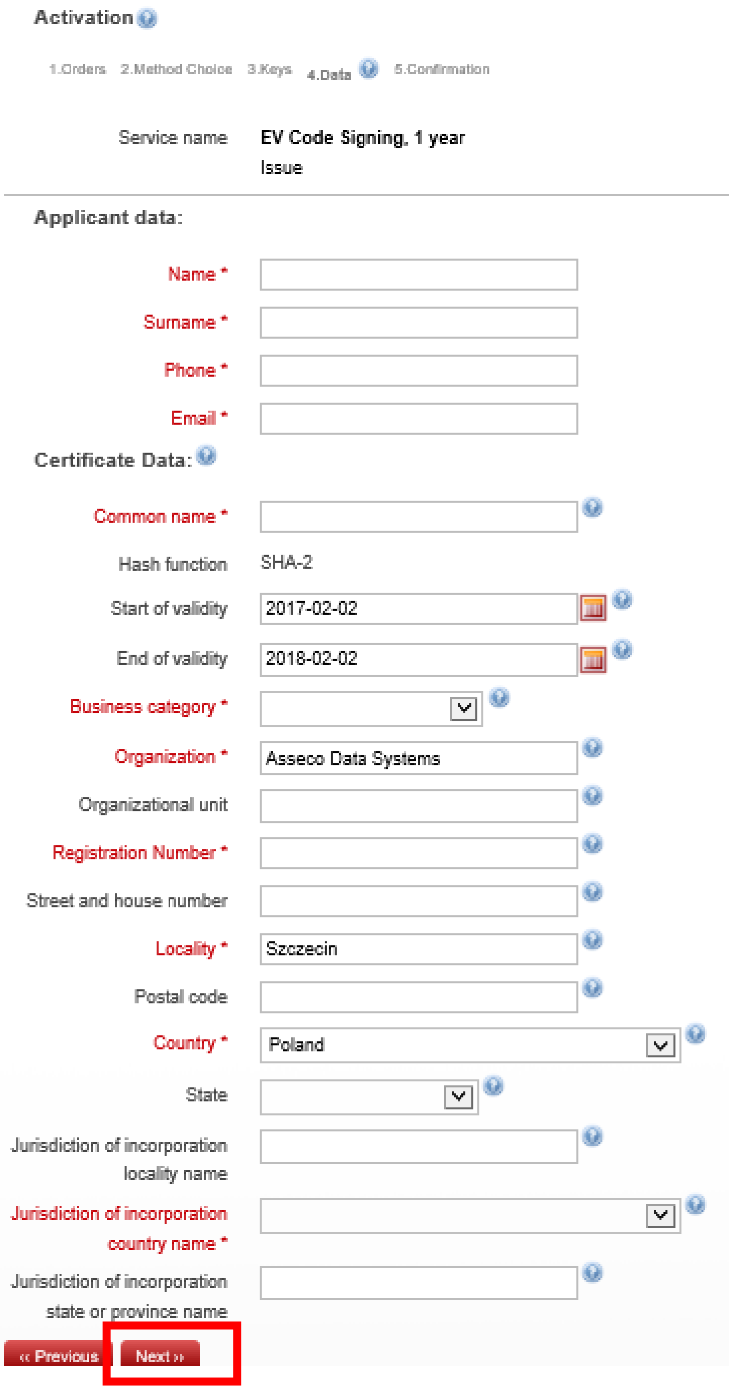


Activation

Service name: **EV Code Signing, 1 year**
Issue

Keys safety level *: Certificate keys have been generated

12. Fill the certification application form with data to be entered in the certificate. Then click **“Next”**



Activation

Service name	EV Code Signing, 1 year Issue

Applicant data:

Name *	
Surname *	
Phone *	
Email *	

Certificate Data:

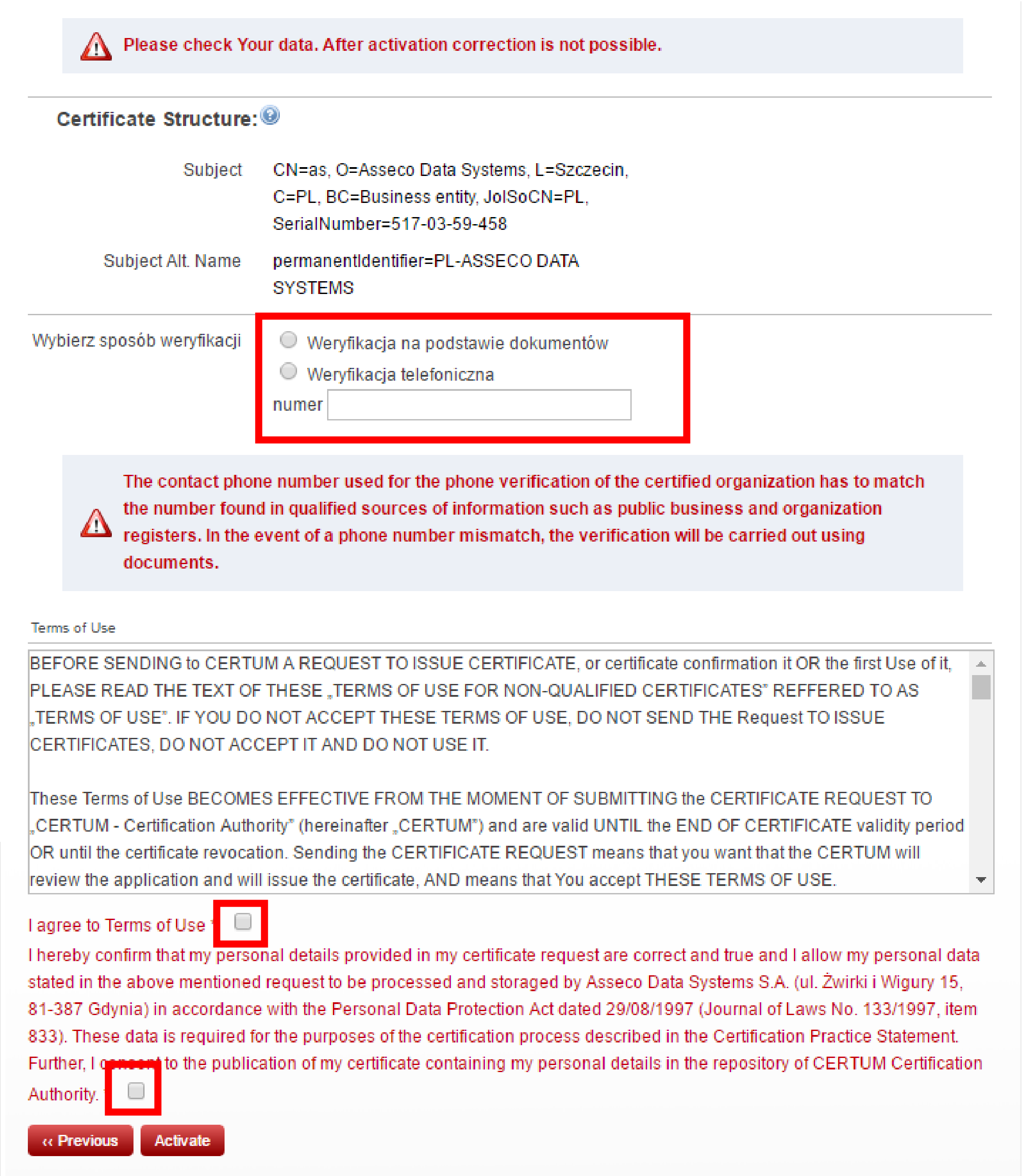
Common name *	
Hash function	SHA-2
Start of validity	2017-02-02
End of validity	2018-02-02
Business category *	
Organization *	Asseco Data Systems
Organizational unit	
Registration Number *	
Street and house number	
Locality *	Szczecin
Postal code	
Country *	Poland
State	
Jurisdiction of incorporation locality name	
Jurisdiction of incorporation country name *	
Jurisdiction of incorporation state or province name	

13. Check again to make sure that the **data** are correct. Select to accept the **Conditions of use** and confirm that the **information provided in the form is true** than click **“Activate”.**

Phone verification

If you select phone verification CERTUM will contact the given phone number within 48 working hours.

The phone number used for the phone verification of the certified organization must be available in public business and organization registers e.g. DUNS, www.yellopages.com, www.numberway.com.



Please check Your data. After activation correction is not possible.

Certificate Structure:

Subject CN=as, O=Asseco Data Systems, L=Szczecin, C=PL, BC=Business entity, JoISoCN=PL, SerialNumber=517-03-59-458

Subject Alt. Name permanentIdentifier=PL-ASSECO DATA SYSTEMS

Wybierz sposób weryfikacji
○ Weryfikacja na podstawie dokumentów
○ Weryfikacja telefoniczna
numer

The contact phone number used for the phone verification of the certified organization has to match the number found in qualified sources of information such as public business and organization registers. In the event of a phone number mismatch, the verification will be carried out using documents.

Terms of Use

BEFORE SENDING to CERTUM A REQUEST TO ISSUE CERTIFICATE, or certificate confirmation it OR the first Use of it, PLEASE READ THE TEXT OF THESE „TERMS OF USE FOR NON-QUALIFIED CERTIFICATES" REFFERED TO AS „TERMS OF USE". IF YOU DO NOT ACCEPT THESE TERMS OF USE, DO NOT SEND THE Request TO ISSUE CERTIFICATES, DO NOT ACCEPT IT AND DO NOT USE IT.

These Terms of Use BECOMES EFFECTIVE FROM THE MOMENT OF SUBMITTING the CERTIFICATE REQUEST TO „CERTUM - Certification Authority" (hereinafter „CERTUM") and are valid UNTIL the END OF CERTIFICATE validity period OR until the certificate revocation. Sending the CERTIFICATE REQUEST means that you want that the CERTUM will review the application and will issue the certificate, AND means that You accept THESE TERMS OF USE.

I agree to Terms of Use □

I hereby confirm that my personal details provided in my certificate request are correct and true and I allow my personal data stated in the above mentioned request to be processed and storaged by Asseco Data Systems S.A. (ul. Żwirki i Wigury 15, 81-387 Gdynia) in accordance with the Personal Data Protection Act dated 29/08/1997 (Journal of Laws No. 133/1997, item 833). These data is required for the purposes of the certification process described in the Certification Practice Statement. Further, I consent to the publication of my certificate containing my personal details in the repository of CERTUM Certification Authority. □

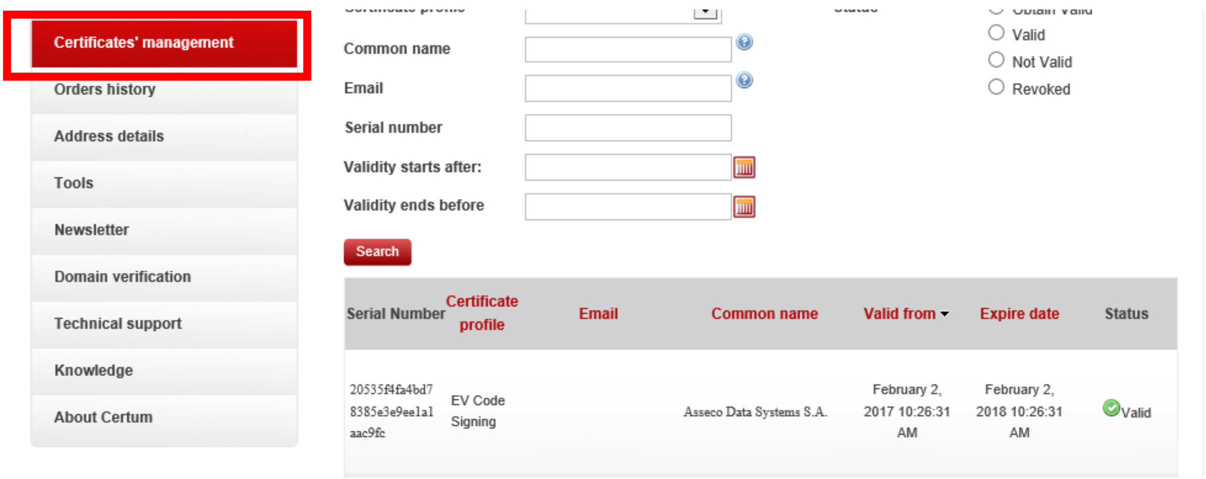
14. The application status should change to **“Realization in progress”**. Further instructions will be sent to the **email address** provided in the certification application form. The list of required documents necessary for identity verification can be found here : **http://certum.eu/certum/cert,expertise_tsupp_cs_requaired.xml**

15. Upon submitting the required documentation to Certum and accepting the certification request a notification will be sent to the **email address** on successfully issued **Code Signing certificate**.

5 Storing the certificate on the card

Upon completion of the entire **activation** process upload the **certificate** to the **card** on which the **keys** were generated (points 10-12), here is how to do it:

1. In Certum Store go to the **“Certificates' management”** tab

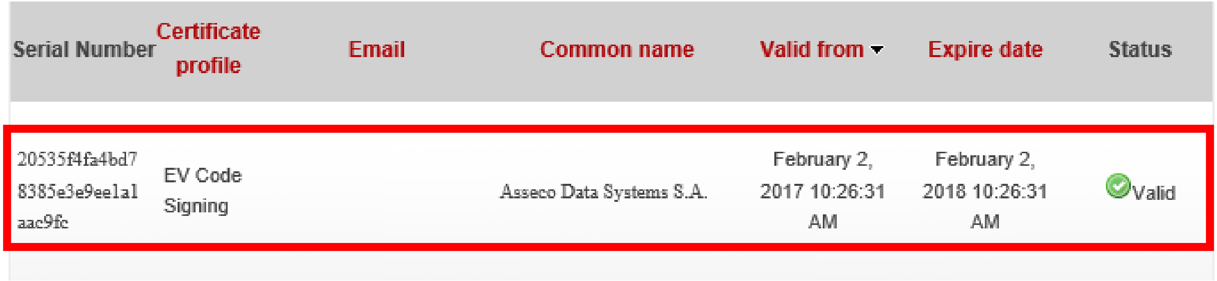


Common name
Email
Serial number
Validity starts after:
Validity ends before

○ Valid
○ Not Valid
○ Revoked

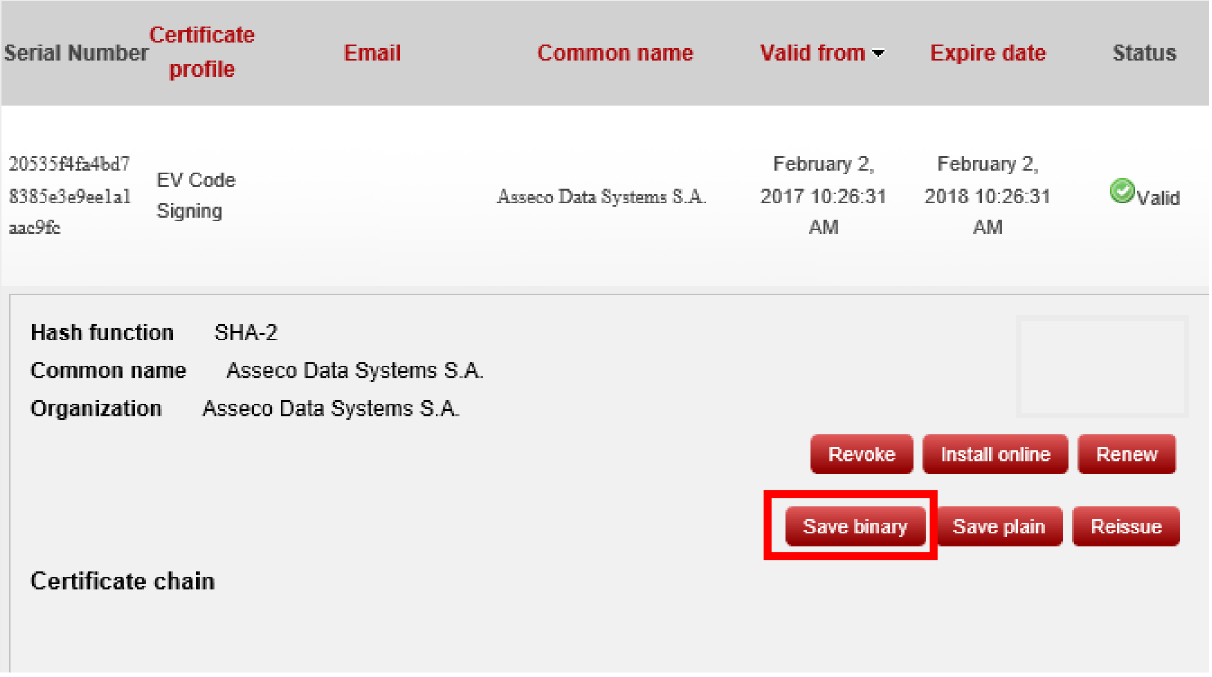
Serial Number	Certificate profile	Email	Common name	Valid from ▾	Expire date	Status
20535f4fa4bd7 8385e3e9ee1a1 aac9fc	EV Code Signing		Asseco Data Systems S.A.	February 2, 2017 10:26:31 AM	February 2, 2018 10:26:31 AM	✓Valid

2. Find the **certificate** for which the **key pair** was generated and click this certificate



Serial Number	Certificate profile	Email	Common name	Valid from ▾	Expire date	Status
20535f4fa4bd7 8385e3e9ee1a1 aac9fc	EV Code Signing		Asseco Data Systems S.A.	February 2, 2017 10:26:31 AM	February 2, 2018 10:26:31 AM	✓Valid

3. Click **“Save binary”**



Serial Number	Certificate profile	Email	Common name	Valid from	Expire date	Status
20535f4fa4bd7 8385e3e9ee1a1 aac9fc	EV Code Signing		Asseco Data Systems S.A.	February 2, 2017 10:26:31 AM	February 2, 2018 10:26:31 AM	✓Valid

Hash function SHA-2

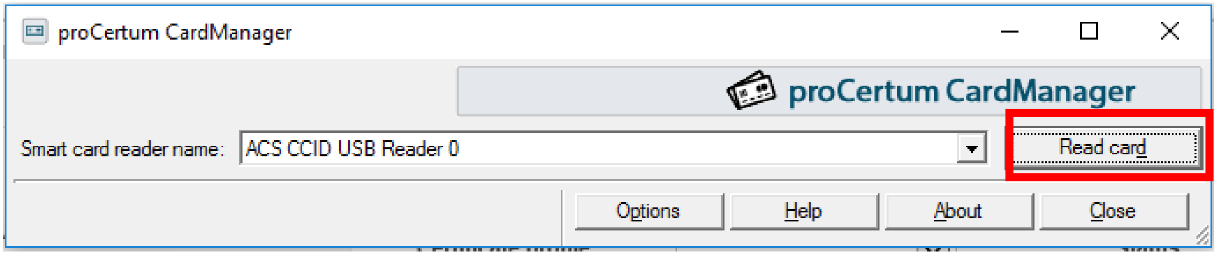
Common name Asseco Data Systems S.A.

Organization Asseco Data Systems S.A.

4. Store the **certificate file** to your computer hard drive.

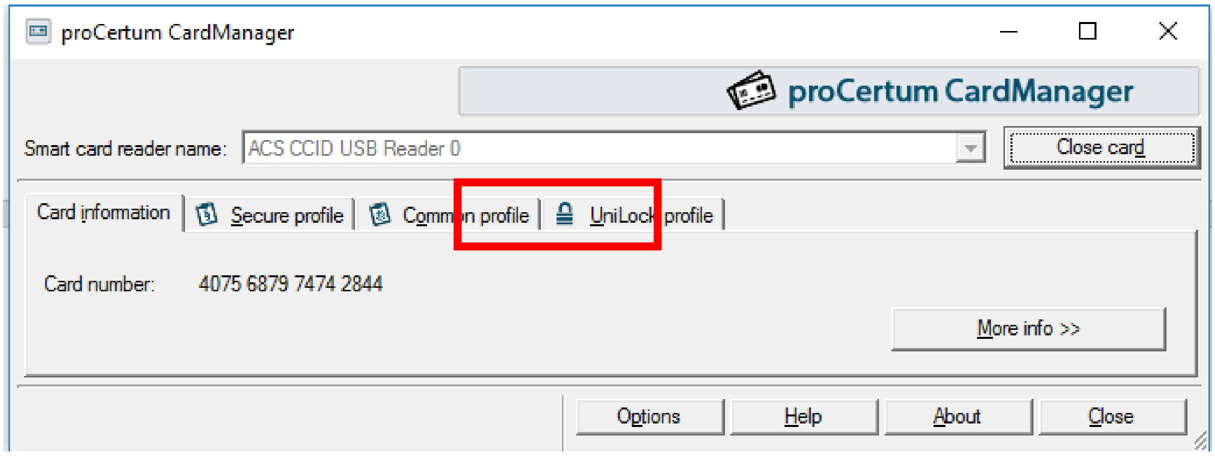
5. Open **proCertum CardManager.**

6. Select the right **reader** (if more readers are configured) and click **“Read card”.**



Smart card reader name: ACS CCID USB Reader 0

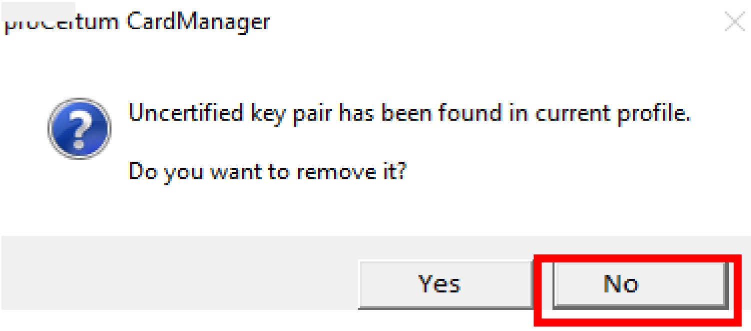
8. Go to the **“Common profile”** tab



Smart card reader name: ACS CCID USB Reader 0

Card number: 4075 6879 7474 2844

9. If the message on **uncertified keys** stored on the card appears on the screen, click **“No”**

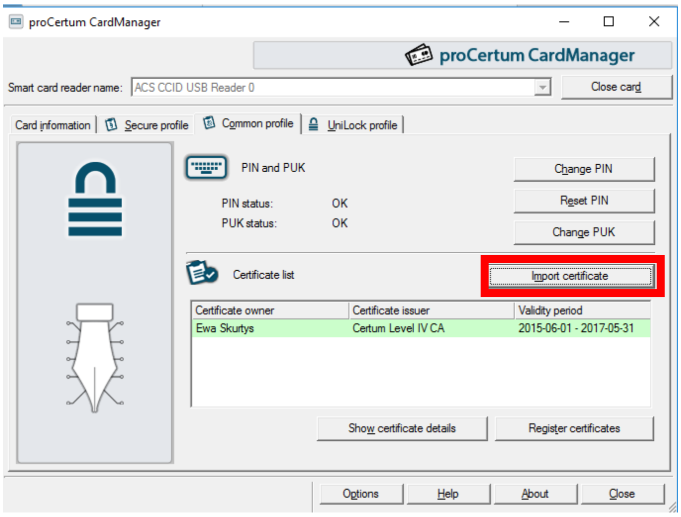


proCertum CardManager

Uncertified key pair has been found in current profile.

Do you want to remove it?

9. Click the **"Import certificate"** button

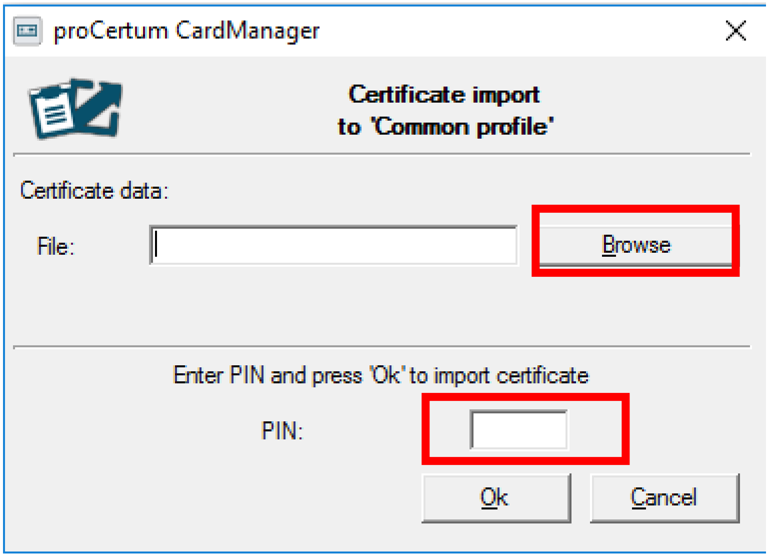


Smart card reader name: ACS CCID USB Reader 0

PIN status: OK
PUK status: OK

Certificate owner	Certificate issuer	Validity period
Ewa Skurtys	Certum Level IV CA	2015-06-01 - 2017-05-31

10. Select the certificate file downloaded previously, enter the card **pin** and click "**OK**"



proCertum CardManager

Certificate import to 'Common profile'

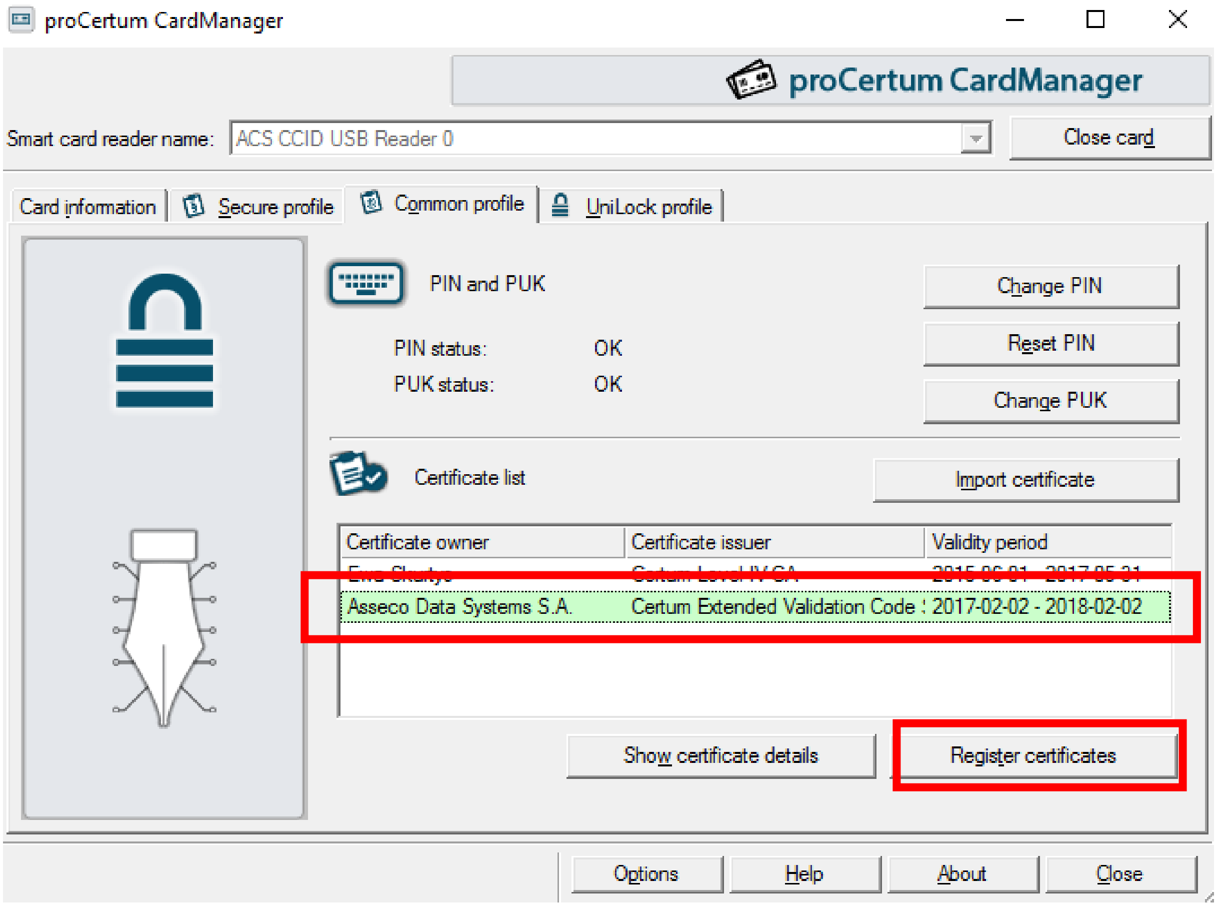
Certificate data:

File:

Enter PIN and press 'Ok' to import certificate

PIN:

11. If the process of adding the **certificate** was completed **successfully**, the **Code Signing** certificate should appear in the list.



proCertum CardManager

Smart card reader name: ACS CCID USB Reader 0

PIN and PUK

PIN status: OK

PUK status: OK

Certificate list

Certificate owner	Certificate issuer	Validity period
Ewa Skutys	Certum Level IV CA	2015-06-01 - 2017-05-31
Asseco Data Systems S.A.	Certum Extended Validation Code :	2017-02-02 - 2018-02-02

12. Register the selected certificate in the operating system. To do so click the "**Register certificates**" button.

6 Signtool

6.1 Tool description

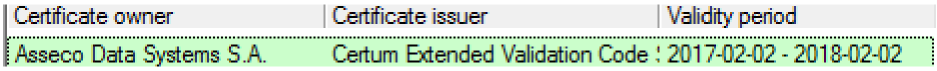
Signtool is a command-line tool for **code signing of files, signature verification in files and date stamping of files.** The tool is available in Windows development kit [(Windows SDK[Software Development Kit]).] All operations with Code Signing require a reader connected with the card on which the Code Signing certificate is stored. Find out more about the tool here: https://msdn.microsoft.com/pl-pl/library/8s9b9yaz(v=vs.110).aspx

6.2 Signing

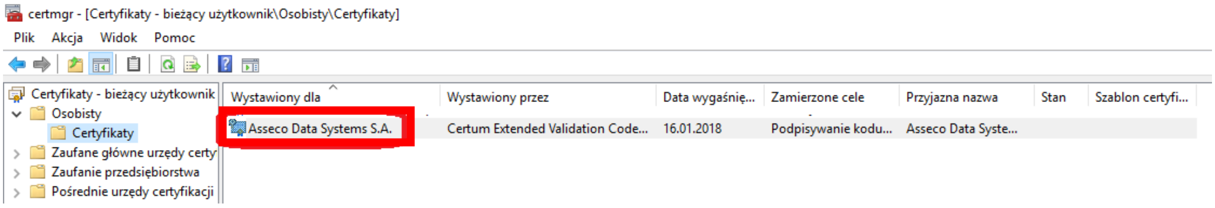
To sign a file use the following command in the command line (cmd.exe):

signtool sign /n "[1] " / t [2] /fd [3] /v [4]

[1] – Name of certificate owner, which can be verified in the proCertum CardManager application or system tool certmgr.msc



Certificate owner	Certificate issuer	Validity period
Asseco Data Systems S.A.	Certum Extended Validation Code ;	2017-02-02 - 2018-02-02



certmgr - [Certyfikaty - bieżący użytkownik\Osobisty\Certyfikaty]

Plik
Akcja
Widok
Pomoc
Certyfikaty - bieżący użytkownik
Osobisty
Certyfikaty
Zaufane główne urzędy certy
Zaufanie przedsiębiorstwa
Pośrednie urzędy certyfikacji

Wystawiony dla	Wystawiony przez	Data wygaśnię...	Zamierzone cele	Przyjazna nazwa	Stan	Szablon certyfi...
Asseco Data Systems S.A.	Certum Extended Validation Code...	16.01.2018	Podpisywanie kodu...	Asseco Data Syste...		

[2] – Time stamp address. For Certum http://time.certum.pl,

[3] – Name of signature algorithm. Available are sha1 and sha256,

[4] – Path for the file being signed.

Here is an example of a correct command:

```
signtool sign /n "Asseco Data Systems S.A." / t http://time.certum.pl/ /fd sha1 /v
file.exe
```

6.3 Verification

To verify the file, use the following command in the command line (cmd.exe):

signtool verify /pa [1]

[1] – Name the file being signed

Here is an example of a correct command:

```
signtool verify /pa file.exe
```

7 Jarsigner

7.1 Tool description

Jarsigner is a command-line tool for **digital signing of files and signature verification.** The tool is available in Oracle development kit (JDK [Java Development Kit]). All operations with Code Signing require a reader connected with the card on which the Code Signing certificate is stored. Find out more about the tool here:
http://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html

7.2 Configuration

An additional configuration is necessary before *jarsigner* can be used. Provider configuration file must be created for PKCS#11. To do this, create new file in *.cfg format (such as for example: provider.cfg). The content of the file is as follows:

```
name=[1]
library=[2]
slot=[3]
```

[1] – Provider's name. Recommended: Crypto3PKCS.
[2] – Path to PKCS library. If the proCertum CardManager application is already installed, the default path is: *C:\Windows\System32\crypto3PKCS.dll*
[3] – Number of the slot with the card in. The default value is -1 which will automatically detect the first available slot.

Here is an example of configuration:

```
name=Crypto3CSP
library=C:\Windows\System32\crypto3PKCS.dll
slot=-1
```

Example of Certum Virtual Card configuration:

```
name=SimplySignPKCS.dll
library=C:\Windows\System32\SimplySignPKCS.dll
slot=-1
```

7.3 Signing

To sign a file use the following command in the command line (cmd.exe):

```
jarsigner -keystore NONE -tsa "[1]" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "[2] " -storepass "[3]" "[4]" "[5]"
```

[1] – Time stamp address. For Certum http://time.certum.pl,
[2] – Path to provider configuration file (“Configuration” section),
[3] – Password for the card,
[4] – Path for the file being signed.
[5] – Name of certificate owner, which can be verified in the proCertum CardManager application.

Here is an example of a correct command:

```
jarsigner -keystore NONE -tsa "http://time.certum.pl" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "provider.cfg" -storepass "123456" "[signed]proCertumJavaApi.jar" "Asseco Data Systems S.A."
```

7.4 Verification

To verify the file, use the following command in the command line (cmd.exe):

```
jarsigner -verify -verbose -keystore NONE -tsa "[1]" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "[2] " -storepass "[3]" "[4]" "[5]"
```

[1] – Time stamp address. For Certum http://time.certum.pl,
[2] – Path to provider configuration file (“Configuration” section),
[3] – Password for the card,
[4] – Path for the file being signed.
[5] – Name of certificate owner, which can be verified in the proCertum CardManager application.

Here is an example of a correct command:

```
jarsigner -verify -verbose -keystore NONE -tsa "http://time.certum.pl" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "provider.cfg" -storepass "123456" "[signed]proCertumJavaApi.jar" "Asseco Data Systems S.A."
```