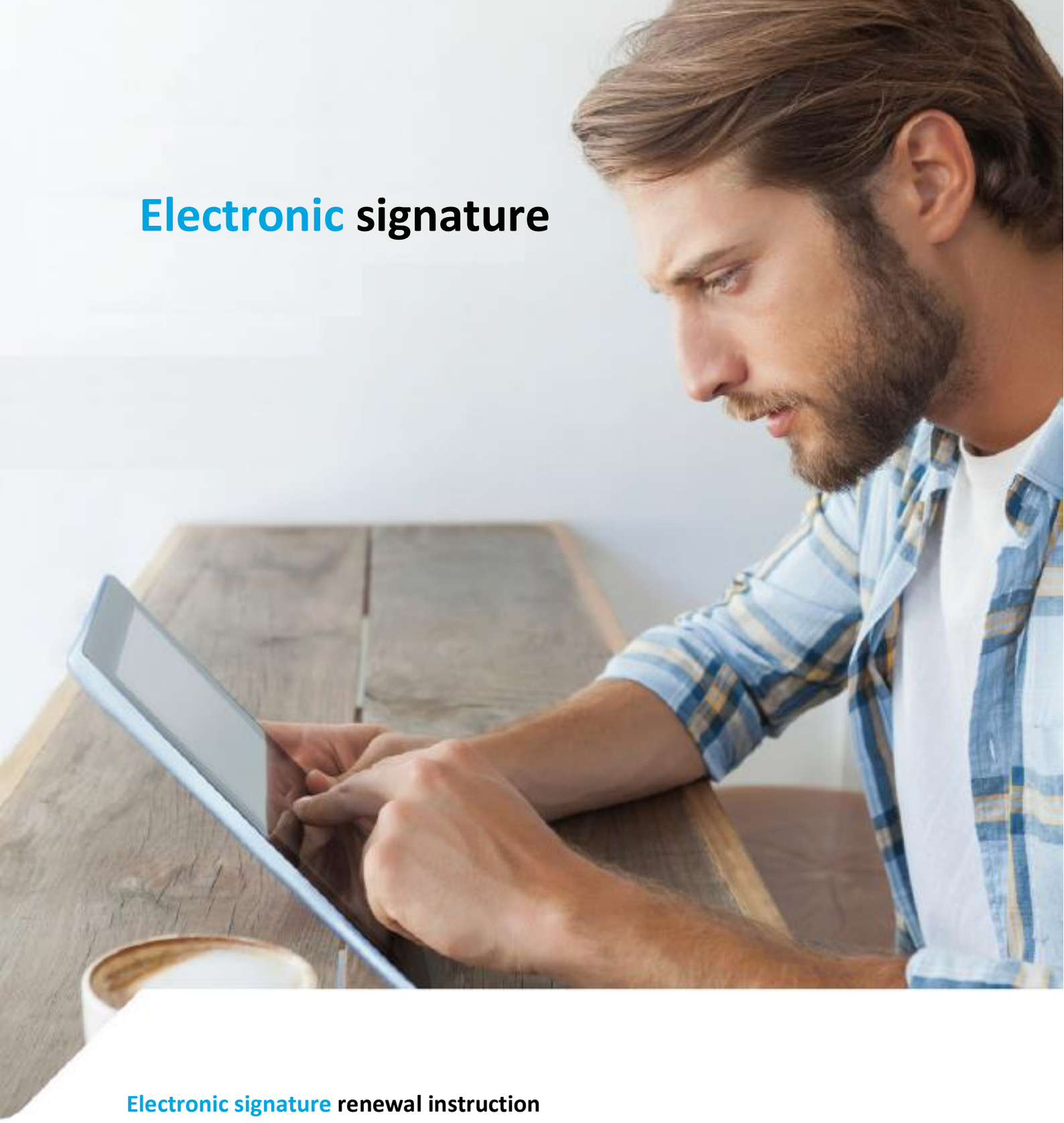


Electronic signature

Electronic signature renewal instruction

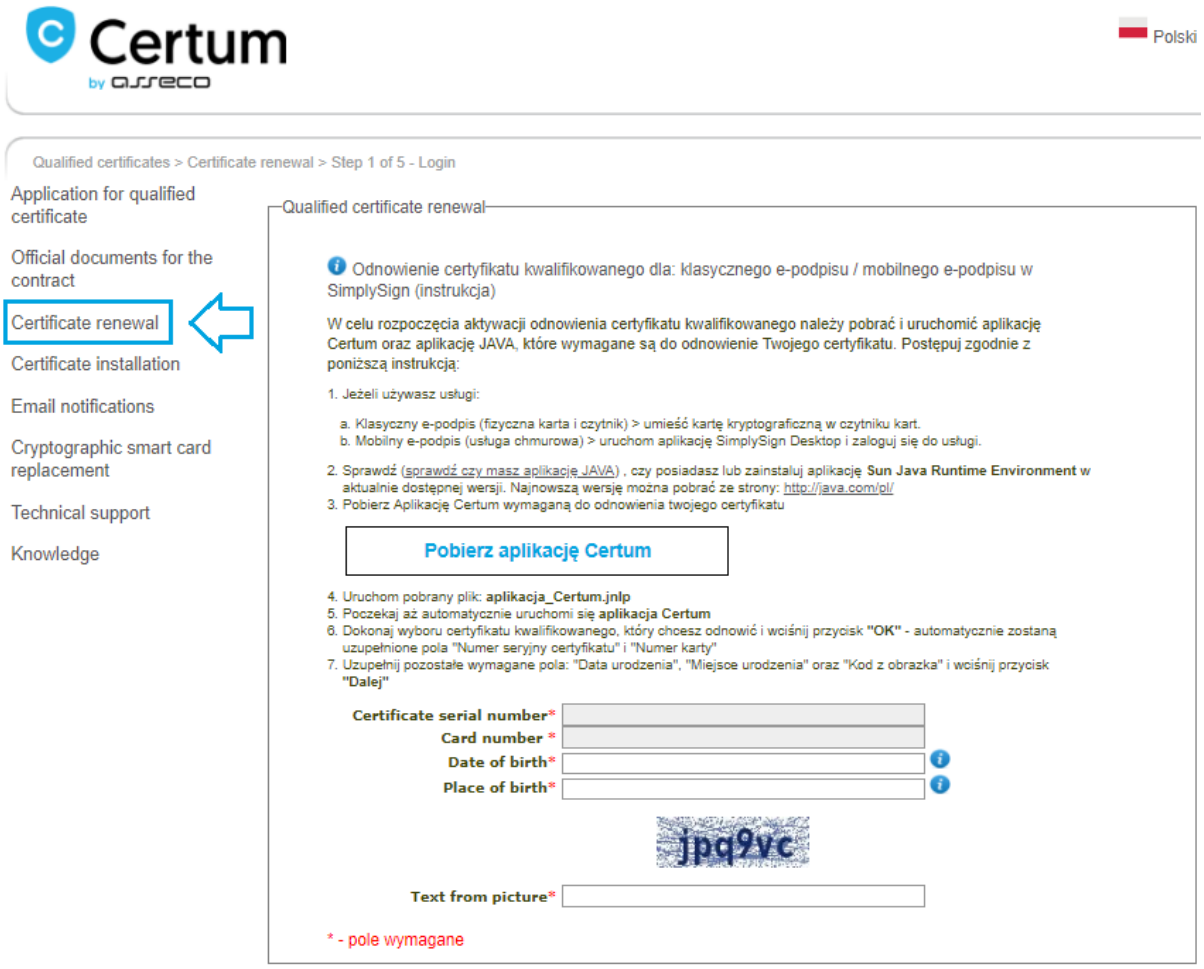
version 1.1

Certum by asseco

Table of Contents

1. Start the renewal process

Please go on website https://status.certum.pl/odnowienia/auth



1. If you use the service:

- **Classic e-signature** (physical card and reader) --> place the cryptographic card in the card reader.
- **Mobile e-signature** (cloud service) --> launch the **SimplySign Desktop** application and log in to the service.

2. Check whether you have or install the **Sun Java Runtime Environment** application in the currently available version. The latest version can be downloaded from: https://www.java.com/en/

3. Download the Certum Application (Pobierz aplikację Certum button) required to renew your certificate.

4. Run the downloaded file: application_Certum.jnlp **.**

5. Wait for the Certum application to start automatically.

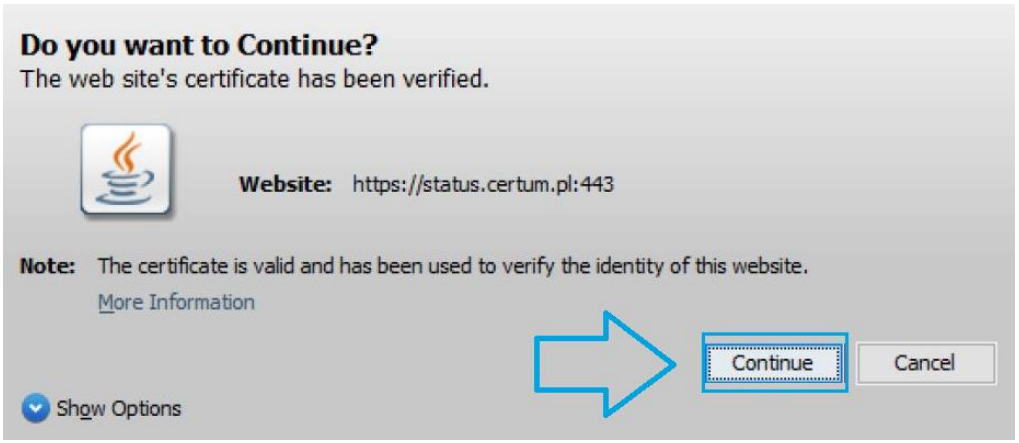
6. Select the qualified certificate you want to renew and press OK - **"Certificate serial number"**

and "**Card number**" fields will be automatically completed.

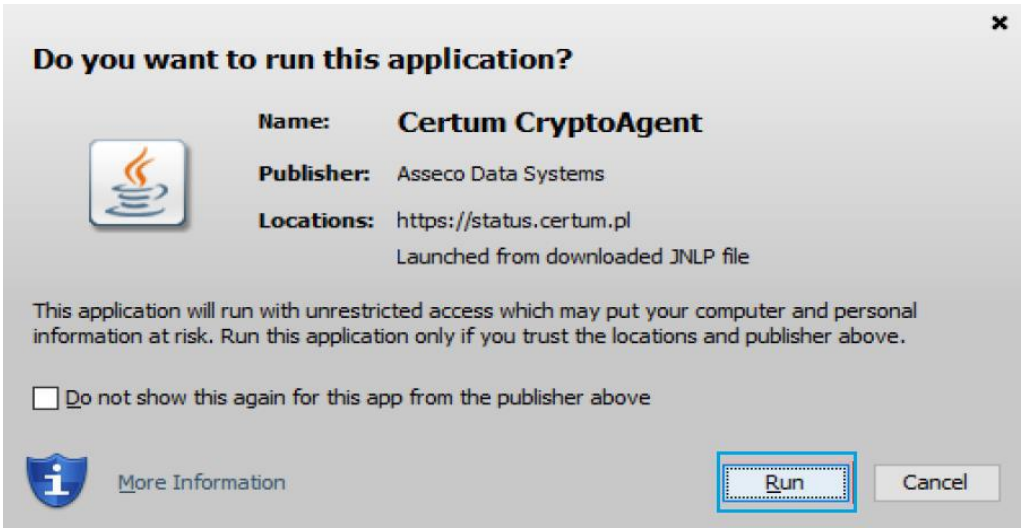
7. Complete the remaining required fields: "**Date of birth**", "**Place of birth**", "**Text from picture**" and press Next.

Starting Certum application - message.

A message appears asking if you want to continue working. Select Continue button:

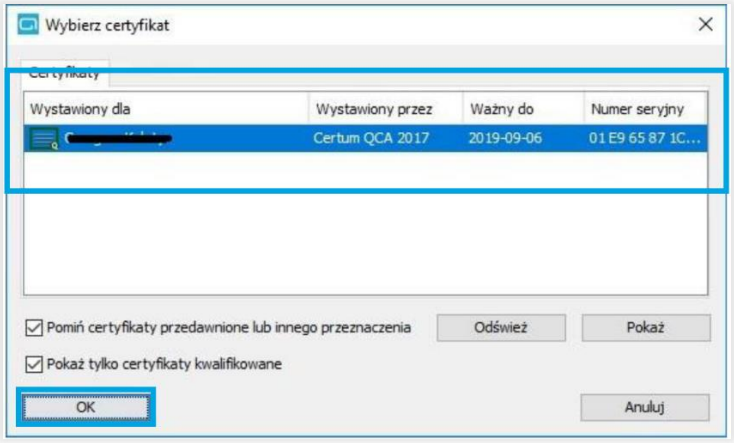


When a similar window pops up, select Run button.



How to choose a certificate?

After a moment a window will appear with a choice of certificate. Choose the one you want to use and press OK. If the window does not appear, refresh the page with the F5 key.



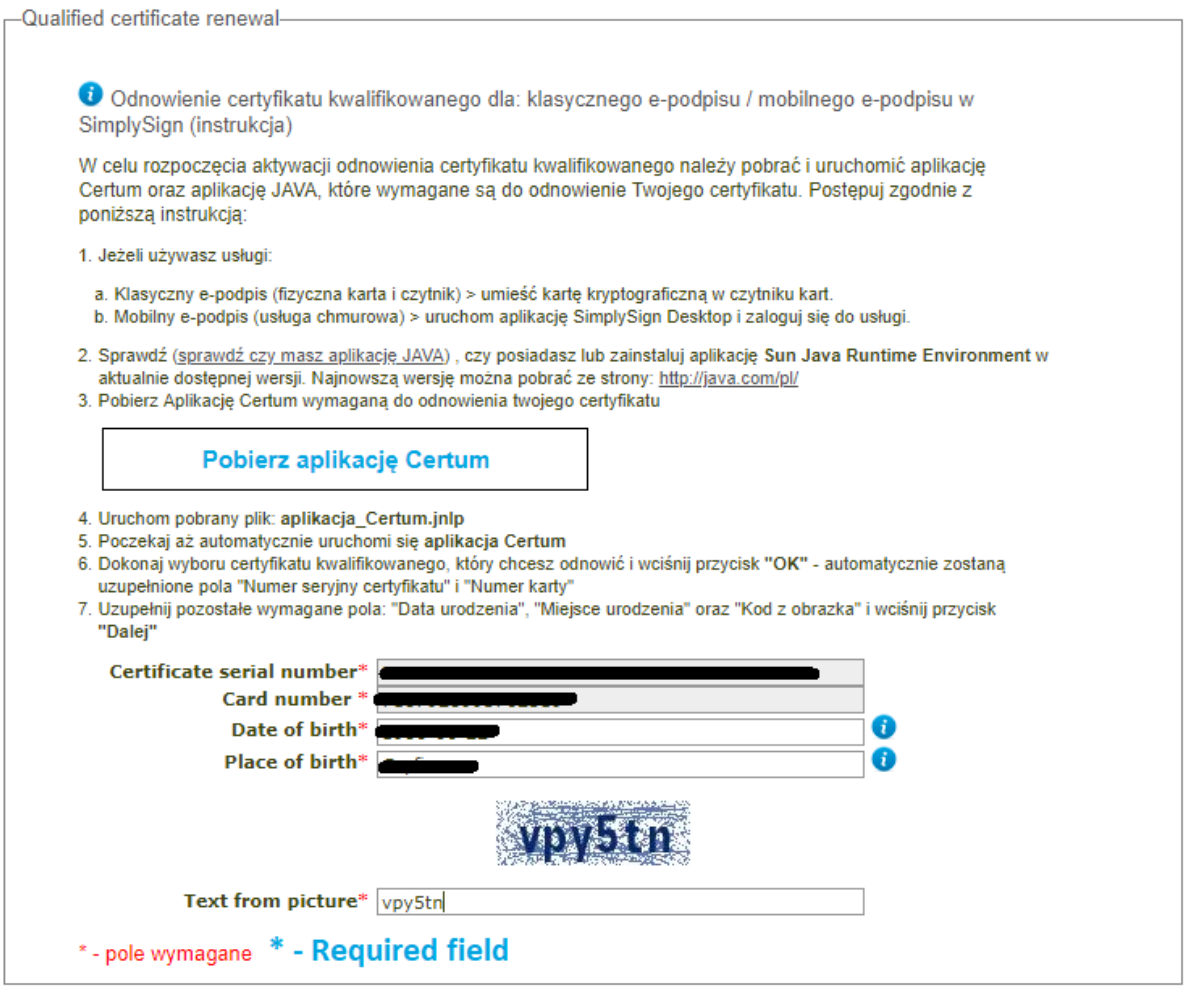
Selecting the certificate will complete the grey fields in the completed form. Fill out the remaining fields as specified in the contract.

If the certificate selection window is empty, make sure that **proCertum Card Manager** is in the current version. The cryptographic card can be removed from the reader and wiped with anti-static material, e.g. a silk tissue handkerchief.

In case if you have a SimplySign (cloud based certificate) please make sure that you are connected to SimplySign Desktop app.

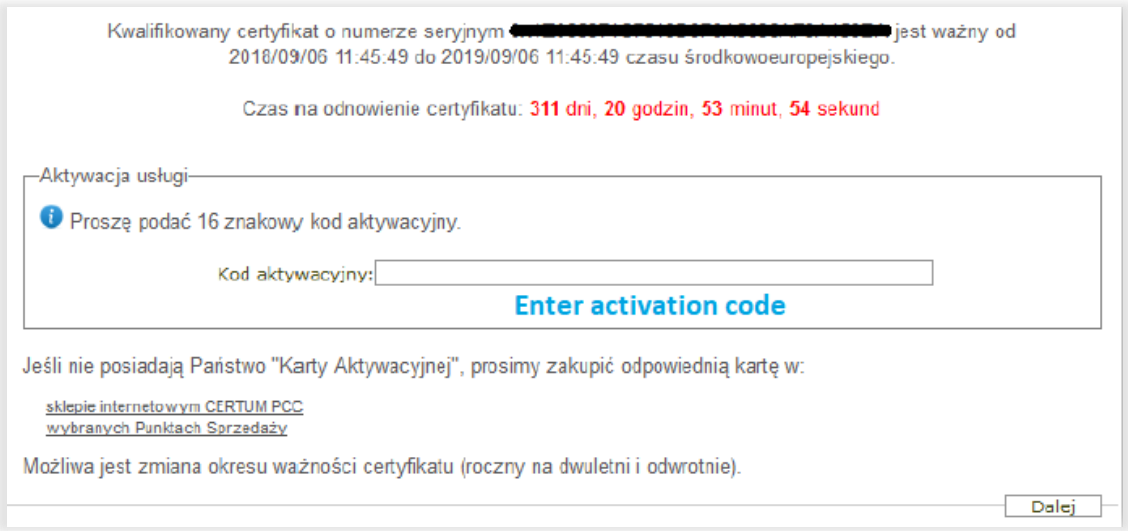
Login to the panel.

After completing the fields, go to rewriting the code from the picture. Read the information and select the button at the bottom Next**.**



2. Activation Code

At this stage, enter the activation code and click Dalej (Next):



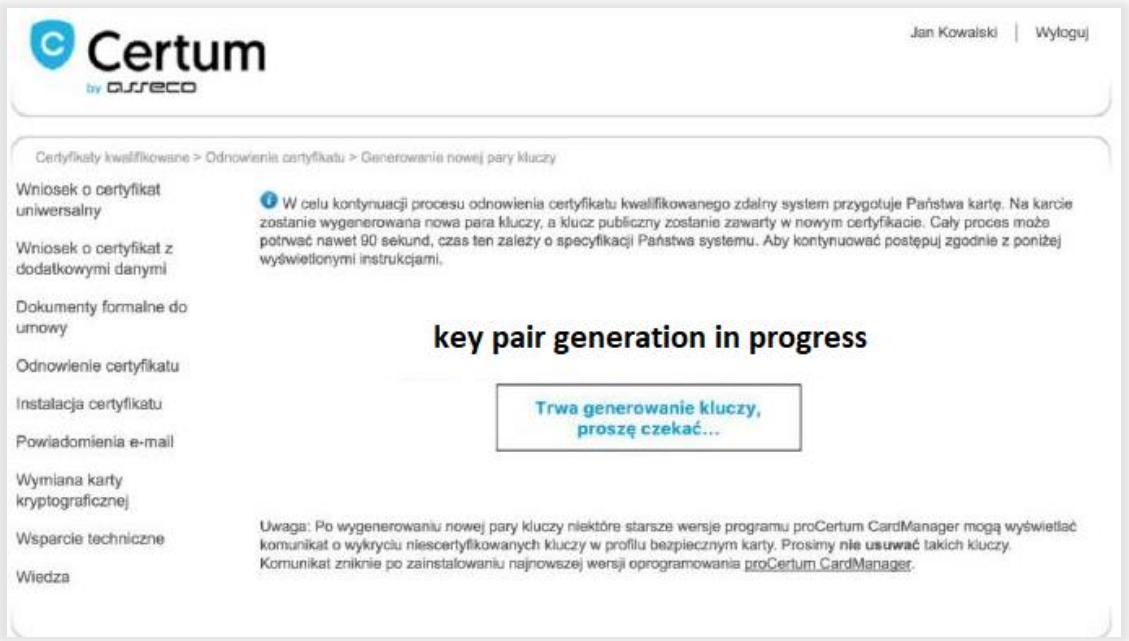
3. Generating a new key pair

When the "Generate new key pair" window appears, go to the Wygeneruj nową parę kluczy (Generate a new key pair) option.

!	**IMPORTANT** – If you not see the stage of generating a key pair and the site has moved you to complete the form, it means that the key pair is already on the card and you can go ahead with the renewal process.

Do not remove the card from the reader and patiently wait up to 90 seconds for a new pair of keys to be generated.
At this stage, the system will ask you for the PIN. Remember that this is the PIN code for the secure profile.

Wait a moment until the keys are generated.



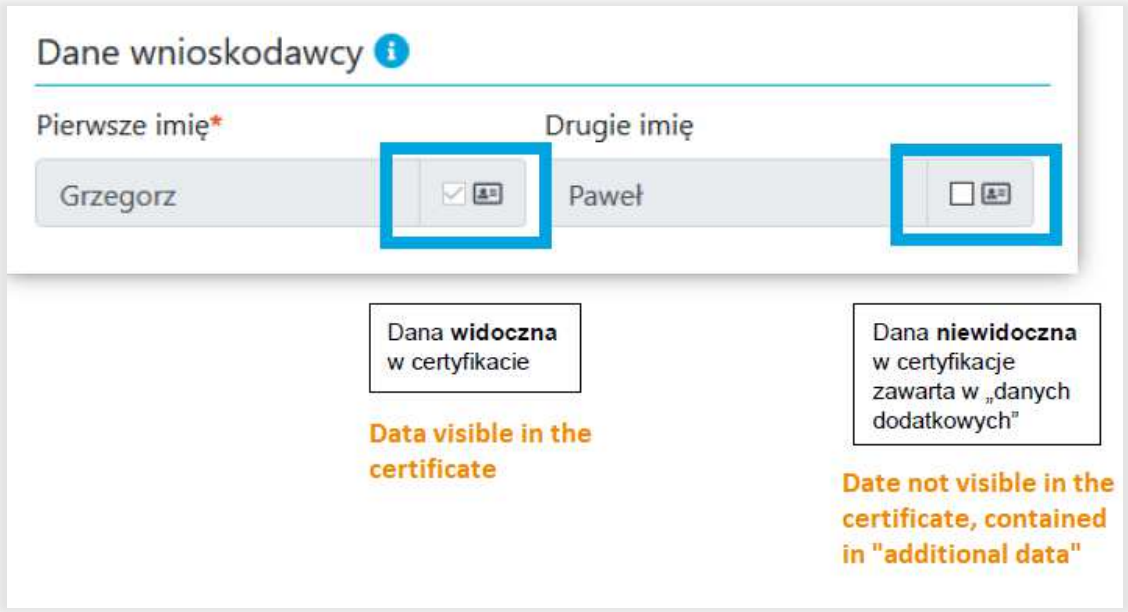
If the PIN code was entered correctly, the application will go to the key pair generation process.
If the page does not move you automatically, press Dalej (Next).

4. Data in the certificate

When filling out the form, remember to update the information. **Check carefully - not all of them have been filled in automatically, e.g. field ID document.**

Remember to check if your current email address is valid. Information will be sent to your email address with instructions on how to upload the certificate onto the card - the last stage of renewal after signing the annex.

Personal details visible in the certificate and additional identification data are marked as below:



5. Signing the annex to the agreement

In the next step You will have **Annex to the agreement**.

Aneks nr [redacted] **do**
Umowy z Subskrybentem
nr [redacted]
o świadczenie kwalifikowanych usług zaufania
zawarty w [redacted] roku

pomiędzy Stronami:

Asseco Data Systems S.A. z siedzibą w Gdyni, przy ul. Podolskiej 21, korespondencja: ul. Bajeczna 13, 71-838 Szczecin wpisaną do rejestru sądowego prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, numer KRS 0000421310 oraz do rejestru dostawców usług zaufania, numer NIP: 5170359458, kapitał zakładowy (wpłacony w całości): 120 002 940 zł, reprezentowaną zgodnie z zasadami ujawnionymi w Krajowym Rejestrze Sądowym albo przez upoważnionego pełnomocnika, zwaną dalej "Asseco Data Systems", a

[redacted] **First name and last name**
IMIĘ I NAZWISKO

[redacted] **Date and place of birth**
DATA I MIEJSCE URODZENIA

[redacted] **Identifier (e.g. passport, PESEL ID number)**
NUMER PESEL

[redacted]
SERIA I NUMER, RODZAJ, ORGAN WYDAJĄCY ORAZ DATA WAŻNOŚCI DOKUMENTU TOŻSAMOŚCI

Data regarding the identity document

zwaną dalej "Subskrybentem", o następującej treści:

§1 PRZEDMIOT UMOWY

Przedmiotem niniejszego Aneksu jest rozszerzenie zakresu zawartej pomiędzy Stronami Umowy o świadczenie usług zaufania w zakresie wydawania i unieważniania certyfikatu oraz świadczenie usług zaufania zgodnie z warunkami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym eIDAS, w Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016 poz.1579) oraz w wykazie danych rejestracyjnych.
Rozszerzenie zakresu Umowy polega na przedłużeniu okresu świadczenia usług zaufania na kolejny okres ważności certyfikatów wydanych na jej podstawie. Wydanie certyfikatu odbędzie się na karcie kryptograficznej o numerze 4938164593148857 stanowiącej komponent techniczny, zawierający klucze kryptograficzne, które podlegają wyłącznej kontroli Subskrybenta. Dane zawarte w certyfikacie nie ulegną zmianie poza nowym numerem seryjnym certyfikatu, nowym okresem jego ważności oraz podpisem Certum.
Poprzez podpisanie niniejszego Aneksu Subskrybent wyraża zgodę na umieszczenie w certyfikacie danych służących do weryfikacji podpisu elektronicznego wymienionych w załączniku, które to dane zostaną zawarte w certyfikacie Subskrybenta oraz na stosowanie tych danych do weryfikacji jego podpisu elektronicznego.
Wygenerowany certyfikat będzie wydany na kolejną parę kluczy, na okres jednego roku .
Wygenerowany certyfikat będzie zawierał jeden z wymienionych kluczy publicznych:
4EF2041E196897EB4FAB4901ADC1CD72EF2C0D84
9DEF970F2FF17C450ECC3E3F0899D88FBDEA73E6
98144B58606B319CE96EB3348E5313D893A17BDD
Gwarantowany przez Asseco Data Systems czas obsługi w zakresie unieważniania certyfikatu na każde złożone przez Subskrybenta żądanie jest określonym w aktualnie obowiązującej na dzień złożenia wniosku o unieważnienie Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.

§2 OBOWIĄZYWANIE UMOWY

Aneks wchodzi w życie z dniem podpisania i obowiązuje do czasu wygaśnięcia terminu ważności certyfikatów będących przedmiotem niniejszego Aneksu do umowy o świadczenie usług zaufania.

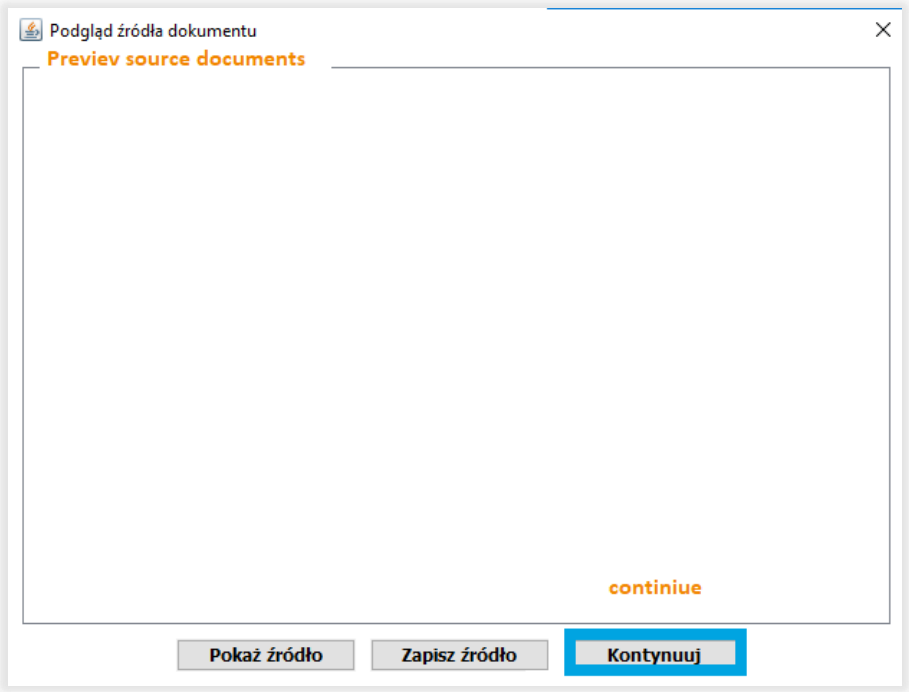
§4 POSTANOWIENIA KONCOWE

Aneks został sporządzony w formie elektronicznej i jest podpisany certyfikatem kwalifikowanym.
Zmiany niniejszego Aneksu wymagają formy pisemnej lub jej równoważnej pod rygorem nieważności.

Data regarding the identity document: **Serial number, type of the document, Organisation that issued the document**

To sign the annex click on Przejdź do podpisania aneksu (Go to sign the annex).
Select your certificate and press OK.

Next step:



The application process is completed with information:

Dziękujemy!

Proces składania wniosku o odnowienie certyfikatu kwalifikowanego został zakończony.

Najpóźniej w ciągu 7 dni roboczych od momentu wpłynięcia poprawnie podpisanych elektronicznie dokumentów do Certum, zostanie wydany odnowiony certyfikat kwalifikowany, który będzie można pobrać drogą elektroniczną na posiadaną kartę kryptograficzną. Informacja o wydaniu certyfikatu kwalifikowanego oraz instrukcja dalszego postępowania zostanie przekazana drogą elektroniczną.
W wiadomości zawarty będzie także adres, przez który będzie możliwość pobrania podpisanego obustronnie Aneksu do Umowy z Subskrybentem.

Thank you!

The aplication process for the renewal of the qualified certificate has been complited.

At the latest within 7 business days of the receipt of correctly electronically signed documents to Certum, a renewed qualified certificate will be issued, which can be downloaded electronically to your cryptographic card. Information on the issue of a qualified certificate and instructions on how to proceed will be sent electronically. The message will also include the address through which it will be possible to download the Annex signed by both parties to the Agreement with Subscriber.

An e-mail with information about issuing the certificate will contain a link to instructions on how to upload the certificate to the card - this is the last, third stage.
The certificate saved on the card enables its use.