



# INSTRUKCJA UŻYTKOWNIKA

Instrukcja dot. ścieżki odnowień  
certyfikatów kwalifikowanych

wersja 1.4

# Spis treści

WSTĘP.....	3
KROK 1 - ZAKUP ODNOWIENIA CERTYFIKATU .....	4
1.1 E-mail do użytkownika.....	4
1.2 Przygotowanie do odnowienia .....	5
KROK 2 - AKTYWACJA ODNOWIENIA CERTYFIKATU KWALIFIKOWANEGO .....	5
2.1 ETAP 1 Z 5 - LOGOWANIE.....	5
2.2 ETAP 1 Z 5 – GENEROWANIE NOWEJ PARY KLUCZY .....	8
2.3 ETAP 2 Z 5 – AKTYWACJA USŁUGI.....	9
2.4 ETAP 3 Z 5 – WERYFIKACJA DANYCH SUBSKRYBENTA.....	9
2.5 ETAP 4 Z 5 – PREZENTACJA ANEKSU DO UMOWY Z SUBSKRYBENTEM.....	16
2.6 ETAP 5 Z 5 – PODPISYWANIE ANEKSU.....	19
KROK 3 - POBRANIE ODNOWIONEGO CERTYFIKATU NA KARTĘ KRYPTOGRAFICZNĄ.....	21
3.1 Automatyczna instalacja certyfikatu kwalifikowanego.....	26
3.2 Zaawansowana instalacja certyfikatu kwalifikowanego .....	30

## WSTĘP

Certyfikat kwalifikowany służy do podpisu elektronicznego i w świetle [Ustawy o podpisie elektronicznym](#), jest równoważny podpisowi własnoręcznemu. Gdy kończy się okres ważności, certyfikat kwalifikowany należy odnowić.

Odnowienie można zrealizować w 3 krokach:

1. Zakup odnowienia certyfikatu.
2. Aktywacja odnowienia certyfikatu kwalifikowanego,
3. Pobranie odnowionego certyfikatu na kartę kryptograficzną.

Poniższa instrukcja dotyczy opisu 2 oraz 3 kroku odnawiania certyfikatu kwalifikowanego.

Odnowienie certyfikatu kwalifikowanego możliwe jest przy wykorzystaniu przeglądarek:

- Internet Explorer w wersji 6 lub wyższej,
- Mozilla FireFox w wersji 2.5 lub wyższej.

Proces odnowienia certyfikatu kwalifikowanego wymaga zainstalowanego środowiska **Sun Java Runtime Environment** (w wersji 1.6.0\_10 lub nowszej). Można je pobrać ze strony - <http://java.com/pl/>

### UWAGA!

Poniższa instrukcja opisuje proces odnowienia jedynie tych certyfikatów kwalifikowanych, które jeszcze nie wygasły.

### UWAGA!

**Nie usuwaj certyfikatu kwalifikowanego przed jego odnowieniem.**

**W trakcie zapisywania nowego certyfikatu kwalifikowanego na kartę kryptograficzną, stary certyfikat zostanie automatycznie podmieniony na nowy bez twojej ingerencji. W przypadku modyfikacji danych w certyfikacie zostanie wydany certyfikat na nową parę kluczy, a poprzedni (odnawiany) zostanie unieważniony.**

*Oprogramowanie zarządzające proCertum CardManager, zgodnie z Ustawą o podpisie elektronicznym z 18 września 2001r., umożliwia usunięcie z karty kryptograficznej certyfikatu kwalifikowanego wraz z przypisanymi do niego kluczami kryptograficznymi. **Operacja ta jest nieodwracalna.** Brak kluczy kryptograficznych na karcie uniemożliwia odnowienie certyfikatu kwalifikowanego i skutkuje koniecznością zakupu nowego certyfikatu kwalifikowanego lub nowej karty kryptograficznej.*

## KROK 1 - ZAKUP ODNOWIENIA CERTYFIKATU

### 1.1 E-mail do użytkownika

#### **UWAGA!**

**Odnówić można tylko te certyfikaty kwalifikowane, które są jeszcze ważne.**

Na 60, 30, 14 oraz 7 dni przed utratą ważności certyfikatu, otrzymają Państwo wiadomość e-mail od CERTUM PCC o zbliżającej się dacie wygaśnięcia certyfikatu kwalifikowanego. Poniżej znajduje się przykładowy mail:

Szanowny Kliencie,

CERTUM - Powszechne Centrum Certyfikacji informuje, że w ciągu **XXXX** dni, **RRRR-MM-DD HH:MM:SS** dobiega końca okres ważności certyfikatu kwalifikowanego o numerze seryjnym **XXXXXX** wydanego dla "NAZWISKO IMIE".

W celu przedłużenia ważności ww. certyfikatu kwalifikowanego zapraszamy do jego odnowienia w CERTUM PCC za pośrednictwem:

- przedstawiciela CERTUM PCC, u którego dokonano zakupu ww. certyfikatu,
- serwisu internetowego CERTUM PCC  
[http://www.certum.pl/certum/cert,oferta\\_odnowienie\\_certyfikatu\\_zestawy.xml](http://www.certum.pl/certum/cert,oferta_odnowienie_certyfikatu_zestawy.xml)
- dowolnego Punktu Rejestracji / Punktu Partnerskiego reprezentującego CERTUM PCC

wykaz wszystkich punktów obsługi znajduje się na stronie  
[http://www.certum.pl/certum/cert,kontakt\\_punkty\\_rejestracji.xml](http://www.certum.pl/certum/cert,kontakt_punkty_rejestracji.xml)

#### **UWAGA!**

Koszt odnowienia jest znacznie niższy od zakupu nowego certyfikatu kwalifikowanego. Co ważne, usługa odnowienia nie ma zastosowania dla certyfikatów, których ważność już wygasła lub zostały unieważnione. W związku z powyższym proces odnowienia certyfikatu kwalifikowanego najlepiej rozpocząć co najmniej 14 dni przed upływem terminu jego ważności.

W przypadku jakichkolwiek pytań prosimy o kontakt z operatorem naszej infolinii:

- e-mail: [infolinia@unizeto.pl](mailto:infolinia@unizeto.pl)
- nr tel.: 0 71 801 540 340 (czynna 24h na dobę),  
dla telefonów komórkowych +48 (0) 91 4801 340

Z poważaniem,  
Zespół CERTUM PCC

## 1.2 Przygotowanie do odnowienia

Przed przystąpieniem do procedury odnowienia drogą elektroniczną, zainstaluj i podłącz czytnik kart. Włóż do czytnika kartę kryptograficzną z certyfikatem kwalifikowanym, który chcesz odnowić.

W celu odnowienia certyfikatu drogą elektroniczną, udaj się na stronę [www.certum.pl](http://www.certum.pl).

Z górnego menu wybierz zakładkę Obsługa certyfikatów > Odnawianie podpisu elektronicznego

Następnie przechodzimy do kroku 2 – Aktywacja odnowienia.

**Odnowienie podpisu elektronicznego (certyfikatu kwalifikowanego)**

Odnowienie podpisu elektronicznego (certyfikatu kwalifikowanego) przedłuża okres jego ważności o kolejny **1 rok** lub **2 lata**.

**UWAGA:** Zaleca się by odnowienie rozpocząć przynajmniej 14 dni przed upływem terminu ważności certyfikatu. Pozwoli to uniknąć dodatkowych kosztów związanych z wydaniem nowego certyfikatu kwalifikowanego.

Odnów podpis elektroniczny

- **Podpis elektroniczny zakupiony w CERTUM PCC** ([sprawdź logo wystawcy na karcie](#)) możesz odnowić samodzielnie online lub korzystając z pomocy naszego Partnera.
- **Podpis elektroniczny zakupiony u innego wystawcy** odnowisz u naszego Partnera.

Odnów online

Odnów u Partnera

**Chcesz dowiedzieć się więcej?**

[Najczęściej zadawane pytania](#)

[Procedura odnowień](#)

**Przejdź do:**

[Krok 2 - Aktywacja odnowienia](#)

[Krok 3 - Pobranie certyfikatu](#)

**Skorzystaj z pomocy naszego Partnera**

## KROK 2 - AKTYWACJA ODNOWIENIA CERTYFIKATU KWALIFIKOWANEGO

### 2.1 Etap 1 z 5 - Logowanie

- Po przekierowaniu do elektronicznego formularza odnowień (<https://status.certum.pl/odnowienia>), postępuj zgodnie z instrukcją.  
Rozpocznij od **kroku 1**.

## Krok 1 z 5 - Logowanie

Odnowienie certyfikatu kwalifikowanego

- Obywatel Polski  
 Obcokrajowiec

- i** W celu rozpoczęcia aktywacji odnowienia certyfikatu kwalifikowanego:
- umieść kartę kryptograficzną w czytniku kart,
  - wciśnij przycisk "WYBIERZ CERTYFIKAT" - zostanie uruchomiony aplet JAVY,
  - wybierz certyfikat, który chcesz odnowić i wciśnij przycisk "OK" - automatycznie zostaną uzupełnione pola Numer seryjny certyfikatu i Numer karty,
  - uzupełnij pozostałe wymagane pola i wciśnij przycisk "Dalej".

- i** Najczęściej występujące problemy z logowaniem [więcej informacji](#)

Certyfikat do odnowienia PESEL **i** Wartość jest wymaganaImię matki 

Wartość jest wymagana

Kod z obrazka 

Wartość jest wymagana

2. Domyślnie zaznaczone jest pole **Obywatel Polski**. Jeżeli certyfikat odnawiany jest dla obywatela Polski - pozostaw ustawienie domyślne. Jeżeli certyfikat przeznaczony jest dla cudzoziemca, wybierz pole **Obcokrajowiec**.
3. Upewnij się, że czytnik podłączony jest do komputera i znajduje się w nim karta kryptograficzna, zawierająca certyfikat kwalifikowany, który ma być odnowiony.

Naciśnij przycisk **Wybierz certyfikat do odnowienia**. Formularz pobierze dane certyfikatu z karty kryptograficznej. Może to chwilę potrwać, więc prosimy o cierpliwość.

## Krok 1 z 5 - Logowanie

Odnowienie certyfikatu kwalifikowanego

- Obywatel Polski  
 Obcokrajowiec

- i** W celu rozpoczęcia aktywacji odnowienia certyfikatu kwalifikowanego:
- umieść kartę kryptograficzną w czytniku kart,
  - wciśnij przycisk "WYBIERZ CERTYFIKAT" - zostanie uruchomiony aplet JAVY,
  - wybierz certyfikat, który chcesz odnowić i wciśnij przycisk "OK" - automatycznie zostaną uzupełnione pola Numer seryjny certyfikatu i Numer karty,
  - uzupełnij pozostałe wymagane pola i wciśnij przycisk "Dalej".

- i** Najczęściej występujące problemy z logowaniem [więcej informacji](#)

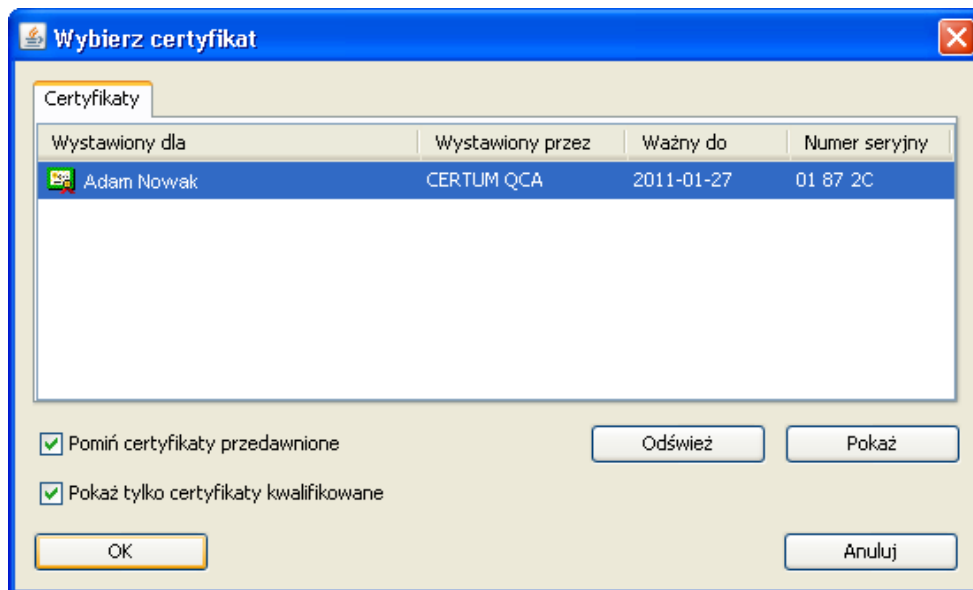
Certyfikat do odnowienia PESEL **i** Wartość jest wymaganaImię matki 

Wartość jest wymagana

Kod z obrazka 

Wartość jest wymagana

4. Pojawi się okno dialogowe z wyborem certyfikatu. Wyświetlone zostaną wyłącznie certyfikaty, które mają status „WAŻNY”. Wybierz odpowiedni certyfikat z listy i naciśnij **OK**.



**Uwaga! Jeżeli posiadasz więcej niż 1 certyfikat kwalifikowany na karcie, w kroku 5 trzeba będzie ponownie wybrać ten sam certyfikat.**

5. Dane z certyfikatu zostaną wczytane automatycznie (numer seryjny certyfikatu i numer karty). Następnie powrócisz do elektronicznego formularza obsługi odnowień.
6. Pozostałe dane (PESEL, imię matki) wymagane do logowania należy uzupełnić samodzielnie. Następnie wpisz kod z obrazka w wyznaczonym polu.

**Krok 1 z 5 - Logowanie**

Odnowienie certyfikatu kwalifikowanego

Obywatel Polski  
 Obcokrajowiec

**i** W celu rozpoczęcia aktywacji odnowienia certyfikatu kwalifikowanego:  
- umieść kartę kryptograficzną w czytniku kart,  
- wciśnij przycisk "WYBIERZ CERTYFIKAT" – zostanie uruchomiony aplet JAVY,  
- wybierz certyfikat, który chcesz odnowić i wciśnij przycisk "OK" – automatycznie zostaną uzupełnione pola Numer seryjny certyfikatu i Numer karty,  
- uzupełnij pozostałe wymagane pola i wciśnij przycisk "Dalej".

**i** Najczęściej występujące problemy z logowaniem [więcej informacji](#)

**!** Błąd! Imię matki nie zostało podane.


Certyfikat do odnowienia

Numer seryjny certyfikatu

Numer karty

PESEL  **i**

Imię matki  **Wartość jest wymagana**



Kod z obrazka  **Wartość jest wymagana**

7. Naciśnij przycisk **Dalej**. Przejdiesz do **kroku 2 – Aktywacja usługi**, w którym należy podać kod

aktywacyjny.

## 2.2 Etap 1 z 5 – Generowanie nowej pary kluczy

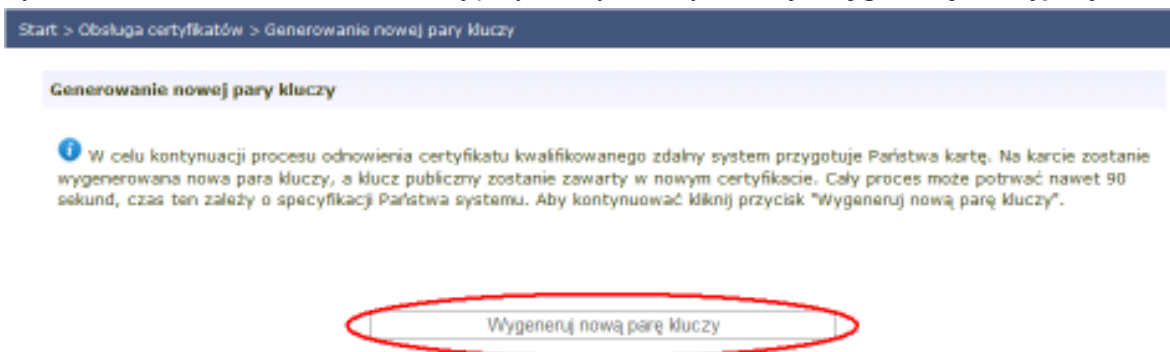
### UWAGA!

Poniższy punkt dotyczy wyłącznie osób posiadających karty, które nie zawierają wolnej pary kluczy na karcie.

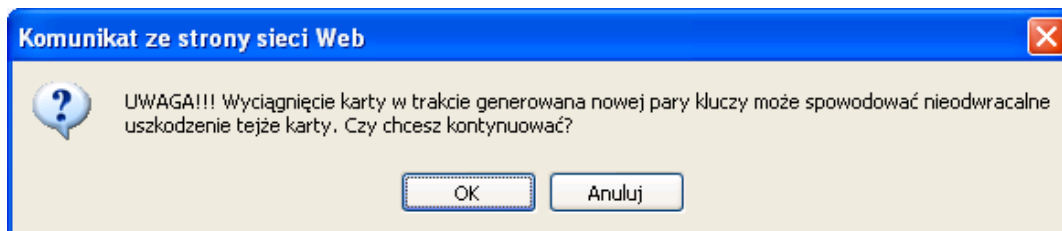


Jeśli po zalogowaniu na stronie do odnowień nie pojawi się poniższe okno, oznacza to, że posiadana przez Ciebie karta nie wymaga generacji dodatkowej pary kluczy. W takim przypadku należy przejść do kolejnego punktu instrukcji Etap 2 z 5 – Aktywacja usługi.

8. Po wyświetleniu okna „Generowanie nowej pary kluczy” należy wcisnąć „**Wygeneruj nową parę kluczy**”.



9. Pojawi się ostrzeżenie, aby w trakcie generowania nowej pary kluczy nie wyciągać karty z czytnika, gdyż może to spowodować uszkodzenie karty. Należy upewnić się, że karta znajduje się w czytniku, a następnie wcisnąć przycisk **OK**.



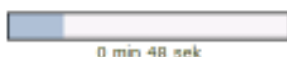
10. Pojawi się okno „Wprowadzanie kodu PIN”, gdzie należy podać **kod PIN do profilu bezpiecznego**, a następnie wcisnąć przycisk **OK**.

11. Po wpisaniu poprawnego kodu PIN pojawi się pasek postępu pokazujący na jakim etapie znajduje się proces generowania kluczy na karcie.

#### Generowanie nowej pary kluczy

**i** W celu kontynuacji procesu odnowienia certyfikatu kwalifikowanego zdalny system przygotowuje Państwa kartę. Na karcie zostanie wygenerowana nowa para kluczy, a klucz publiczny zostanie zawarty w nowym certyfikacie. Cały proces może potrwać nawet 90 sekund, czas ten zależy o specyfikacji Państwa systemu. Aby kontynuować kliknij przycisk "Wygeneruj nową parę kluczy".

Proces generowania kluczy



Po wygenerowaniu kluczy applet automatycznie sam przejdzie do następnego kroku (Etap 2 z 5 – Aktywacja usługi)

### 2.3 Etap 2 z 5 – Aktywacja usługi

#### Krok 2 z 5 - Aktywacja usługi

Kwalifikowany certyfikat o numerze seryjnym 0x1872C jest ważny od 2009/01/27 15:18:51 do 2011/01/27 15:18:51.

Czas na odnowienie certyfikatu: **568 dni, 03 godzin, 46 minut, 32 sekund**

#### Aktywacja usługi

**i** Proszę podać 16 znakowy kod aktywacyjny.

Kod aktywacyjny: 0hcXESDgm1H 5DhU9a7HzPsSF71J Urz8W2CRLDrWyh

Jeśli nie posiadają Państwo "Karty Aktywacyjnej", prosimy zakupić odpowiednią kartę w:

- sklepie internetowym CERTUM PCC
- wybranych Punktach Sprzedaży

Możliwa jest zmiana okresu ważności certyfikatu (roczny na dwuletni i odwrotnie).

12. Jeżeli kod aktywacyjny zostanie przyjęty przez system, przejdziesz do **kroku 3 – Weryfikacja danych Subskrybenta**. W przypadku pojawienia się problemów z kodem aktywacyjnym, skontaktuj się z Infolinią.

### 2.4 Etap 3 z 5 – Weryfikacja danych Subskrybenta

13. W **kroku 3** zweryfikuj dane zawarte w certyfikacie, dane kontaktowe oraz dodatkowe dane identyfikacyjne.

**Uwaga !** – W trakcie procesu odnowienia, istnieje możliwość zmiany niektórych danych kontaktowych, danych identyfikacyjnych oraz danych widocznych w certyfikacie. Zmianom nie podlegają dane takie jak:

imię, nazwisko, numer PESEL oraz wszystkie dodatkowe dane identyfikacyjne: NIP, adres itp.

Zmiana danych może spowodować konieczność przekazania dodatkowych dokumentów identyfikacyjnych do CERTUM PCC. Jeżeli zajdzie taka konieczność, po otrzymaniu wypełnionego przez państwo formularza, nasz operator prześle informacje na podany w danych kontaktowych adres e-mail i poinformuje o dokumentach wymaganych do kontynuowania procesu odnowienia.

**UWAGA:** Wydanie nowego certyfikatu skutkuje unieważnieniem poprzedniego.

Jeśli chcesz, możesz zmodyfikować dane z certyfikatu oraz zaznaczyć czy dane mają być widoczne.

#### Krok 3 z 5 - Weryfikacja danych Subskrybenta

Kwalifikowany certyfikat o numerze seryjnym 0x1872C jest ważny od 2009/01/27 15:18:51 do 2011/01/27 15:18:51.

Czas na odnowienie certyfikatu: **568 dni, 03 godzin, 41 minut, 54 sekund**

#### Dane zawarte w certyfikacie

Nazwa powszechna:	Adam Nowak
Imię / Imiona:	Adam
Nazwisko:	Nowak
Numer PESEL:	80010100111
Kraj pobytu:	PL

*Dane reprezentowanego podmiotu*

Modyfikuj dane zawarte w certyfikacie

#### **UWAGA!**

**W przypadku modyfikacji danych, wszyscy klienci posiadający kartę starego typu z 8 cyfrowym numerem, otrzymają przesyłką kurierską nową kartę kryptograficzną, na którą zostanie wygenerowany odnowiony certyfikat kwalifikowany.**

14. Następnie ukaże się okno do edycji danych zawartych w certyfikacie. Zmodyfikuj odpowiednie dane i naciśnij **Zapisz zmiany**.

**Krok 3 z 5 - Weryfikacja danych Subskrybenta**

**i** Zweryfikuj i zaktualizuj dane zawarte w certyfikacie. Dane, które ulegną zmianie zostaną zweryfikowane przez operatora CERTUM PCC, który w przypadku wątpliwości skontaktuje się z Tobą drogą elektroniczną i poprosi o przysłanie dokumentów wymaganych do weryfikacji nowych danych.

**Dane zawarte w certyfikacie**

**Czy dane mają być widoczne w certyfikacie**

Nazwa powszechna   TAK

*"Jestem osobą fizyczną lub przedstawicielem podmiotu, wobec którego wymagane jest umieszczenie dodatkowych informacji w Nazwie powszechnej certyfikatu kwalifikowanego"*

Pierwsze imię:   TAK

Nazwisko:   TAK

Numer PESEL   TAK

Kraj pobytu   TAK

Okres ważności certyfikatu:

\* - pole dotyczy reprezentowanego podmiotu

W celu modyfikacji **danych kontaktowych**, ukaże się okno z możliwością edycji danych. Zmodyfikuj dane i naciśnij **Zapisz zmiany**.

**Krok 3 z 5 - Weryfikacja danych Subskrybenta**

**i** Zweryfikuj i zaktualizuj dane zawarte w certyfikacie. Dane, które ulegną zmianie zostaną zweryfikowane przez operatora CERTUM PCC, który w przypadku wątpliwości skontaktuje się z Tobą drogą elektroniczną i poprosi o przysłanie dokumentów wymaganych do weryfikacji nowych danych.

**Dane kontaktowe**

**Czy dane mają być widoczne w certyfikacie**

Nazwa korespondencyjna

Ulica

Numer domu / lokalu:

Kod pocztowy:

Miejscowość:

Województwo

Kraj

Telefon   TAK

**Korespondencja dotycząca wydania certyfikatu prowadzona będzie na adres email Subskrybenta**

Adres email Subskrybenta:   TAK

\* - pole dotyczy reprezentowanego podmiotu

Wiersze, w których zmodyfikowano dane, zostaną podświetlone na niebiesko. Po przesunięciu kursora nad zmodyfikowany wiersz, ukaze się informacja o wersji oryginalnej tekstu.

**Dane kontaktowe**

Nazwa korespondencyjna:	Unizeto Technologies S.A.
Ulica:	Królowej Korony Polskiej 
Numer domu / lokalu:	21
Kod pocztowy:	70-486
Miejscowość:	Szczecin

Dana została poprawiona.  
Oryginalna wartość: Królowej Korony Polskiej

15. Aby zmodyfikować dane identyfikacyjne, w polu **Dane identyfikacyjne**, naciśnij na przycisk **Modyfikuj dane identyfikacyjne**.

**UWAGA**


Należy zwrócić uwagę na poprawność adresu e-mail, gdyż na podany adres zostanie wysłany link do pobrania certyfikatu.

**— Dodatkowe dane identyfikacyjne —**

Imię ojca:	Stanisław
Imię matki:	Małgorzata
Rodzaj dokumentu tożsamości:	Dowód osobisty
Seria i numer dokumentu tożsamości:	ABC 123123
Oznaczenie organu wydającego:	Prezydent Miasta Szczecin
Kraj urodzenia:	PL
Miejsce urodzenia:	Szczecin
Obywatelstwo:	PL
Płeć:	M
Data urodzenia:	1980-01-01
<input type="button" value="Modyfikuj dodatkowe dane identyfikacyjne"/>	


16. W nowym oknie wprowadź odpowiednie modyfikacje i naciśnij **Zapisz zmiany**. Jeśli nie chcesz modyfikować danych, naciśnij **Powrót**.
17. Następnie w polu **Początek ważności certyfikatu** zaznacz kiedy ma rozpocząć się okres ważności odnawianego certyfikatu kwalifikowanego. Domyślnie ustawiona jest pierwsza opcja „Bez definiowania początku okresu ważności certyfikatu kwalifikowanego”.
- a. Jeśli chcesz wybrać konkretny dzień od kiedy certyfikat kwalifikowany ma rozpocząć swój okres ważności zaznacz opcję „Data początku okresu ważności certyfikatu w dniu XXXX”.

**— Początek ważności certyfikatu —**

- Bez definiowania początku okresu ważności certyfikatu kwalifikowanego
- Data początku okresu ważności certyfikatu w dniu RRRR-MM-DD 12:00:00 GMT 


- b. Jeśli certyfikat, których chcesz odnowić ważny jest jeszcze przez 3 miesiące w polu Początek ważności certyfikatu pojawią się trzy opcje do wyboru. W tym przypadku jeśli certyfikat ma zostać wydany z datą wygaśnięcia odnawianego certyfikatu kwalifikowanego należy zaznaczyć drugą opcję (z trzech możliwych do wyboru).

**Początek ważności certyfikatu**

- Bez definiowania początku okresu ważności certyfikatu kwalifikowanego
- Początek okresu ważności nowego certyfikatu od dnia końca ważności certyfikatu odnawianego 2010-09-12 10:40:00 GMT
- Data początku okresu ważności certyfikatu w dniu RRRR-MM-DD 12:00:00 GMT 

- c. W przypadku zaznaczenia opcji „Data początku okresu ważności certyfikatu w dniu XXXX” należy nacisnąć kalendarzyk znajdujący się po prawej stronie i wybrać odpowiednią datę rozpoczęcia certyfikatu. Maksymalnie może to być 90 dni od dnia, w którym odnawiany jest certyfikat.

**Początek ważności certyfikatu**

- Bez definiowania początku okresu ważności certyfikatu kwalifikowanego
- Data początku okresu ważności certyfikatu w dniu RRRR-MM-DD 12:00:00 GMT 

**Karta**

- Karta kryptograficzna typu mini (karta SAM z Zestawów CERTUM mini).

**Kto pop**

**przez ścieżkę sprzedaży?**

CLOSE 

Kwiecień 2010

Pn	Wt	Śr	Cz	Pt	Sb	Nd
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

Następny >

Wybór opiekuna klienta:  

- Wyrażam zgodę na przetwarzanie moich danych osobowych dla realizacji procesu certyfikacji. Wyrażam zgodę na przesłanie do mnie drogą elektroniczną na wskazany adres e-mail, dokumentów powyżej danymi.
- Chcę otrzymywać informacje o aktualnej ofercie Unizeto Technologies SA i wyrażam zgodę na przetwarzanie moich danych osobowych w celach

18. Jeśli posiadasz kartę kryptograficzną z zestawu mini, zaznacz okienko w ostatniej części formularza. Następnie możesz wybrać opiekuna klienta, przy pomocy którego realizowany jest proces odnowienia.

**Karta kryptograficzna**

- Posiadam kartę kryptograficzną typu mini (karta SAM z Zestawów CERTUM mini).

**Kto przeprowadził Ciebie przez ścieżkę sprzedaży?**

Wybór opiekuna klienta:  

- \* Wyrażam dobrowolną zgodę potrzeb niezbędną do realizacji przesłanie do mnie drogą elektroniczną na wskazany adres e-mail, dokumentów wypełnionych podanymi powyż

brak  
brak  
Inny  
Akwizytor  
Partner  
Punkt Rejstracji  
Dział Handlowy Unizeto Technologies SA  
Infolinia

19. Następnie przejdź do akceptacji oświadczeń – gwiazdką zostały zaznaczone oświadczenia, których akceptacja jest wymagana do kontynuowania procesu odnowienia. Aby otrzymywać informacje o aktualnej ofercie Unizeto Technologies SA, nieobligatoryjnie zaznacz opcję otrzymywania informacji o ofertach.

- \*\* Wyrażam dobrowolną zgodę na przetwarzanie moich danych osobowych dla potrzeb niezbędnych do realizacji procesu certyfikacji. Wyrażam zgodę na przesłanie do mnie drogą elektroniczną na wskazany adres e-mail, dokumentów wypełnionych podanymi powyżej danymi.
- Chcę otrzymywać informacje o aktualnej ofercie Unizeto Technologies SA i wyrażam zgodę na przetwarzanie moich danych osobowych w celach marketingowych.
- \*\* Zapoznałem się z podstawowymi informacjami na temat zakresu stosowania kwalifikowanego certyfikatu, jego skutkach prawnych, sposobie rozpatrywania skarg i wniosków oraz o systemie dobrowolnej rejestracji kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Zakres stosowania certyfikatu:  
- wydany certyfikat na podstawie podanych danych będzie stosowany do weryfikacji bezpiecznych podpisów elektronicznych składanych przy użyciu klucza prywatnego komplementarnego do klucza publicznego zawartego w wydanym certyfikacie z ograniczeniami wynikającymi z górnej kwoty transakcji określonej we wniosku o wydanie kwalifikowanego certyfikatu oraz zakresu otrzymanego przez wnioskodawcę umocowania do działania w cudzym imieniu.

Skutki prawne składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu:  
- bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu stanowi dowód tego, że został złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny, a dane w postaci elektronicznej nim opatrzone są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, z zastrzeżeniem, że przepisy szczególne mogą stanowić inaczej.

Powyższe dane będą przetwarzane przez Unizeto Technologies SA, z siedzibą w Szczecinie przy ul. Królowej Korony Polskiej 21, zgodnie z Ustawą z dnia 29.08.1997 r. o ochronie danych osobowych, DzU nr 133, poz. 883 ze zmianami. Przysługuje Państwu prawo do wglądu i poprawienia przekazanych danych osobowych.

- \* - pole dotyczy reprezentowanego podmiotu
- \*\* - pole wymagane

Dalej

20. Naciśnij na przycisk **Dalej**, znajduje się on na dole formularza.

21. Zostaniesz przekierowany do **kroku 4**, czyli prezentacji aneksu do umowy z subskrybentem.

## 2.5 Etap 4 z 5 – Prezentacja Aneksu do Umowy z Subskrybentem

### Krok 4 z 5 - Prezentacja Aneksu do Umowy z Subskrybentem

**i** Zapoznaj się z Aneksem do umowy o świadczenie usług certyfikacyjnych, a następnie wciśnij przycisk „Przejdź do podpisania aneksu” znajdujący się na dole strony.

Prosimy zwrócić szczególną uwagę na nr umowy której dotyczy Aneks - powinien być taki sam jak numer umowy o wydanie odnawianego certyfikatu kwalifikowanego.

<p><b>Aneks nr 987654/CCK/2010 do</b> Umowy z Subskrybentem nr 112233/CCK/2010 o świadczenie kwalifikowanych usług certyfikacyjnych zawarty w Szczecinie dnia 19.04.2010 roku</p>
<p> pomiędzy Stronami:</p>
<p>Unizeto Technologies S.A. z siedzibą w Szczecinie, przy ul. Królowej Korony Polskiej 21, wpisaną do rejestru sądowego prowadzonego przez Sąd Rejonowy Szczecin-Centrum, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego w Szczecinie nr KRS 0000233499 oraz do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne pod nr 1, NIP: 852-000-64-44, kapitał zakładowy (wpłacony w całości): 5 600 000 zł, reprezentowaną przez Andrzeja Bendig-Wielowiejskiego - Prezesa Zarządu zwaną dalej "Unizeto", a</p>
<p><b>Adam Nowak</b> IMIĘ I NAZWISKO</p>
<p><b>1980-01-01 Szczecin</b> DATA I MIEJSCE URODZENIA</p>
<p><b>80010100111</b> NUMER PESEL</p>
<p><b>ABC 123123 Prezydent Miasta Szczecin</b> STYLAK, NUMER I RODZAJ DOKUMENTU ROZPOWIAŚCI ORAZ OZNACZENIE ORGANU WYDAJĄCEGO</p>
<p>zwaną dalej "Subskrybentem", o następującej treści:</p>
<p><b>§1 PRZEDMIOT UMOWY</b></p>
<ul style="list-style-type: none"> <li>• Przedmiotem niniejszego Aneksu jest rozszerzenie zakresu zawartej pomiędzy Stronami Umowy o świadczenie usług certyfikacyjnych w zakresie wydawania i unieważniania certyfikatu oraz świadczenie usług certyfikacyjnych zgodnie z warunkami określonymi w Ustawie z dnia 18 września 2001 roku o podpisie elektronicznym (Dz.U.130 poz.1450 z późn.zm), w wykazie danych rejestracyjnych oraz w Regulaminie Usług Certyfikacyjnych.</li> <li>• Rozszerzenie zakresu Umowy polega na przedłużeniu okresu świadczenia usług certyfikacyjnych na kolejny okres ważności certyfikatów wydanych na jej podstawie. Wydanie certyfikatu odbędzie się na karcie kryptograficznej należącej do Subskrybenta o numerze 1010:0:0:0101010 stanowiącej komponent techniczny podlegający wyłącznej kontroli Subskrybenta. Dane zawarte w certyfikacie nie ulegną zmianie poza nowym numerem seryjnym certyfikatu, nowym okresem jego ważności oraz podpisem Centrum Certyfikacji.</li> <li>• 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 na karcie Subskrybenta oraz na stosowanie tych danych do weryfikacji jego podpisu elektronicznego.</li> <li>• Wygenerowany certyfikat będzie wydany na kolejną parę kluczy, na okres dwóch lat.</li> <li>• Wygenerowany certyfikat będzie zawierał jeden z wymienionych kluczy publicznych: 5366C1EFB83A181577325953F0E851F42BEE9C1F 4CA04C16A2CB33E420AC02EA2B6D945A39D600DC 7EACF65E182786FE416053C4F95816D7BCD630F6</li> </ul>
<p><b>§2 OBOWIĄZYWANIE UMOWY</b></p>
<p>Aneks wchodzi w życie z dniem podpisania i obowiązuje do czasu wygaśnięcia terminu ważności certyfikatów będących przedmiotem niniejszego Aneksu do umowy o świadczenie usług certyfikacyjnych.</p>
<p><b>§3 WARUNKI PŁATNOŚCI</b></p>
<p>Wynagrodzenie Unizeto za przedmiot umowy określony w § 1 jest zgodne z obowiązującym cennikiem.</p>
<p><b>§4 POSTANOWIENIA KOŃCOWE</b></p>
<ul style="list-style-type: none"> <li>• Aneks został sporządzony w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.</li> <li>• Zmiany niniejszego Aneksu wymagają formy pisemnej lub jej równoważnej pod rygorem nieważności.</li> </ul>

Poniżej aneksu znajduje się przykładowy załącznik z danymi do certyfikatu kwalifikowanego.

W przypadku zaznaczenia w polu Początek ważności certyfikatu „Bez definiowania początku okresu ważności certyfikatu kwalifikowanego” w załączniku do aneksu pojawi się informacja jak poniżej (zaznaczona na czerwono).

<b>Załącznik nr 1</b> do aneksu nr 987654/CCK/2010	
<b>DANE DO CERTYFIKATU KWALIFIKOWANEGO</b>	
Kwalifikowany certyfikat zgodnie z elektronicznym wnioskiem będzie zawierał następujące dane:	
<b>Adam Nowak</b> ..... Nazwa powszechna	<b>Adam</b> ..... Pierwsze imię
<b>Nowak</b> ..... Nazwisko	<b>80010100111</b> ..... Numer PESEL
<b>PL</b> ..... Kraj pobytu	.....
Termin ważności certyfikatu to dwa lata od daty rozpoczęcia ważności odnowionego certyfikatu. W imieniu własnym.	
<b>DODATKOWE DANE IDENTYFIKACYJNE</b>	

Jeśli w polu Początek ważności certyfikatu zaznaczono dzień od kiedy certyfikat kwalifikowany ma rozpocząć swój okres ważności w załączniku do aneksu pojawi się informacja jak poniżej (zaznaczona na czerwono). Jest to **sugerowana** data rozpoczęcia ważności certyfikatu.

<b>Załącznik nr 1</b> do aneksu nr 987654/CCK/2010	
<b>DANE DO CERTYFIKATU KWALIFIKOWANEGO</b>	
Kwalifikowany certyfikat zgodnie z elektronicznym wnioskiem będzie zawierał następujące dane:	
<b>Adam Nowak</b> ..... Nazwa powszechna	<b>Adam</b> ..... Pierwsze imię
<b>Nowak</b> ..... Nazwisko	<b>800010100111</b> ..... Numer PESEL
<b>PL</b> ..... Kraj pobytu	.....
Termin ważności certyfikatu to dwa lata od daty rozpoczęcia ważności odnowionego certyfikatu. <u>Sugerowana data</u> rozpoczęcia ważności certyfikatu 2010-07-07 12:00:00 GMT. W imieniu własnym.	
<b>DODATKOWE DANE IDENTYFIKACYJNE</b>	

Koniecznie sprawdź wszystkie dane zawarte w załączniku.

DODATKOWE DANE IDENTYFIKACYJNE	
Dodatkowe dane identyfikacyjne Subskrybenta nie zawarte w certyfikacie, a które są niezbędne do Umowy, późniejszej weryfikacji tożsamości lub ewentualnego unieważnienia certyfikatu:	
<b>1980-01-01</b> Data urodzenia	<b>PL</b> Obywatelstwo
<b>PL</b> Kraj urodzenia	<b>Szczecin</b> Miejsce urodzenia
<b>Stanisław</b> Imię ojca	<b>Dowód osobisty</b> Rodzaj dokumentu tożsamości
<b>ABC 123123</b> Seria i numer dokumentu tożsamości	<b>Prezydent Miasta Szczecin</b> Oznaczenie organu wydającego
<b>Małgorzata</b> Imię matki	<b>M</b> Płeć
<b>W imieniu własnym</b> Sposób działania	

**OŚWIADCZENIA DO ANEKSU NR 987654/CCK/2010**

Oświadczam, że wyrażam zgodę na stosowanie przez CERTUM danych służących do weryfikacji mojego podpisu elektronicznego (czyli klucza publicznego), które zostaną zawarte w certyfikacie, o który się ubiegam.

Oświadczam, że przed zawarciem umowy zapoznałem(am) się z warunkami użycia certyfikatu (dokument opublikowany w Internecie pod adresem <http://www.certum.pl>), o który się ubiegam, w tym o sposobie rozpatrywania skarg i wniosków, a w szczególności o istotnych jego warunkach obejmujących:

- zakres i ograniczenia jego stosowania,
- skutki prawne składania podpisów.

Oświadczam, że wszystkie informacje podane przeze mnie w formularzu, są zgodne z prawdą. Wyrażam zgodę na przetwarzanie moich danych osobowych przez Unizeto Technologies S.A. i sieć Systemu Rejestracji, dla potrzeb niezbędnych do realizacji procesu certyfikacji. Ponadto, przyjmuję do wiadomości iż: mam prawo dostępu do treści danych osobowych, o których mowa wyżej, mam prawo do ich poprawiania, a administratorem tych danych będzie Unizeto Technologies S.A. z siedzibą w Szczecinie, ul. Królowej Korony Polskiej 21.

Adres do korespondencji:

<b>+48 91 48 01 278</b> Telefon	<b>adam.nowak@unizeto.pl</b> Adres email Subskrybenta
<b>Adam Nowak</b> Nazwa korespondencyjna	<b>Królowej Korony Polskiej</b> Ulica
<b>21</b> Numer domu / lokalu	<b>70-486</b> Kod pocztowy
<b>Szczecin</b> Miejscowość	<b>zachodniopomorskie</b> Województwo
<b>PL</b> Kraj	

Powrót

Przejdź do podpisania aneksu

22. Przeczytaj uważnie aneks i zweryfikuj dane w załączniku. Jeżeli wszystkie dane są poprawne, naciśnij przycisk **Przejdź do podpisania aneksu**. Zostaniesz przekierowany do ostatniego, piątego kroku procedury.

## 2.6 Etap 5 z 5 – Podpisywanie aneksu

23. Pozwól na uruchomienie apletu Java. Zostanie wyświetlona lista plików do podpisania.

### Krok 5 z 5 - Podpisywanie aneksu

**i** Po uruchomieniu apletu zostaną wyświetlone dokumenty, które należy podpisać w celu zakończenia procesu odnowienia. Możesz je wyświetlić zaznaczając odpowiedni z nich i wciskając przycisk Otwórz lub Pokaż źródło.

W celu kontynuowania procesu upewnij się, że karta kryptograficzna z certyfikatem kwalifikowanym jest umieszczona w czytniku, a następnie wciśnij przycisk Podpisz i postępuj zgodnie z pojawiającymi się instrukcjami.

Uwaga: proces składania podpisu jest zależny od posiadanego komputera i łącza internetowego i może trwać od kilku do kilkudziesięciu sekund.



24. Upewnij się, że czytnik jest podłączony do komputera, a karta umieszczona jest w środku czytnika. Naciśnij **Podpisz**.

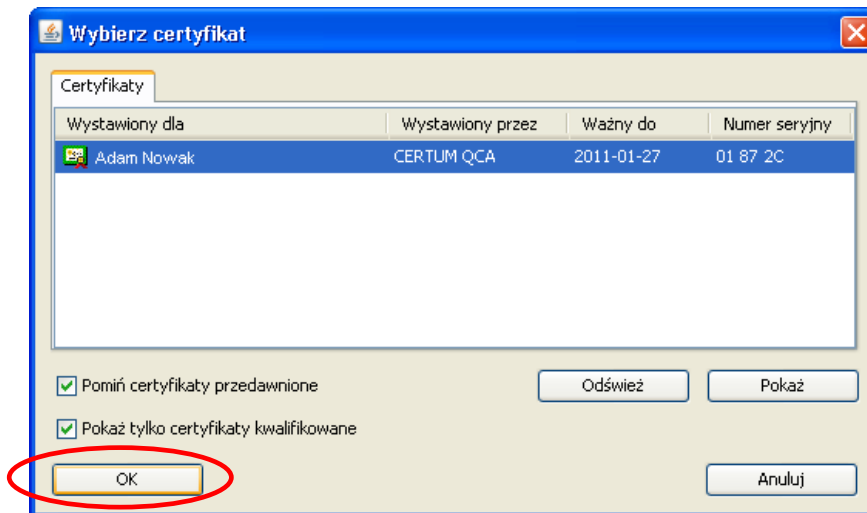
Dane są gotowe do podpisania

Nazwa pliku	Opis	Rozmiar	Pobrany?
aneks.html		3,99 KB	Tak
załącznik.html		5,89 KB	Tak

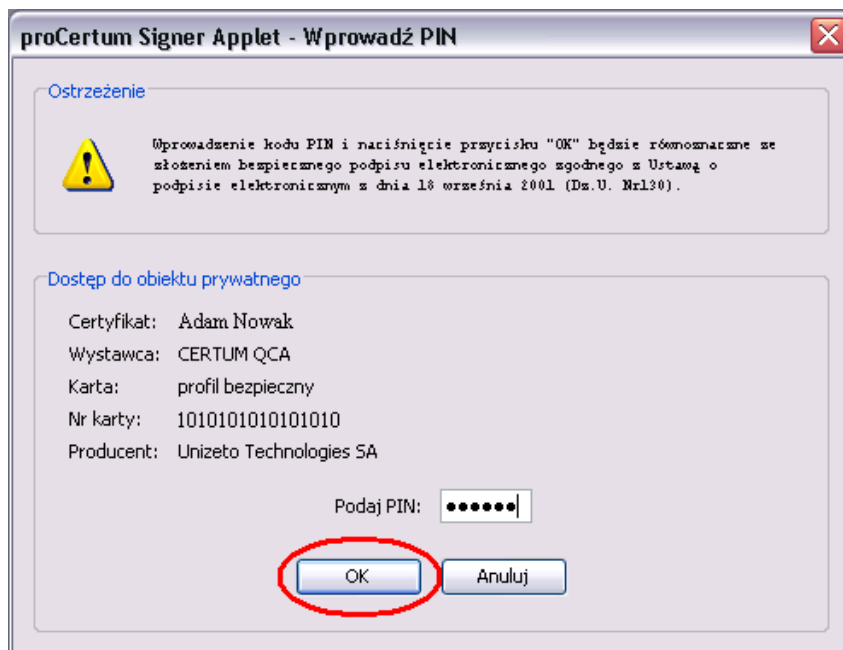
Otwórz   Pokaż źródło   Zapisz   **Podpisz**

25. Otworzy się okno dialogowe. Wybierz certyfikat do podpisu i naciśnij **OK**.

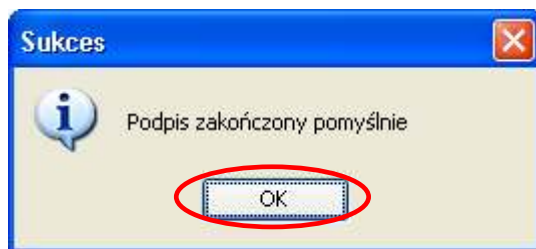
**Uwaga!** Jeżeli na karcie znajdują się dwa certyfikaty, wybierz z listy ten sam, który został wybrany w kroku 1.



26. W kolejnym oknie podaj PIN do certyfikatu i naciśnij **OK**.



27. Jeśli dokumenty zostaną prawidłowo podpisane, ukaże się odpowiedni komunikat.



28. Naciśnij **OK**. Zapoznaj się z informacjami zawartymi w **Podsumowania**.

**Podsumowanie**

Dziękujemy!

**i** Proces składania wniosku o odnowienie certyfikatu kwalifikowanego został zakończony.

W ciągu 48 godzin (w dni robocze) otrzymasz informacje na podany adres e-mail, o weryfikacji przesłanych dokumentów formalnych. W wiadomości zawarty będzie także adres przez który, będzie możliwość pobrania podpisanego obustronnie Aneksu do Umowy z Subskrybentem. W przypadku jakichkolwiek wątpliwości nasz operator skontaktuje się z państwem i udzieli dalszych informacji.

Najpóźniej w ciągu 7 dni kalendarzowych od momentu wpłynięcia poprawnie podpisanych dokumentów elektronicznych do CERTUM PCC, 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 przypadku jakichkolwiek wątpliwości prosimy o kontakt z naszą infolinią:

- drogą telefoniczną – 0 801 540 340
- drogą elektroniczną – infolinia@unizeto.pl
- przez Chat Online – dostępnym na serwisie www.certum.pl

W ciągu 7 dni, od momentu wpłynięcia poprawnie podpisanych dokumentów elektronicznych do CERTUM PCC (bez względu na to jak długo jest ważny poprzedni certyfikat), zostanie wydany odnowiony certyfikat kwalifikowany. Certyfikat ten będzie można pobrać drogą elektroniczną i zapisać na posiadanej karcie kryptograficznej. W przypadku, w którym zaistnieje konieczność uzupełnienia lub potwierdzenia podanych danych, skontaktuje się państwem nasz operator.

**Po otrzymaniu powyższego e-maila użytkownik, może przystąpić do procesu odnowienia certyfikatu, który został opisany poniżej.**

**Nowy certyfikat kwalifikowany zostanie wydany w terminie nie przekraczającym 7 dni od daty obustronnej podpisania umowy.**

### **KROK 3 - POBRANIE ODNOWIONEGO CERTYFIKATU NA KARTĘ KRYPTOGRAFICZNĄ**

Certyfikat kwalifikowany wydawany jest przez CERTUM PCC po otrzymaniu kompletu poprawnie wypełnionych dokumentów. W poniższej instrukcji zawarte zostały kolejne kroki procesu pobierania certyfikatu kwalifikowanego.

**Poniżej przykładowy mail potwierdzający zatwierdzenie przesłanego elektronicznie Aneksu.**

**TEMAT: CERTUM PCC: Informacja o statusie odnowienia certyfikatu kwalifikowanego**

Szanowni Państwo,

Pragniemy poinformować o podpisaniu przez pracownika CERTUM PCC przesłanego elektronicznie Aneksu.

Dotyczy  
Adam Nowak  
Aneks 987654/CCK/2010 do umowy 112233/CCK/2009

Aneks można pobrać po adresem:

<https://status.certum.pl/wniosek/>

Podczas logowania w pole "Numer umowy" należy wpisać numer aneksu 987654/CCK/2010.

Odnowiony certyfikat kwalifikowany zostanie dla Państwa wydany najpóźniej w ciągu 7 dni roboczych od momentu wpłynięcia do CERTUM podpisanego Aneksu do Umowy z Subskrybentem. O możliwości pobrania odnowionego certyfikatu kwalifikowanego informujemy Państwa drogą elektroniczną.

W przypadku pytań prosimy o kontakt z naszą Infolinią:

- e-mail: [infolinia@unizeto.pl](mailto:infolinia@unizeto.pl),
- nr tel.: 0 801 540 340 (czynna 24h na dobę),  
dla telefonów komórkowych: +48 (0) 91 4801 340.

Z poważaniem,  
Zespół CERTUM PCC

Procedurę pobierania certyfikatu kwalifikowanego możesz rozpocząć w momencie otrzymania na podany w dokumentach adres e-mail, informacji potwierdzającej wydanie przez CERTUM PCC certyfikatu kwalifikowanego.

**Temat: CERTUM PCC: Informacja o wydaniu certyfikatu kwalifikowanego**

Szanowni Państwo,

Na podstawie złożonego wniosku o numerze 987654, został wydany certyfikat kwalifikowany.

W celu zainstalowania certyfikatu na karcie kryptograficznej, należy udać się na stronę:  
<https://status.certum.pl/cua/>

TELEKOD: XXXX333YYY666ZZZ999BBB222KKK579A

TELEKOD jest Państwa unikalnym identyfikatorem, który umożliwi instalację wydanego certyfikatu kwalifikowanego.

Wszelkie informacje odnośnie procedury instalacji certyfikatu znajdują Państwo w dokumencie PDF pod adresem:

[http://www.certum.pl/upload\\_module/wysiwyg/certum/instrukcje/krok\\_3\\_pobieranie\\_certyfikatow\\_kwalifikowanych\\_1.6.pdf](http://www.certum.pl/upload_module/wysiwyg/certum/instrukcje/krok_3_pobieranie_certyfikatow_kwalifikowanych_1.6.pdf)

W przypadku wszelkich pytań prosimy o kontakt z naszą infolinią:




- e-mail: [infolinia@unizeto.pl](mailto:infolinia@unizeto.pl)
- nr tel.: 0 801 540 340 (czynna 24h na dobę),  
 dla tel. komórkowych: +48 (0) 91 4801 340

Z poważaniem,  
 CERTUM - Powszechne Centrum Certyfikacji  
 www.certum.pl

- W wiadomości elektronicznej otrzymasz TELEKOD – jest to unikalny, przypisany do Twojej karty numer, który będzie wykorzystywany w procesie pobierania certyfikatu kwalifikowanego.
- Otrzymaś także link do strony, za pośrednictwem której możesz pobrać certyfikat kwalifikowany. Jeżeli posiadasz polskie obywatelstwo, wybierz opcję „Obywatel Polski”.

**Logowanie do systemu**

- Obywatel Polski (Polish citizen)
- Obcokrajowiec (Foreigner)

TELEKOD	<input type="text"/>	 Wartość jest wymagana
PESEL	<input type="text"/>	 Wartość jest wymagana
Numer karty	<input type="text"/>	 Wartość jest wymagana


Zaloguj się

- Zaloguj się do systemu podając TELEKOD, numer swojej karty kryptograficznej, numer PESEL oraz kod z obrazka.

- Jeżeli nie posiadasz polskiego obywatelstwa, wybierz opcję „Obcokrajowiec”.

**Logowanie do systemu**

- Obywatel Polski (Polish citizen)  
 Obcokrajowiec (Foreigner)

<b>TELEKOD</b>	<input type="text"/>	 <b>Wartość jest wymagana</b>
<b>Data urodzenia</b> Birth date	<input type="text"/>	 <b>Wartość jest wymagana</b>
<b>Miejsce urodzenia (miejscowość)</b> Birth location	<input type="text"/>	 <b>Wartość jest wymagana</b>
<b>Imię</b> First name	<input type="text"/>	<b>Wartość jest wymagana</b>
<b>Nazwisko</b> Last name	<input type="text"/>	<b>Wartość jest wymagana</b>
<b>Numer karty</b> Card number	<input type="text"/>	 <b>Wartość jest wymagana</b>

Zaloguj się

- Zaloguj się do systemu podając TELEKOD, datę urodzenia, miejsce urodzenia, imię i nazwisko oraz numer swojej karty kryptograficznej.
- Po zalogowaniu się sprawdź dane właściciela certyfikatu kwalifikowanego. Jeżeli wszystkie dane są poprawne, wciśnij przycisk „Pobierz certyfikat”. W przypadku wykrycia jakichkolwiek niezgodności skontaktuj się z Infolinią Unizeto Technologies SA.

**Informacje o Subskrybencie**

<b>Imię</b>	Adam
<b>Nazwisko</b>	Nowak
<b>Numer PESEL</b>	80010100111
<b>Adres e-mail</b>	adam.nowak@unizeto.pl
<b>Numer karty</b>	1010 1010 1010 1010

Podane powyżej informacje identyfikują osobę dla której został wystawiony certyfikat kwalifikowany przypisany do karty kryptograficznej o podanym numerze. Jeżeli którakolwiek z powyższych danych się nie zgadza prosimy o kontakt telefoniczny z [naszą infolinią](#).

Jeżeli wszystkie dane się zgadzają, można przystąpić do pobierania certyfikatu kwalifikowanego na kartę.

<input type="button" value="Pobierz certyfikat"/>	<input type="button" value="Wyloguj"/>
---	--

- W kolejnym oknie możesz wybrać tryb wgrzania certyfikatu na kartę kryptograficzną. Istnieją dwie możliwości:

– automatyczna instalacja certyfikatu za pośrednictwem apletu JAVA – w dwóch prostych krokach otrzymasz kod PUK, nadasz kod PIN oraz wgrasz certyfikat na kartę

LUB

– zaawansowana (niestandardowa) instalacja certyfikatu – za jej pośrednictwem pobierzesz certyfikat w postaci pliku .cer na dowolną lokalizację na swojej stacji roboczej, zapiszesz kod PUK z konta, a następnie za pomocą aplikacji proCertum CardManager wgrasz samodzielnie certyfikat na kartę oraz zaakceptujesz certyfikat.

Start > Obsługa certyfikatów > Pobieranie certyfikatu kwalifikowanego

### Pobieranie certyfikatu kwalifikowanego

#### Automatyczna instalacja certyfikatu

Wciśnięcie przycisku „Automatyczna instalacja certyfikatu” uruchomi aplikację JAVA, która krok po kroku przeprowadzi Państwa przez proces pobierania certyfikatu na kartę kryptograficzną oraz pozwoli na nadanie kodów PIN. Przed przystąpieniem do automatycznej instalacji certyfikatu, należy zainstalować Zestaw CERTUM zgodnie z załączoną do niego instrukcją, a następnie umieścić w czytniku kartę kryptograficzną.

#### UWAGA !

**Trzykrotne błędne podanie kodu PIN blokuje kartę. W celu jej odblokowania wymagane będzie podanie kodu PUK. Trzykrotne błędne podanie kodu PUK trwale zablokuje kartę kryptograficzną. W przypadku trwałego zablokowania karty należy zakupić nowy Zestaw CERTUM i ponownie wystąpić o certyfikat kwalifikowany.**

W przypadku wątpliwości, czy na komputerze możliwe jest uruchamianie aplikacji JAVA, można skorzystać ze [strony umożliwiającej sprawdzenie instalacji](#), lub [strony umożliwiającej pobranie oraz opisującej proces instalacji środowiska JAVA](#).

Automatyczna instalacja certyfikatu Wyloguj

#### Zaawansowana instalacja certyfikatu (niestandardowa)

Poniższa procedura umożliwia przeprowadzenie ręcznej instalacji certyfikatu na karcie kryptograficznej przy wykorzystaniu oprogramowania proCertum CardManager. Jest to rozwiązanie przeznaczone dla tych z Państwa, u których z różnych powodów występują problemy z obsługą apletu JAVA lub istnieje konieczność przeprowadzenia instalacji w trybie offline.

W celu rozpoczęcia procedury należy

- wcisnąć przycisk **Pobierz certyfikat** i zapisać certyfikat (w formacie .cer) w dowolnej lokalizacji na stacji roboczej
- wcisnąć przycisk **Pobierz kod PUK** i zapisać uzyskany kod
- uruchomić oprogramowanie [proCertum CardManager](#) i postępować zgodnie z instrukcją instalacji certyfikatu.

Pobierz certyfikat

Pobierz kod PUK

Status certyfikatu

[do góry](#) ↗

### 3.1 Automatyczna instalacja certyfikatu kwalifikowanego

Przed przystąpieniem do automatycznej instalacji certyfikatu kwalifikowanego upewnij się, że w czytniku kart kryptograficznych znajduje się **prawidłowa karta kryptograficzna**.

Automatyczna instalacja certyfikatu kwalifikowanego odbywa się w 2 krokach:

- krok 1 - nadanie kodu PIN,
- krok 2 – wgranie certyfikatu kwalifikowanego na kartę i jego akceptacja.

#### **Krok 1 - Nadanie kodu PIN**

Aby nadać nowy kod PIN:

- w pierwszej kolejności zaznacz opcję „Pobierz kod PUK”. Następnie zapisz i wydrukuj wyświetlony **kod PUK**. Jeżeli wcześniej w oprogramowaniu proCertum CardManager dokonana była zmiana kodu PUK, zaznacz pole „Zmieniłem już wcześniej fabryczny kod PUK w oprogramowaniu proCertum CardManager”, a następnie wprowadź odpowiedni kod w polu „KOD PUK”.

#### **UWAGA!**

**Trzykrotne błędne podanie kodu PUK, trwale i nieodwracalnie blokuje kartę kryptograficzną. W przypadku zablokowania karty kryptograficznej nie jest możliwe jej odblokowanie. Taki przypadek oznacza konieczność zakupu nowego certyfikatu razem z kartą kryptograficzną. Dlatego zalecamy by kod PUK, w wydrukowanej formie przechowywać w znanym i bezpiecznym miejscu, niedostępnym dla osób trzecich.**

- Następnie w polu „Wprowadzenie kodu PIN” podaj nowy kod PIN.

#### **Wgrywanie certyfikatu**

Applet znajdujący się na tej stronie wymaga środowiska JAVA w wersji 1.6. Jeżeli aplikacja się nie uruchamia należy skorzystać z pomocy znajdującej się na [tej](#) stronie.

#### **Krok 1 z 2 – Wprowadzenie kodu PIN**

Kod PIN: 

Dla danej karty kryptograficznej kod PIN jest już ustanowiony, prosimy o jego podanie.

Operacja wykonywana na karcie nr: 10101010101010

Trzykrotne błędne podanie kodu PIN prowadzi do jego zablokowania. W celu jego odblokowania wymagane będzie podanie kodu PUK.

Zatwierdź PIN i wgraj certyfikat

**UWAGA!**

Kod PIN może składać się z następujących znaków a-z, A-Z, 0-9, wielkość liter ma znaczenie. Kod PIN będzie wymagany w procesie składania bezpiecznego podpisu elektronicznego. Trzykrotne błędne podanie kodu PIN prowadzi do jego zablokowania. W celu jego odblokowania wymagane będzie podanie kodu PUK.

- Należy kliknąć na przycisk „Zatwierdź PIN i wgraj certyfikat”.

**Wgrywanie certyfikatu**

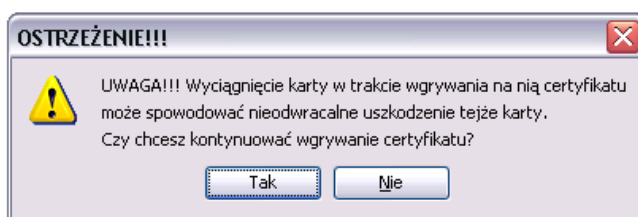
Applet znajdujący się na tej stronie wymaga środowiska JAVA w wersji 1.6. Jeżeli aplikacja się nie uruchamia należy skorzystać z pomocy znajdującej się na [tej](#) stronie.

**Krok 1 z 2 – Wprowadzenie kodu PIN**Kod PIN: 

Dla danej karty kryptograficznej kod PIN jest już ustanowiony, prosimy o jego podanie.

Operacja wykonywana na karcie nr: 1010101010101010

Trzykrotne błędne podanie kodu PIN prowadzi do jego zablokowania. W celu jego odblokowania wymagane będzie podanie kodu PUK.



Następnym krokiem jest potwierdzenie wgrywania certyfikatu.

## Krok 2 - Akceptacja certyfikatu

### Wgrywanie certyfikatu

Applet znajdujący się na tej stronie wymaga środowiska JAVA w wersji 1.6. Jeżeli aplikacja się nie uruchamia należy skorzystać z pomocy znajdującej się na [tej](#) stronie.

#### Krok 2 z 2 – Akceptacja certyfikatu

Certyfikat został wgrany prawidłowo. Prosimy o jego wyświetlenie poprzez przycisk **Pokaż Certyfikat** i zweryfikowanie zawartych w nim informacji

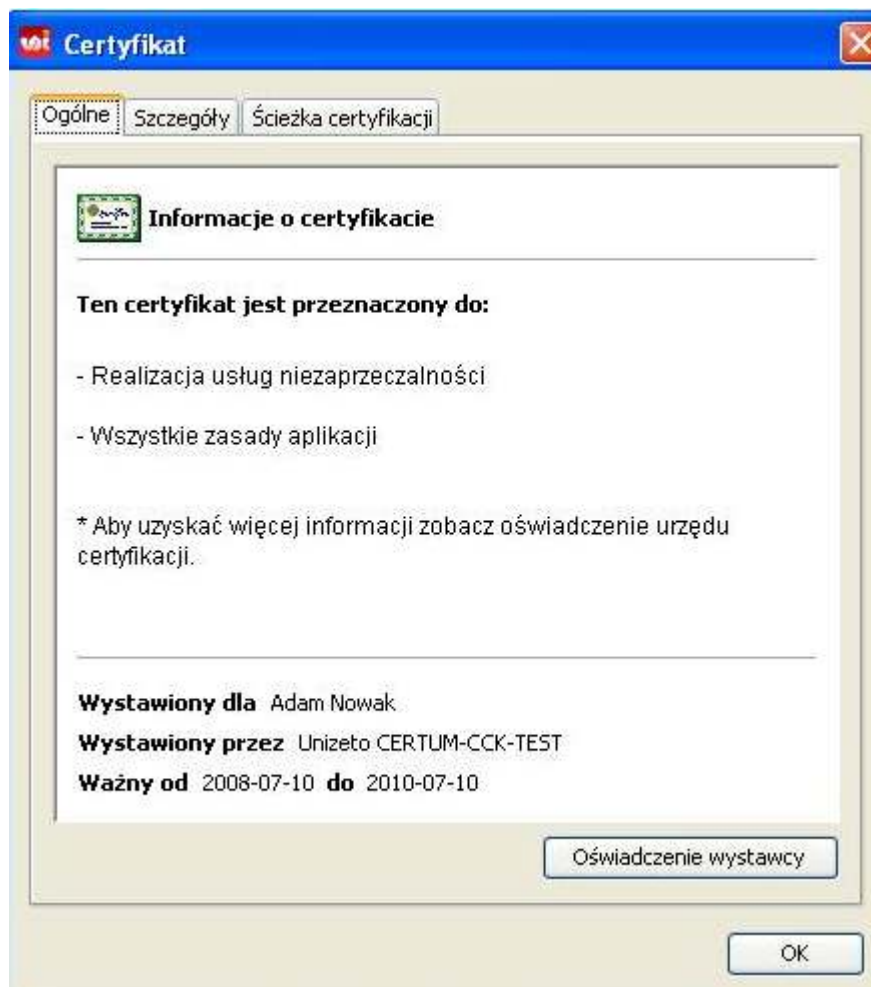
Oświadczenie o akceptacji certyfikatu:

- Akceptuje wydany certyfikat o numerze seryjnym XX XX XX na nazwisko Adam Nowak , który został wgrany na kartę kryptograficzną o numerze 1010101010101010
- Nie akceptuje wydanego certyfikatu o numerze seryjnym XX XX XX z powodu:

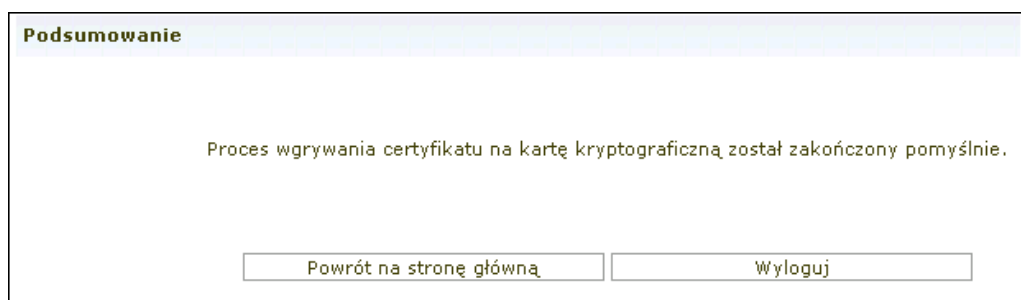
- Na samym początku, w celu zweryfikowania danych zawartych w certyfikacie, wciśnij przycisk „**Pokaż certyfikat**”.
- W oknie, które się następnie pojawi, zawarte zostaną wszystkie informacje dotyczące danego certyfikatu kwalifikowanego.

### **UWAGA!**

**Decyzja o akceptacji certyfikatu może być podjęta tylko jeden raz. Można ją zmienić tylko w przypadku wcześniejszego niezaakceptowania certyfikatu, klikając „Status certyfikatu” w oknie „Pobieranie certyfikatu kwalifikowanego”.**



- Jeżeli po weryfikacji dane zawarte w certyfikacie są poprawne, wciśnij przycisk „OK” oraz wybierz opcję „**Akceptuję wydany certyfikat o numerze seryjnym XXXXXX wydany na nazwisko XXXXX, który został wgrany na kartę kryptograficzną o numerze XXXXXXXXXXXXXXXXX**”.
- Jeżeli dane zawarte w certyfikacie zawierają błąd, wybierz opcję „**Nie akceptuję wydanego certyfikatu o numerze seryjnym XXXXXXX z powodu**”. W polu poniżej koniecznie podaj powód niez zaakceptowania certyfikatu kwalifikowanego.
- Zatwierdź zaznaczone oświadczenie klikając na przycisk „**Zakończ i zatwierdź oświadczenie**”.
- Po zatwierdzeniu oświadczenia wyświetla się **podsumowanie** z następującą informacją: „proces wgrывania certyfikatów na kartę kryptograficzną został zakończony pomyślnie”.



### 3.2 Zaawansowana instalacja certyfikatu kwalifikowanego

Poniższa procedura umożliwia ręczną instalację certyfikatu kwalifikowanego na karcie kryptograficznej przy użyciu oprogramowania proCertum CardManager. Jest to rozwiązanie przeznaczone dla tych z Państwa, u których z różnych powodów występują problemy z obsługą apletu JAVA, pojawia się konieczność instalacji w trybie offline.

Proces zaawansowanej instalacji certyfikatu kwalifikowanego składa się z:

1. pobrania certyfikatu kwalifikowanego,
2. pobrania kodu PUK,
3. wgrania certyfikatu kwalifikowanego na kartę kryptograficzną za pośrednictwem oprogramowania proCertum CardManager,
4. potwierdzenie Statusu Certyfikatu.

#### KROK 1 - Pobranie certyfikatu kwalifikowanego

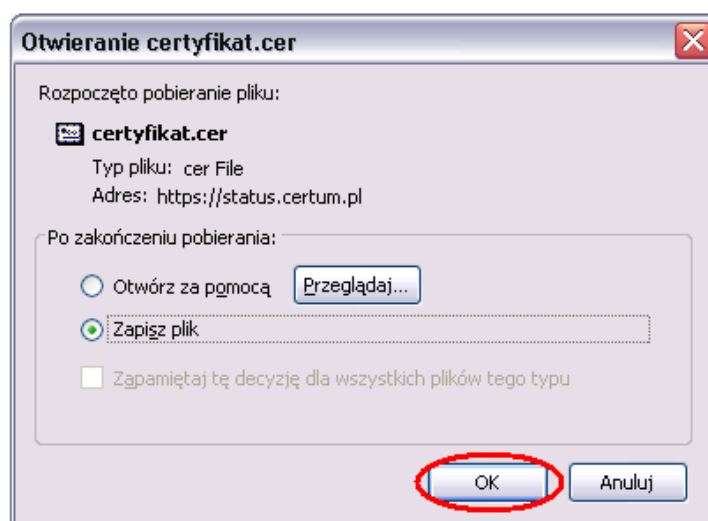
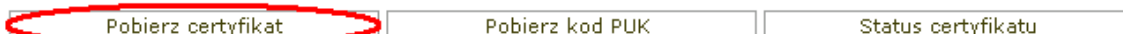
- Naciśnij przycisk **Pobierz certyfikat** i zapisz certyfikat w formacie .cer w dowolnej lokalizacji na stacji roboczej.

#### Zaawansowana instalacja certyfikatu (niestandardowa)

Poniższa procedura umożliwia przeprowadzenie ręcznej instalacji certyfikatu na karcie kryptograficznej przy wykorzystaniu oprogramowania proCertum CardManager. Jest to rozwiązanie przeznaczone dla tych z Państwa, u których z różnych powodów występują problemy z obsługą apletu JAVA lub istnieje konieczność przeprowadzenia instalacji w trybie offline.

W celu rozpoczęcia procedury należy

- wcisnąć przycisk **Pobierz certyfikat** i zapisać certyfikat (w formacie .cer) w dowolnej lokalizacji na stacji roboczej
- wcisnąć przycisk **Pobierz kod PUK** i zapisać uzyskany kod
- uruchomić oprogramowanie proCertum CardManager i postępować zgodnie z instrukcją instalacji certyfikatu.



**KROK 2 - Pobranie kodu PUK**

Kod PUK będzie potrzebny do ustalenia kodu PIN w oprogramowaniu proCertum CardManager.

- Aby pobrać kod PUK, wciśnij przycisk „Pobierz kod PUK”.

**Zaawansowana instalacja certyfikatu (niestandardowa)**

Poniższa procedura umożliwi przeprowadzenie ręcznej instalacji certyfikatu na karcie kryptograficznej przy wykorzystaniu oprogramowania proCertum CardManager. Jest to rozwiązanie przeznaczone dla tych z Państwa, u których z różnych powodów występują problemy z obsługą apletu JAVA lub istnieje konieczność przeprowadzenia instalacji w trybie offline.

W celu rozpoczęcia procedury należy

- wcisnąć przycisk **Pobierz certyfikat** i zapisać certyfikat (w formacie .cer) w dowolnej lokalizacji na stacji roboczej
- wcisnąć przycisk **Pobierz kod PUK** i zapisać uzyskany kod
- uruchomić oprogramowanie [proCertum CardManager](#) i postępować zgodnie z instrukcją instalacji certyfikatu.

Pobierz certyfikat	<b>Pobierz kod PUK</b>	Status certyfikatu
--------------------	------------------------	--------------------

- Jeżeli jesteś Obywatelą Polski, zostaniesz poproszony o wprowadzenie numeru PESEL oraz numeru karty kryptograficznej. Następnie naciśnij przycisk „Pokaż kody”.

**Pobieranie kodu PUK - Weryfikacja danych użytkownika**

PESEL  Pole wymagane  
 Numer karty  Pole wymagane

Pokaż kody	Powrót
------------	--------

- Jeżeli posiadasz niepolskie obywatelstwo, zostaniesz poproszony o wprowadzenie następujących danych: miejsce urodzenia oraz numer karty kryptograficznej.

**Pobieranie kodu PUK - Weryfikacja danych użytkownika**

Miejsce urodzenia (miejscowość)  Pole wymagane  
 Birth location  
 Numer karty  Pole wymagane  
 Card number

Pokaż kody	Powrót
------------	--------

- W następnym kroku, zapisz wyświetlony na ekranie kod PUK. Po zainstalowaniu certyfikatu należy, za pośrednictwem oprogramowania proCertum CardManager, ustawić nowy kod PUK, który należy przechowywać w miejscu niedostępnym dla osób trzecich.

- Kod PUK będzie potrzebny do odblokowania karty kryptograficznej w momencie, gdy zostanie ona zablokowana przez trzykrotne błędne wpisanie kodu PIN. W przypadku zablokowanie karty kryptograficznej skontaktuj się z naszą Infolinią.

**Pobieranie kodu PUK**

Kod PUK 11001100

Ilość wyświetleń kodu PUK 0

Data ostatniego wyświetlenia -

**"UWAGA !**

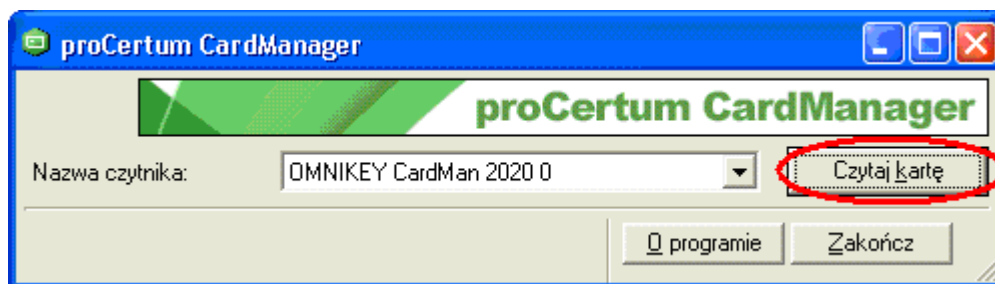
**Kod PUK należy zapisać i przechowywać w bezpiecznym miejscu, niedostępnym dla osób trzecich. Kod PUK będzie wymagany do ustanowienia kodu PIN przy wykorzystaniu aplikacji proCertum CardManager . "**

Po zainstalowaniu certyfikatu, należy ustanowić nowy kod PUK za pośrednictwem aplikacji proCertum CardManager. Kod PUK będzie potrzebny do odblokowania karty kryptograficznej w momencie gdy zostanie ona zablokowana poprzez trzykrotne błędne wpisanie kodu PIN.

Trzykrotne błędne wpisanie kodu PIN, a następnie trzykrotne błędne wpisanie kodu PUK trwale blokuje kartę i uniemożliwia dalsze z niej korzystanie.

**KROK 3 - Wgranie certyfikatu kwalifikowanego na kartę kryptograficzną**

1. Po zapisaniu certyfikatu w formacie .cer uruchom oprogramowanie proCertum CardManager i postępuj zgodnie z poniższą instrukcją instalacji certyfikatu. Należy używać najnowszej wersji oprogramowania znajdującej się na stronie [www.certum.pl](http://www.certum.pl).
2. W celu uruchomienia aplikacji z menu **Start** w zakładce z programami wybierz folder „Unizeto”, a następnie **proCertum CardManager**. Wyświetlone zostanie okno główne oprogramowania **proCertum CardManager**. Aby odczytać zawartość karty, naciśnij przycisk **Czytaj kartę**.



3. W trakcie pierwszego uruchomienia oprogramowania **proCertum CardManager** z nową kartą należy koniecznie nadać karcie nowy kod PIN. W tym celu naciśnij przycisk **Nowy PIN** w zakładce **Profil bezpieczny**.

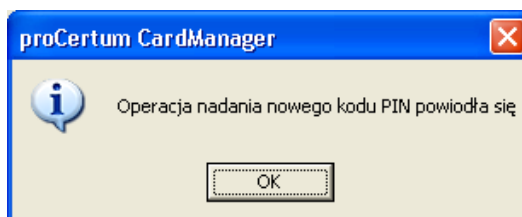
**UWAGA! W przypadku odnowienia certyfikatu na tej samej karcie należy pominąć poniższy podpunkt.**



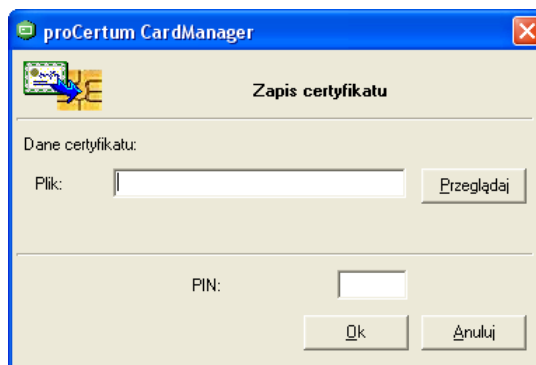
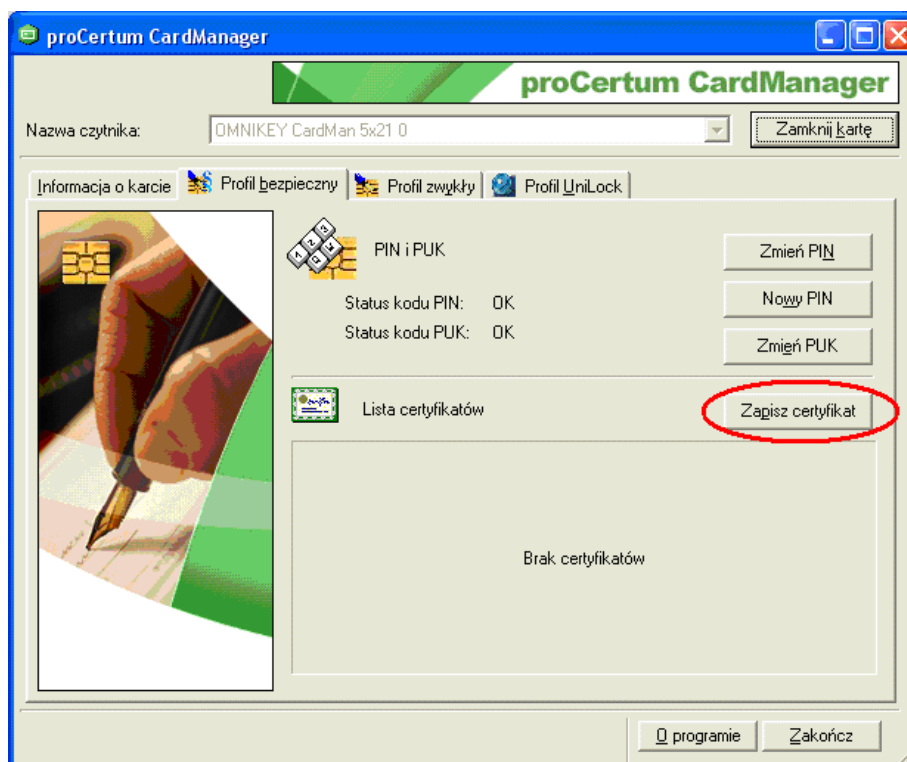
Aplikacja poprosi o podanie kodu PUK (sposób jego uzyskania opisany został w kroku 2 zaawansowanej instalacji certyfikatu kwalifikowanego) oraz ustalenie nowego kodu PIN.



Aby zatwierdzić wprowadzony PIN, naciśnij przycisk **Ok**. Wciśnięcie przycisku **Anuluj** spowoduje anulowanie nowego kodu PIN. Oprogramowanie **proCertum CardManager** potwierdzi poprawność dokonanych zmian.



4. Aby zapisać certyfikat kwalifikowany na karcie kryptograficznej, naciśnij przycisk **Zapisz certyfikat** w zakładce **Profil bezpieczny**. Pojawi się okno umożliwiające zapis certyfikatu do **Profilu bezpiecznego**.



5. Wskaż plik .cer z odpowiednim certyfikatem (sposób uzyskania pliku opisany został w kroku 1 zaawansowanej instalacji certyfikatu kwalifikowanego), a następnie podaj poprawny kod PIN. Naciśnięcie przycisku **OK** spowoduje wgranie certyfikatu na kartę kryptograficzną.

**UWAGA!**

**Certyfikat kwalifikowany jest przypisany wyłącznie do karty kryptograficznej, której numer podano we wniosku o wydanie certyfikatu. Należy zwrócić szczególną uwagę na to, aby certyfikat został zapisany na odpowiedniej karcie kryptograficznej.**

## KROK 4 - Potwierdzenie Statusu Certyfikatu

Ostatnim krokiem po zapisaniu certyfikatu na kartę kryptograficzną jest akceptacja certyfikatu.

Aby zaakceptować certyfikat kwalifikowany w zaawansowanej instalacji certyfikatu kwalifikowanego naciśnij przycisk „Status Certyfikatu”.

### Zaawansowana instalacja certyfikatu (niestandardowa)

Poniższa procedura umożliwia przeprowadzenie ręcznej instalacji certyfikatu na karcie kryptograficznej przy wykorzystaniu oprogramowania proCertum CardManager. Jest to rozwiązanie przeznaczone dla tych z Państwa, u których z różnych powodów występują problemy z obsługą apletu JAVA lub istnieje konieczność przeprowadzenia instalacji w trybie offline.

W celu rozpoczęcia procedury należy

- wcisnąć przycisk **Pobierz certyfikat** i zapisać certyfikat (w formacie .cer) w dowolnej lokalizacji na stacji roboczej
- wcisnąć przycisk **Pobierz kod PUK** i zapisać uzyskany kod
- uruchomić oprogramowanie proCertum CardManager i postępować zgodnie z instrukcją instalacji certyfikatu.



- Jeżeli dane zawarte w certyfikacie są poprawne, wybierz opcję „**Akceptuję certyfikat wydany na nazwisko XXXXX, który został wgrany na kartę kryptograficzną o numerze XXXXXXXXXXXXXXXXX.**”
- Jeżeli dane zawarte w certyfikacie zawierają błąd, wybierz opcję „**Nie akceptuję wydanego certyfikatu z powodu.**” W polu poniżej należy podać powód niezaakceptowania certyfikatu kwalifikowanego.
- Zatwierdź oświadczenia klikając na przycisk „**Zakończ i zatwierdź oświadczenia.**”

Po zatwierdzeniu oświadczenia wyświetla się **podsumowanie** z następującymi informacjami:

- jeżeli Subskrybent zaakceptował certyfikat.

**Status certyfikatu**

Certyfikat został zaakceptowany 2010-04-13 11:49:02 i decyzja ta nie może być zmieniona.

### UWAGA!

**Nie usuwaj certyfikatu kwalifikowanego przed jego odnowieniem.**

**W trakcie zapisywania nowego certyfikatu kwalifikowanego na kartę kryptograficzną, stary certyfikat zostanie automatycznie podmieniony na nowy bez twojej ingerencji.**

*Oprogramowanie zarządzające proCertum CardManager, zgodnie z Ustawą o podpisie elektronicznym z 18 września 2001r., umożliwia usunięcie z karty kryptograficznej certyfikatu kwalifikowanego wraz z przypisanymi do niego kluczami kryptograficznymi.*

**Operacja ta jest nieodwracalna.** Brak kluczy kryptograficznych na karcie uniemożliwia odnowienie certyfikatu kwalifikowanego i skutkuje koniecznością zakupu nowego certyfikatu kwalifikowanego lub nowej karty kryptograficznej.