



## Instrukcja – Certum Standard Code Signing

Aktywacja i instalacja certyfikatu Certum Standard Code Signing na kartę kryptograficzną

wersja 2.7



## Spis treści

1. Opis produktu.....	2
2. Instalacja oprogramowania.....	3
3. Elementy niezbędne przed rozpoczęciem aktywacji i instalacji certyfikatu Code Signing na kartę kryptograficzną.....	3
4. Proces aktywacji certyfikatu.....	4
4.1. Wymagania.....	4
4.2. Rozpoczęcie aktywacji certyfikatu.....	4
4.3. Aktywacja certyfikatu.....	6
<b>4.3.1. Generowanie pary kluczy</b> .....	7
4.4. Wypełnienie formularza przy aktywacji.....	9
5. Weryfikacja.....	11
5.1. Weryfikacja na podstawie dokumentów.....	11
5.2. Weryfikacja z AriadNEXT.....	12
6. Pobranie i wgranie certyfikatu na kartę.....	15

## 1. Opis produktu

Certyfikat Code Signing umożliwia cyfrowe podpisanie aplikacji, sterowników oraz programów, poświadczając ich autentyczność i bezpieczeństwo. Dzięki temu użytkownicy Twojego oprogramowania zyskują pewność, że nie zostało ono zmodyfikowane, zainfekowane lub uszkodzone przez osoby trzecie.

Uwierzytelnienie aplikacji z pomocą Code Signing eliminuje problem anonimowości kodu w sieci. Dzięki cyfrowemu podpisowi zyskasz pewność, że użytkownicy nie zobaczą ostrzeżenia o "nieznanym wydawcy" w trakcie instalacji lub uruchamiania Twojego programu i upewnią się o jego bezpieczeństwie.

Certyfikacja aplikacji pozwala chronić zarówno użytkowników, jak i reputację Twojej marki.

Cyfrowe podpisywanie kodu sprawia, że korzystanie z aplikacji jest w pełni bezpieczne, co przekłada się na większe zaufanie do Twojej marki i poszerzenie grona klientów.

Instrukcja opisuje ścieżkę aktywacji oraz instalacji certyfikatu Standard Code Signing.

## 2. Instalacja oprogramowania

Do poprawnego działania certyfikatu Code Signing potrzebna jest aplikacja proCertum CardManager. Najnowsza wersja oprogramowania jest do pobrania [TUTAJ](#).

Aby poprawnie zainstalować aplikację trzeba wykonać następujące kroki:

1. Pobierz najnowszą wersję oprogramowania z oficjalnej strony Certum.
2. Uruchom pobrany instalator.
3. Po uruchomieniu instalatora kliknij przycisk [Dalej](#).
4. Po pojawieniu kolejnego ekranu zaznacz [Akceptuję warunki umowy licencyjnej](#) i kliknij [Dalej](#).
5. Po pojawieniu się kolejnego ekranu wybierz ścieżkę, w której ma być zainstalowana aplikacja.
6. W następnym kroku kliknij na przycisk [Instaluj](#).
7. Na koniec instalacji uruchom ponownie komputer, zaznaczając [Tak, chcę teraz uruchomić ponownie komputer](#).

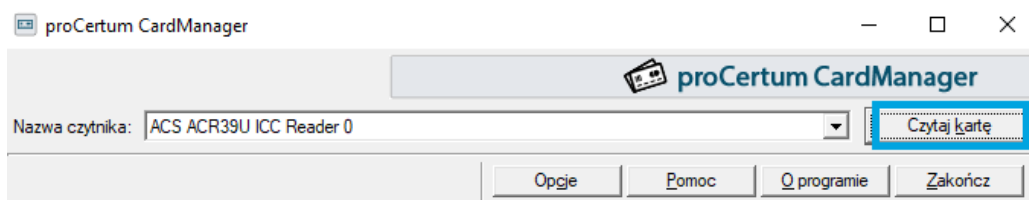
### UWAGA

Jeżeli po podłączeniu czytnika kart sterowniki nie zainstalują się automatycznie, należy je pobrać ze strony producenta [TUTAJ](#).

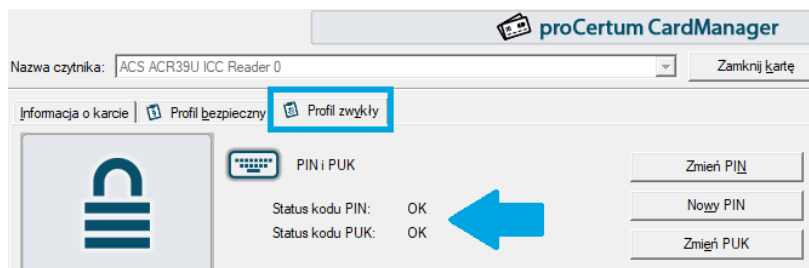
## 3. Elementy niezbędne przed rozpoczęciem aktywacji i instalacji certyfikatu Code Signing na kartę kryptograficzną

Aby wgrać certyfikat Code Signing na kartę kryptograficzną należy postępować zgodnie z poniższą instrukcją:

1. Uruchom oprogramowanie proCertum CardManager (aktualna wersja oprogramowania dostępna jest [TUTAJ](#)).
2. Jeżeli karta została odczytana pomyślnie powinno pojawić się okno jak na grafice poniżej:

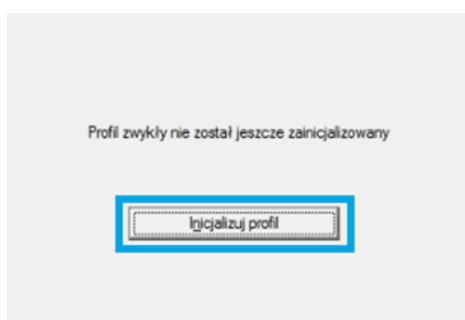


3. Przejdź do zakładki [Profil zwykły](#).
4. Sprawdź czy [Profil zwykły](#) jest aktywny - oprogramowanie wyświetli informacje na temat wybranego profilu oraz listę certyfikatów. Jeżeli nie jest aktywny przejdź do punktu nr 5. Profil jest aktywny jeżeli Status kodu **PIN** i **PUK** ma wartość **OK**.



5. Jeżeli **Profil zwykły** nie jest aktywny, naciśnij przycisk **Inicjalizuj profil**.

Karta procesorowa standardowo zawsze dostarczana jest z „niezainicjalizowanym” profilem zwykłym, tzn. nie zostały jeszcze dla niej nadane kody PUK i PIN. W celu aktywowania profilu, należy nacisnąć przycisk **Inicjalizuj profil**:



W następnym kroku pozostaje zdefiniować nowy kod PUK i nowy kod PIN. Użytkownik zostanie poproszony o potwierdzenie wprowadzonego kodu. Aby zatwierdzić zmiany należy nacisnąć przycisk OK. Po zainicjalizowaniu profilu jest on gotowy do użycia.

Po nadaniu kodu PIN i PUK użytkownik może przejść do aktywacji certyfikatu.

#### UWAGA

Kod PIN i PUK jest nadawany przez użytkownika, w przypadku utraty kodów lub ich zablokowania dostęp do usługi będzie niemożliwy. W tej sytuacji należy zakupić nową kartę kryptograficzną i przeprowadzić proces reissue – ponowne wydanie certyfikatu.

W celu zakupu nowej karty należy wejść na stronę: <https://sklep.certum.pl/zestaw-cryptocertum-mini.html> i wybrać wariant bez czytnika.

## 4. Proces aktywacji certyfikatu

### 4.1. Wymagania

Do instalacji certyfikatu będzie potrzebna aplikacja proCertum CardManager (opis instalacji i konfiguracji znajduje się powyżej) oraz czytnik z kartą kryptograficzną, na której zainicjowany jest profil zwykły, podpięty do komputera.

Instrukcja przygotowana jest na przykładzie przeglądarki Google Chrome.

### 4.2. Rozpoczęcie aktywacji certyfikatu

Po złożonym zamówieniu w sklepie Certum aktywacja dostępna będzie w zakładce **Aktywacja certyfikatów** (patrz rozdział 4.3).

Jeżeli chcesz aktywować produkt z otrzymanego np. na adres email kodu elektronicznego – przed rozpoczęciem

aktywacji kod dodaj w zakładce [Kody elektroniczne](#). W tym celu zaloguj się do konta na stronie <https://sklep.certum.pl>



Szukaj...



Pomoc

Konto ▾

Koszyk ▾



W przypadku gdy nie posiadasz konta kliknij na przycisk [Zakładam konto](#), dzięki temu utworzysz nowe konto. Jeżeli posiadasz już konto wybierz opcję [Zaloguj się](#).

## Logowanie

### Zarejestrowani klienci

[Zaloguj się](#)[Nie pamiętasz hasła?](#)

### Nowi klienci

Posiadanie konta ma wiele zalet. Szybszy proces składania zamówienia, możliwość zapisywania swoich adresów i śledzenie stanu zamówień to tylko niektóre z nich.

[Zakładam konto](#)

Po zalogowaniu kliknij na [Twoje konto](#) (na górze głównej strony).



Szukaj...



Pomoc

Aleksandra ... ▾

Koszyk ▾



PODPIS ELEKTRONICZNY ▾

BEZPIECZEŃSTWO DANYCH ▾

KARTY I CZYTNIKI ▾

SZKOLENIA ONLINE ▾

ROZWIĄZANI

Twoje konto

Wyloguj się

Aby dodać kod należy wybrać zakładkę [Kody elektroniczne](#). W polu [Nowy kod z karty aktywacyjnej](#) wpisz posiadany kod i kliknij [Dodaj](#).

**Uwaga!** Pamiętaj, że kod aktywacyjny składa się z 16 znaków. Po wpisaniu lub skopiowaniu kodu sprawdź czy ilość znaków się zgadza.

## Twoje konto

Twoje konto  
Zamówienia  
Produkty do pobrania  
Książka adresowa  
Dane konta  
**Kody elektroniczne**  
Subskrypcje newslettera  
Salda konta  
Karty zarejestrowane w Dotpay  
Archiwalne zamówienia  
Aktywacja certyfikatów  
Zarządzanie certyfikatami  
Narzędzia  
Weryfikacja domen

### Kody elektroniczne

Nowy kod z karty aktywacyjnej

Dodaj

### Twoje kody

Zakupione w sklepie

Wprowadzone ręcznie

Szukaj kodu



Wszystkie kody

Nie znaleziono kodów spełniających warunki.

Gdy poprawnie wprowadzisz kod, produkt pojawi się na liście w sekcji [Twoje kody/Wprowadzone ręcznie](#). Po przetworzeniu kodu przejdź do zakładki [Aktywacja Certyfikatów](#) (patrz kolejny punkt 4.3).

### 4.3. Aktywacja certyfikatu

Po złożonym zamówieniu lub dodaniu kodu do konta aktywację należy rozpocząć w zakładce [Aktywacja certyfikatów](#).

**Kody elektroniczne**

**Aktywacja certyfikatów**

Zarządzanie certyfikatami

Historia zamówień

Dane adresowe

Narzędzia

Weryfikacja domen

Newsletter

Wsparcie techniczne

Wiedza

### Aktywacja certyfikatów

Nazwa usługi

Status aktywacji

Numer zamówienia

Status płatności

**Szukaj**

Na liście wybierz certyfikat, który chcesz aktywować i kliknij przycisk [Aktywuj](#).

Nazwa usługi	Data zamówienia	Numer zamówienia	Status płatności
Standard Code Signing, 1 rok Wydanie	11 październik 2019	ZDRAPKA/Zyysa9PCNkyDooBG/11/10/19	Zaksięgowano
			Certyfikat nieaktywny <b>Aktywuj</b>

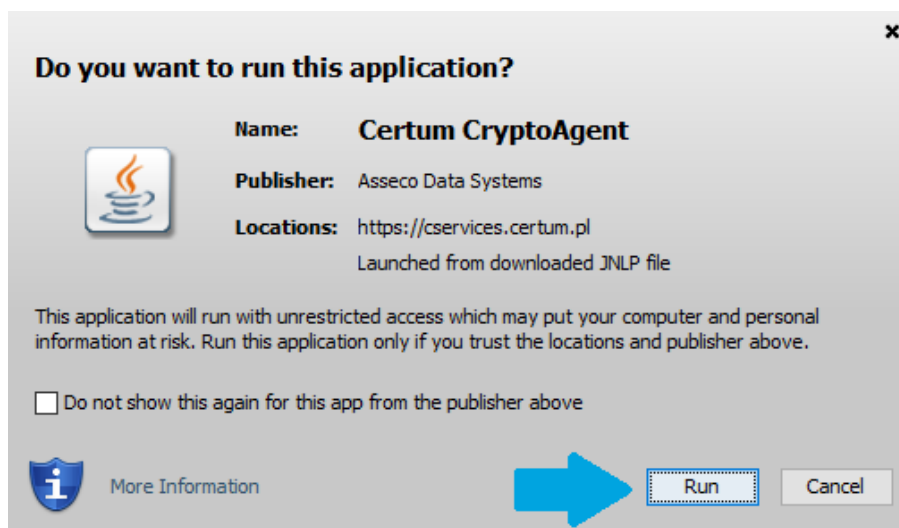
W celu wygenerowania certyfikatu Standard Code Signing należy wybrać metodę [Generowania pary kluczy](#) i kliknij na przycisk [Dalej](#).

#### 4.3.1. Generowanie pary kluczy

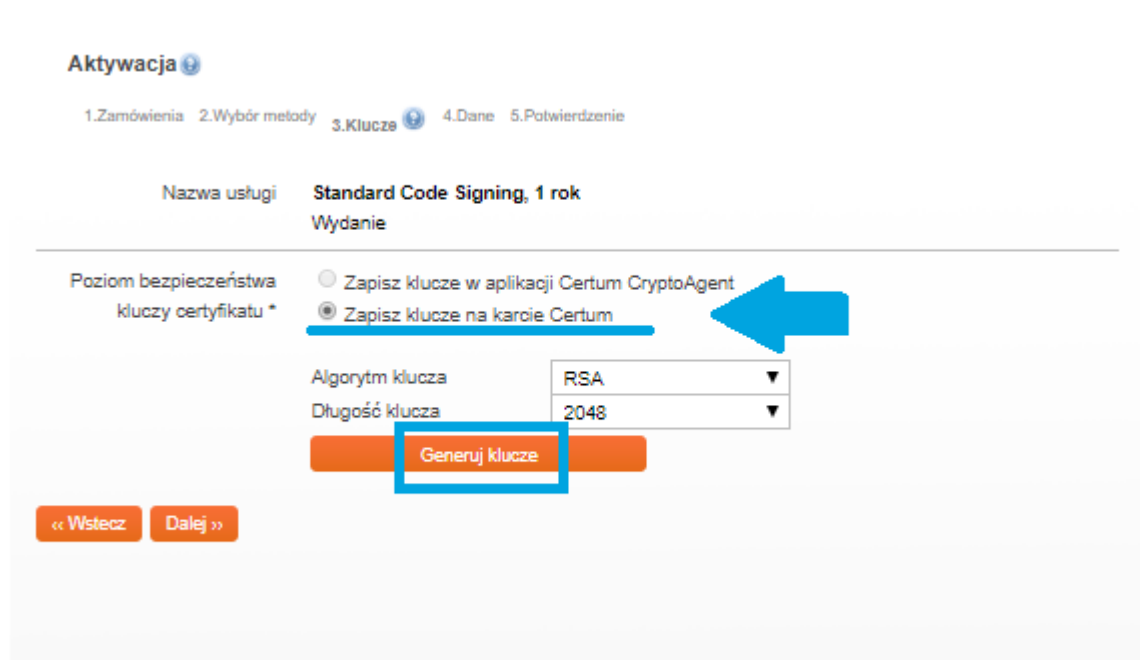
Uruchom aplikację [Certum CryptoAgent](#) (do uruchomienia aplikacji niezbędne jest zainstalowane na komputerze środowisko Java <https://www.java.com/pl/>).

Po kliknięciu na przycisk [Urunoć Aplikację CryptoAgent](#), na dolnym pasku przeglądarki pojawi się komunikat ostrzegawczy, przy którym kliknij na przycisk [Zachowaj](#) i uruchom pobraną aplikację [Certum](#).

Gdy pojawi się okno [Certum CryptoAgent](#) włącz aplikację klikając na [Run](#).

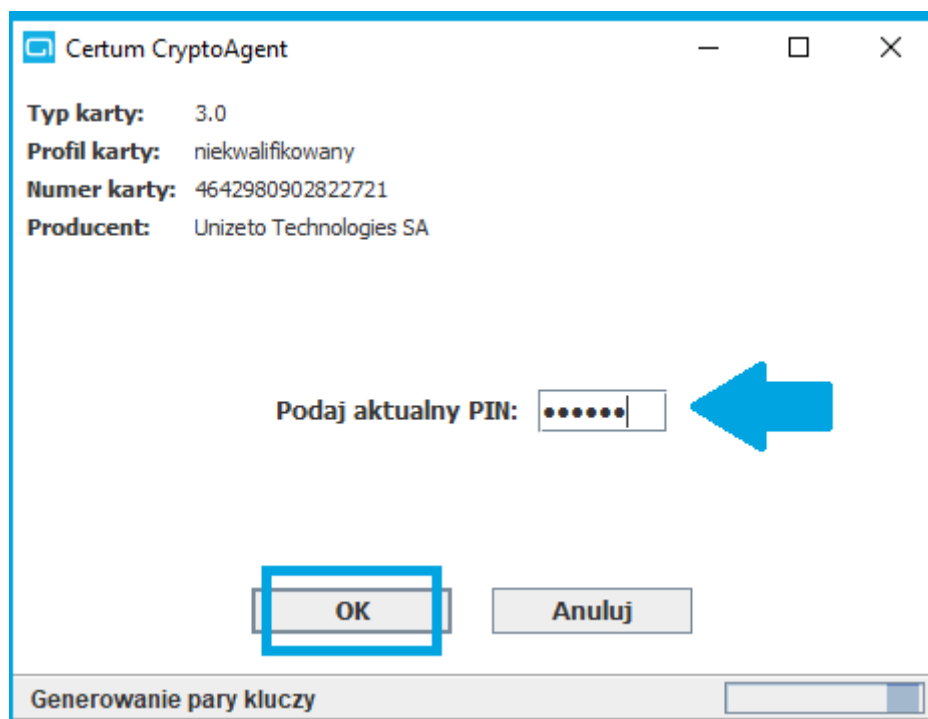


Po krótkiej chwili aplikacja uruchomi się w tle, a przy procesie aktywacji pojawi się możliwość [zapisania kluczy na karcie Certum](#).

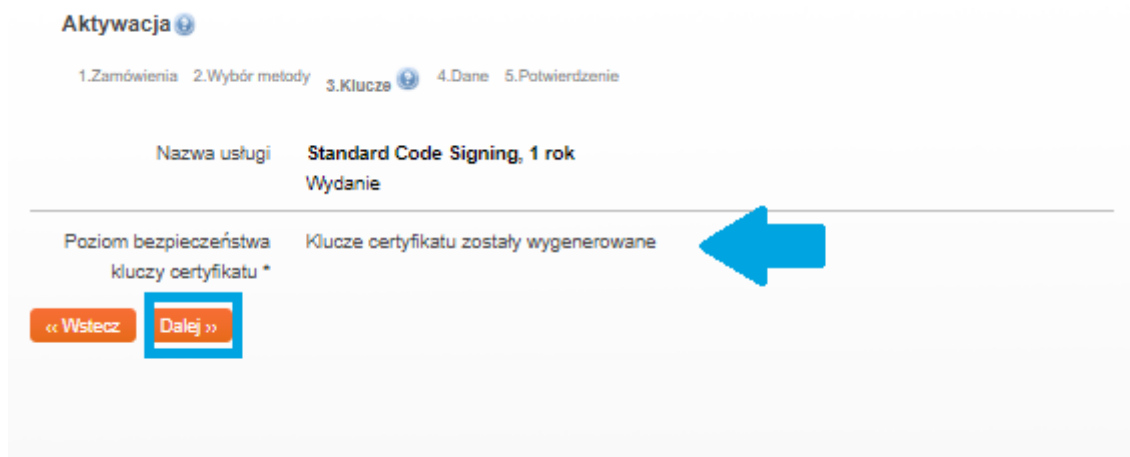


Gdy klikniesz na przycisk [Generuj klucze](#) wyświetli się komunikat, aby wpisać kod PIN nadany do profilu zwykłego na karcie kryptograficznej. Po wpisaniu kodu kliknij przycisk [OK](#).





Po przejściu do kolejnego ekranu z informacją o pomyślnym wygenerowaniu kluczy na karcie kliknij przycisk [Dalej](#), by móc przejść do wypełniania formularza przy aktywacji.



#### 4.4. Wypełnienie formularza przy aktywacji

Kolejnym krokiem jest uzupełnienie formularza wniosku certyfikacyjnego danymi, które zamieszczone zostaną w certyfikacie. Pamiętaj, że pola z gwiazdką są obowiązkowe.

**Dane do certyfikatu:**

Nazwa \* Asseco Data Systems S.A.

Funkcja skrótu RSA-SHA256

Koniec ważności certyfikatu

Rodzaj działalności \* jednostka podlegająca obowiązkowi wpisu do KRS

Organizacja \* Asseco Data Systems S.A.

Jednostka organizacyjna

Numer rejestrowy \* 0000421310

Ulica i numer domu

Miejscowość \* Gdynia

Kod pocztowy

Kraj \* Polska

Województwo

Miejsce rejestracji organizacji (miejscowość)

Miejsce rejestracji organizacji (kraj) \* Polska

Miejsce rejestracji organizacji (województwo)

\*Pole wymagane

Jeśli chcesz zachować pełen okres ważności certyfikatu, pozostaw to pole puste

W ostatnim kroku (Potwierdzeniu) sprawdź czy dane są poprawne, wybierz sposób weryfikacji, zaznacz wymagane akceptacje oraz potwierdzenia i kliknij przycisk **Aktywuj** na dole strony.

**⚠ Prosimy o dokładną weryfikację danych do certyfikatu. Po dokonaniu aktywacji usługi, zmiana danych nie będzie możliwa.**

#### Struktura certyfikatu: ⓘ

Podmiot CN=Asseco Data Systems S.A., O=Asseco Data Systems S.A., OU=Certum, L=Gdynia, C=PL

Wybierz sposób weryfikacji \*

Weryfikacja na podstawie dokumentów

Weryfikacja telefoniczna

numer

**⚠ Numer podany do weryfikacji telefonicznej certyfikowanej organizacji musi być zgodny z numerem telefonu dostępnym w kwalifikowanych źródłach informacji, czyli publicznych rejestrach przedsiębiorstw i organizacji. W przeciwnym razie weryfikacja zostanie przeprowadzona na podstawie dokumentów.**

#### Warunki Użytkowania

ZANIM ZŁOŻYSZ WNIOSEK O WYDANIE CERTYFIKATU, ZAAKCEPTUJESZ CERTYFIKAT BĄDŹ UŻYJESZ GO PROSIMY ABYŚ PRZECZYTAŁ NINIEJSZE „WARUNKI UŻYTKOWANIA CERTYFIKATÓW NIEKWALIFIKOWANYCH” ZWANE DALEJ „WARUNKAMI UŻYTKOWANIA”. JEŚLI NIE ZGADZASZ SIĘ Z WARUNKAMI UŻYTKOWANIA, NIE SKŁADAJ WNIOSKU O WYDANIE CERTYFIKATU, NIE AKCEPTUJ CERTYFIKATU I NIE UŻYWAJ GO.

NINIEJSZE WARUNKI UŻYTKOWANIA OBOWIĄZUJĄ OD MOMENTU PRZESŁANIA PRZEZ CIEBIE DO „CERTUM – POWSZECHNEGO CENTRUM CERTYFIKACJI” ZWANEGO DALEJ „CERTUM PCC” WNIOSKU CERTYFIKACYJNEGO DO ZAKOŃCZENIA OKRESU WAŻNOŚCI LUB UNIEWAŻNIENIA OTRZYMANEGO CERTYFIKATU. PRZEDKŁADAJĄC WNIOSEK O WYDANIE CERTYFIKATU ŻĄDASZ OD ORGANU WYDAJĄCEGO CERTYFIKATY ROZPATRZENIA GO I

- Akceptuję Warunki Użytkowania \*
- Oświadczam i potwierdzam, że jest mi wiadome, że certyfikat może uwidocznić moje dane osobowe w takim zakresie w jakim zostały one wskazane do umieszczenia w treści certyfikatu. Potwierdzam nadto, że wszelkie dane dotyczące czynności dokonanych przy użyciu tego certyfikatu mogą być, zgodnie z moją decyzją, dostępne bez ograniczenia uwzględniając w szczególności dane o lokalizacji. Na użycie certyfikatu nie ma wpływu Asseco Data Systems S.A., dostawca usług bezpieczeństwa. \*
- Potwierdzam że jestem osobą pełnoletnią \*
- Niniejszym potwierdzam zgodność z prawdą moich danych osobowych zawartych we wniosku o wydanie certyfikatu. \*

« Wstecz

Aktywuj

\*Pole wymagane

## 5. Weryfikacja

W zależności, który sposób weryfikacji wybrano, na **maila przyjdzie instrukcja związana z weryfikacją**.

**Uwaga:** Jeżeli w danych do certyfikatu został wpisany adres email (w kroku 4) to po przejściu przez aktywację na maila przyjdzie wiadomość uwierzytelniająca. Jednym z warunków wydania certyfikatu będzie kliknięcie w przesłany link weryfikacyjny.

### 5.1. Weryfikacja na podstawie dokumentów

Wydanie certyfikatu Standard Code Signing wymaga weryfikacji tożsamości Subskrybenta/Organizacji. W tym celu osoba wnioskująca o certyfikat powinna dostarczyć do [Certum](#) następujące dokumenty:

Weryfikacja tożsamości osoby prywatnej występującej o certyfikat we własnym imieniu

- potwierdzenie tożsamości w Punkcie Rejestracji lub Punkcie Potwierdzenia Tożsamości (szczegóły: [https://www.certum.pl/certum/cert.kontakt\\_punkty\\_rejestracji.xml](https://www.certum.pl/certum/cert.kontakt_punkty_rejestracji.xml)) lub

- notarialne potwierdzenie tożsamości lub w celu szybszego wydania
- kopia dokumentu tożsamości osoby zamawiającej (dowód osobisty, paszport, prawo jazdy, karta stałego pobytu). Kopia powinna być kompletnie odwzorowanym dokumentem (obie strony).

Tożsamość potwierdzić również można na podstawie ważnego certyfikatu kwalifikowanego wydanego dla Subskrybenta przez [Certum](#).

Weryfikacja tożsamości osoby występującej o certyfikat w imieniu organizacji:

1.

- potwierdzenie tożsamości w Punkcie Rejestracji lub Punkcie Potwierdzania Tożsamości (szczegóły: <https://sklep.certum.pl/partnersmap/>) lub
- notarialne potwierdzenie tożsamości lub w celu szybszego wydania
- kopia dokumentu tożsamości osoby zamawiającej (dowód osobisty, paszport, prawo jazdy, karta stałego pobytu). Kopia powinna być kompletnie odwzorowanym dokumentem (obie strony).

Tożsamość potwierdzić również można na podstawie ważnego certyfikatu kwalifikowanego wydanego dla Subskrybenta przez [Certum](#).

oraz

2. pełnomocnictwo lub upoważnienie potwierdzające związek osoby zamawiającej certyfikat z organizacją – wówczas, gdy zamawiający nie widnieje w odpowiednim rejestrze jako osoba upoważniona do reprezentacji firmy,
3. dokument rejestrowy firmy – wówczas, gdy firma nie widnieje w rejestrze KRS/GUS/CEiDG

W uzasadnionych przypadkach, zespół [Certum](#) może poprosić o dostanie dodatkowych dokumentów niezbędnych do prawidłowej weryfikacji.

Wszystkie zebrane dokumenty prosimy wysłać do [Certum](#) na jeden z poniższych sposobów:

- e-mailem w formie pliku zabezpieczonego hasłem na adres: [ccp@certum.pl](mailto:ccp@certum.pl) (forma zalecana), w celu ustalenia sposobu przekazania hasła prosimy o kontakt z infolinią wsparcia technicznego,
- faxem na numer fax: +48 91 4257 422
- pocztą na adres:

**Certum**  
**ul. Bajeczna 13**  
**71-838 Szczecin**

## 5.2. Weryfikacja z AriadNEXT

Automatyczna weryfikacja tożsamości to jedna z trzech metod, jakie Certum udostępnia klientom celem potwierdzenia tożsamości Wnioskodawcy o certyfikaty zawierające dane osobowe. Pozwala na szybkie sprawdzenie autentyczności dokumentów tożsamości oraz potwierdzenia, że Wnioskodawca

jest ich właścicielem. Cały proces odbywa się z poziomu komputera lub innego urządzenia z dostępem do kamery, z poziomu bezobsługowego interfejsu. W trakcie skanowania Dane dokumentu są automatycznie wyodrębniane i analizowane oraz porównywane z twarzą Właściciela. Proces opiera się na porównaniu zdjęcia twarzy ze zdjęciem wyodrębnionym z dokumentu tożsamości. Dzięki rozwiązaniu biometrycznemu pozwala zagwarantować, że Użytkownik jest obecny w trakcie potwierdzenia tożsamości. Cały proces odbywa się na żywo, w czasie rzeczywistym i nie wymaga wysłania dokumentów, są one jedynie skanowane w trakcie procesu celem wyodrębnienia potrzebnych do weryfikacji danych, a następnie usuwane. Cały proces trwa około 60 sekund.

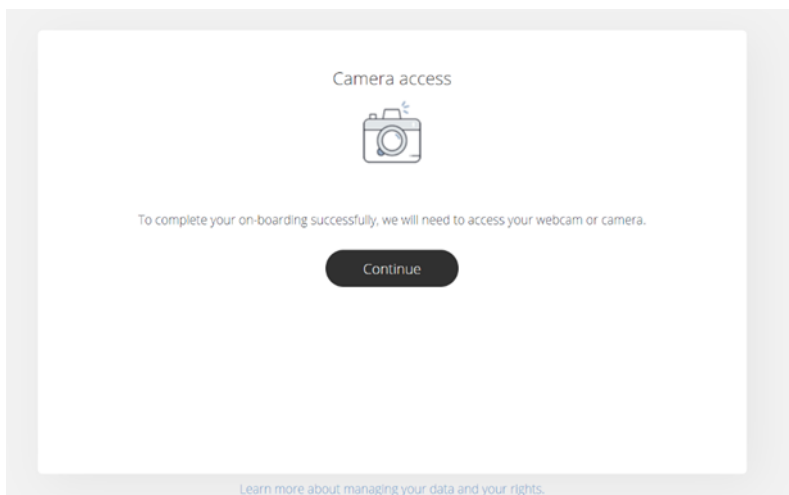
Jak wygląda proces w trakcie aktywacji certyfikatu?

- W procesie aktywacji certyfikatu, podczas wyboru metody weryfikacji tożsamości, należy wybrać metodę: **Automatyczna weryfikacja tożsamości**
- Po złożeniu wniosku Użytkownik otrzymuje unikalny link na wskazany adres e-mail
- Po kliknięciu w link Użytkownik zostanie przeniesiony na ekran Certum, z poziomu którego generuje proces Automatycznej Weryfikacji. Następnie Użytkownik otrzyma linka, który inicjuje weryfikację.
- W zależności od urzędowania, na jakim wykonywana jest weryfikacja proces przebiega inaczej.

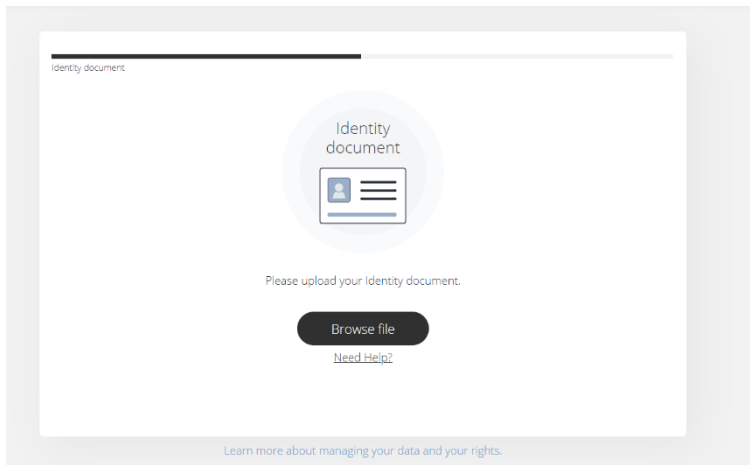
#### 5.2.1. Weryfikacja z poziomu komputera

### Krok 1 – Weryfikacja dokumentu

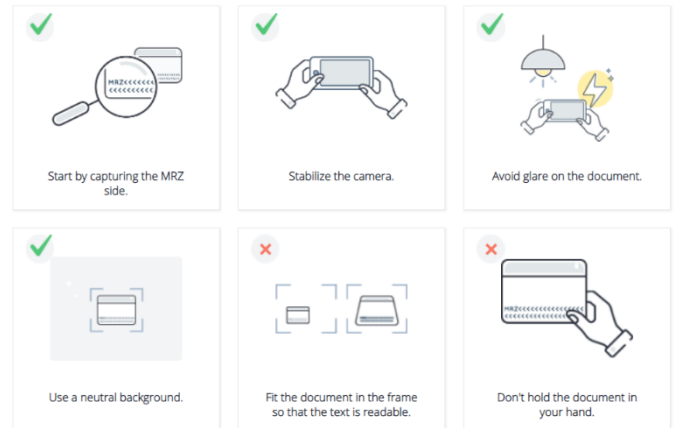
Po wejściu na linka inicjującego weryfikację, zostaniesz poinformowany o konieczności włączenia kamery na czas weryfikacji tożsamości. Kliknij Continue i przejdź do następnego kroku.



Następnie zostaniesz poproszony o wgranie zdjęcia Twojego dokumentu tożsamości. Dostarczone zdjęcie powinno zostać wykonane zgodnie ze wskazówkami dostępnymi podczas procesu.



How to take a good picture of a document.

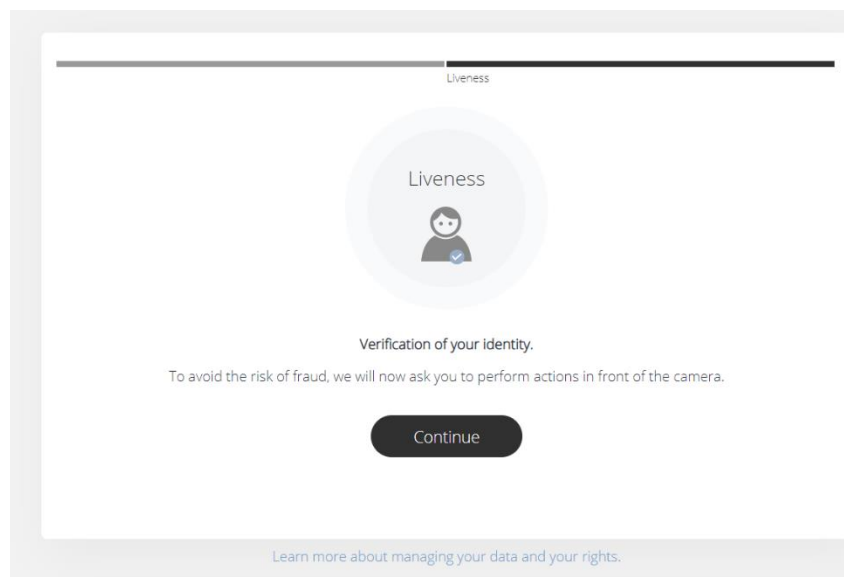


I understand

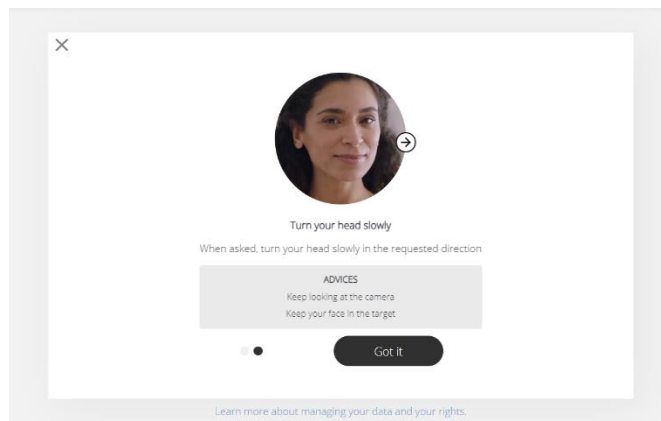
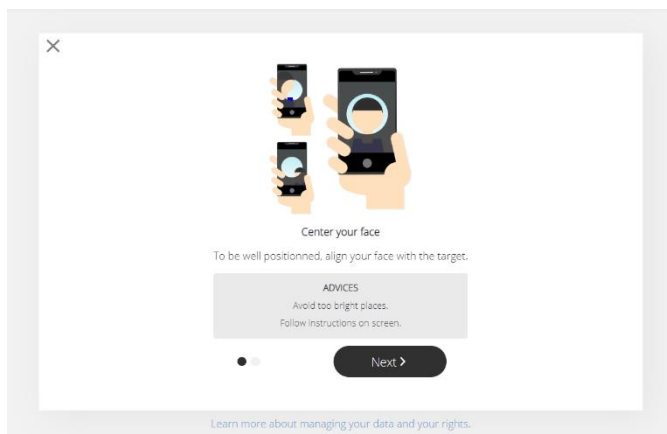
Po dostarczeniu danych system przez około 12 sekund będzie je procesował, celem wyodrębnienia danych z dokumentu. Po tym procesie zdjęcie dokumentu zostanie usunięte.

## Krok 2 - Porównanie twarzy

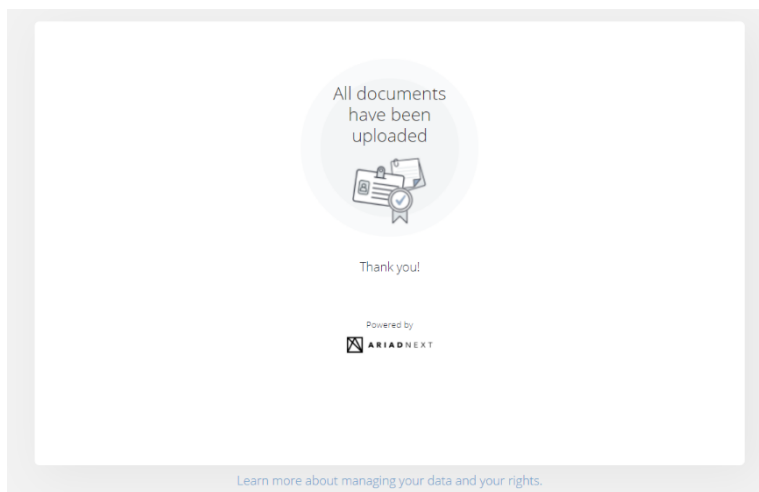
Podczas tego kroku zostaniesz poproszony o wykonanie ruchu twarzą przed kamerą. To rozwiązanie biometryczne pozwala zagwarantować, że Użytkownik jest obecny w trakcie potwierdzenia tożsamości oraz jest osobą z dokumentu.



Wykonanie tego kroku wymaga nakierowania twarzy na środek kamery, a następnie wykonania ruchu głowy w kierunku prawej strony, patrząc cały czas na kamerę.



Po wykonaniu tego kroku zobaczysz ekran informujący, że weryfikacja przebiegła pomyślnie. Wkrótce zostanie wydany Twój certyfikat.



### 5.2.2. Weryfikacja z poziomego telefonu

Weryfikacja przebiega podobnie, jednak w kroku pierwszy użytkownik nie dostarcza gotowego zdjęcia a wykonuje je na żywo w procesie.

**Uwaga!** W przypadku złożenia zamówienia przez przelew tradycyjny do wydania certyfikatu niezbędne jest również zaksięgowanie wpłaty.

## 6. Pobranie i wgranie certyfikatu na kartę

Po przejściu całego procesu aktywacji, należy wgrać certyfikat na karcie na której były uprzednio generowane klucze. W tym celu należy:

1. W sklepie Certum, przejdź do zakładki **Zarządzanie certyfikatami**:

Strona główna » Moje konto » Zarządzanie certyfikatami

Kody elektroniczne

Aktywacja certyfikatów

**Zarządzanie certyfikatami**

Historia zamówień

Dane adresowe

Narzędzia

Weryfikacja domen

Newsletter

Wsparcie techniczne

Wiedza

O Certum

### Zarządzanie certyfikatami

Profil certyfikatu

Nazwa

Email

Numer seryjny

Uzyska ważność po

Straci ważność przed

**Szukaj**

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r. (zwanego dalej „Rozporządzenie”) informuję, iż:

- Administratorem Pana/Pani danych osobowych jest Asseco Data Systems S.A. z siedzibą w Gdyni, ul. Podolska 21, 81-321 Gdynia;
- Kontakt do Inspektora ochrony danych w Asseco Data Systems S.A. można uzyskać pod adresem e - mail: [IOD@asseccods.pl](mailto:IOD@asseccods.pl), tel.+48 42 676 63 80.
- Pana/Pani dane osobowe przetwarzane będą w celu niezbędnym do wykonania umowy o certyfikat niekwalifikowany na podstawie art. 6 ust. 1 lit. b Rozporządzenia.

Nr seryjny	<a href="#">Profil certyfikatu</a>	Email	Nazwa	<a href="#">Ważny od</a>	<a href="#">Ważny do</a>	Status
------------	------------------------------------	-------	-------	--------------------------	--------------------------	--------

2. Odszukaj odpowiedni certyfikat, do którego generowana była para kluczy i kliknąć w niego:

Nr seryjny	<a href="#">Profil certyfikatu</a>	Email	Nazwa	<a href="#">Ważny od</a>	<a href="#">Ważny do</a>	Status
45de8eb75e 8398bb912d a4614f2727 9b	Standard Code Signing		Asseco Data Systems S.A.	31 październik 2019 11:37:50	30 październik 2020 11:37:50	✔ Ważny


3. Kliknij przycisk [Zapisz binarnie](#):

Nr seryjny	<a href="#">Profil certyfikatu</a>	Email	Nazwa	<a href="#">Ważny od</a>	<a href="#">Ważny do</a>	Status
45de8eb75e 8398bb912d a4614f2727 9b	Standard Code Signing		Asseco Data Systems S.A.	31 październik 2019 11:37:50	30 październik 2020 11:37:50	✔ Ważny

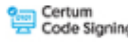
**Funkcja skrótu** RSA-SHA256

**Nazwa** Asseco Data Systems S.A.

**Organizacja** Asseco Data Systems S.A.



Certum Standard  
Code Signing



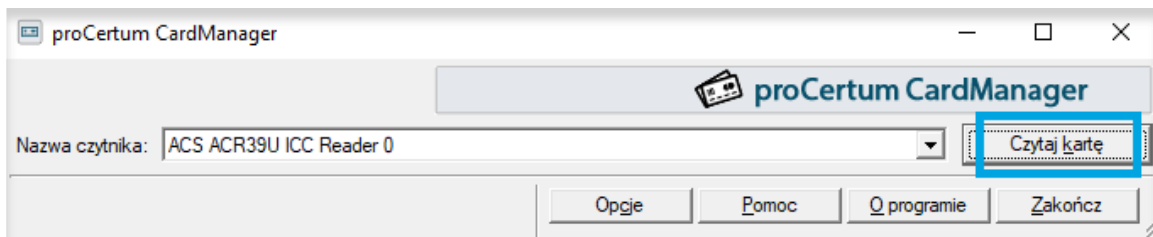
Certum  
Code Signing

[Unieważnij](#)
[Zainstaluj online](#)
[Odnów](#)

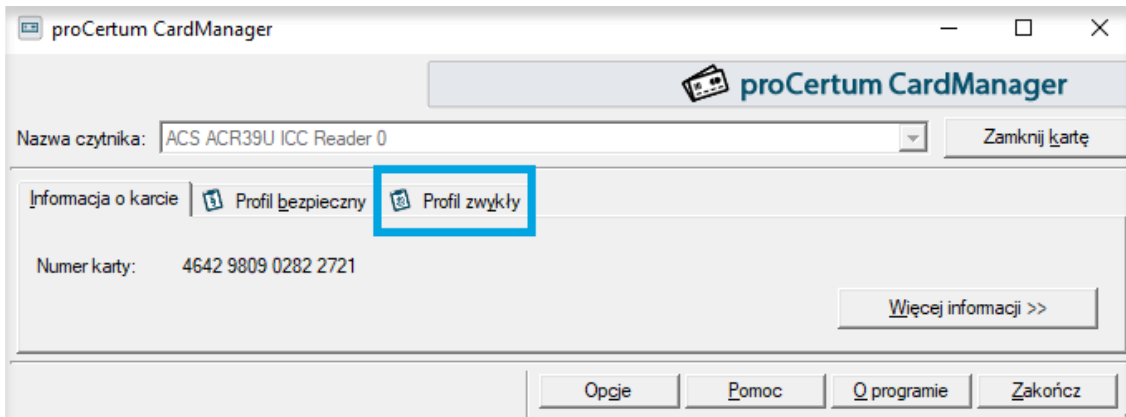
[Zapisz binarnie](#)
[Zapisz tekstowo](#)
[Reissue](#)

4. Pobierz plik certyfikatu na dysk komputera.
5. Otwórz program [proCertum CardManager](#):

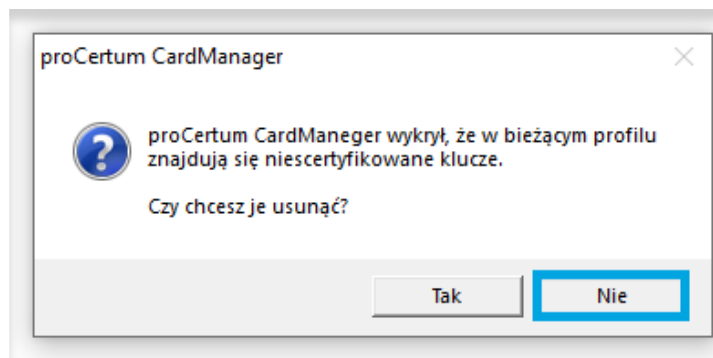




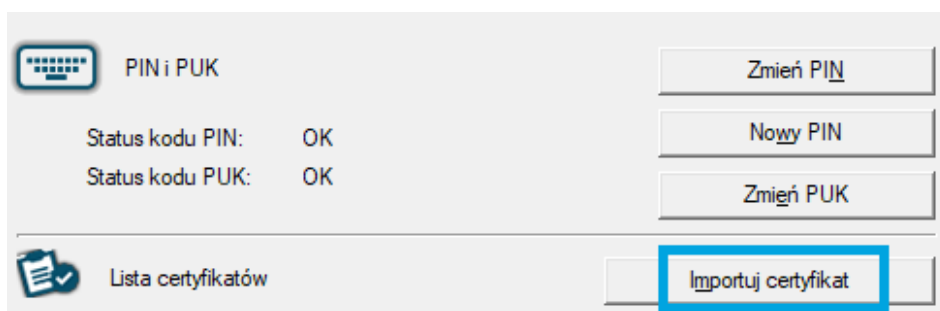
6. Przejdź do zakładki **Profil zwykły**:



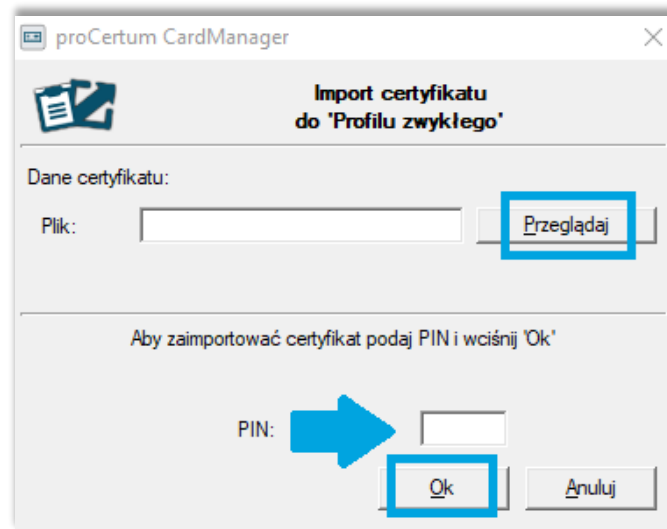
7. W przypadku pojawienia się powiadomienia o niecertyfikowanych kluczach na karcie wciśnij przycisk **Nie**:



8. Kliknij przycisk **Importuj certyfikat**:



9. Wybierz pobrany uprzednio plik certyfikatu, podaj pin do karty (do Profilu zwykłego):



10. Jeżeli proces dodawania certyfikatu zakończył się pomyślnie, na liście powinien ukazać się certyfikat Code Signing:

