

# Aktywacja certyfikatu EV Code Signing na karcie kryptograficznej

Wer. 3.1

**assecO**

 **Certum**  
by assecO

## Spis treści

1. Opis produktu .....	3
2. Aktywacja certyfikatu .....	3
Krok Weryfikacja danych .....	4
Krok Aktywacja certyfikatu.....	9

## 1. Opis produktu

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

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

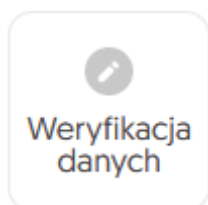
Cyfrowe podpisywanie kodu sprawia, że korzystanie z aplikacji jest bezpieczne, co przekłada się na większe zaufanie do Twojej marki i poszerzenie grona klientów.

## 2. Aktywacja certyfikatu

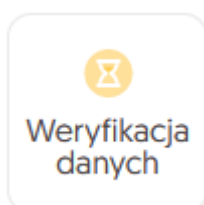
Rozpoczęcie procesu aktywacji będzie możliwe z poziomu **Twojego konta** w sklepie, w zakładce **Produkty bezpieczeństwa**. Proces składa się z kilku kroków:

- **Weryfikacja danych** – podanie danych subskrybenta i organizacji oraz ich weryfikacja
- **Aktywacja certyfikatu** – wygenerowanie kluczy, wybór pól do certyfikatu i przekazanie go do wydania.

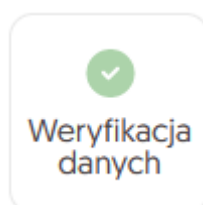
Każdy z kroków w miarę postępu aktywacji będzie przechodził przez kolejne statusy:



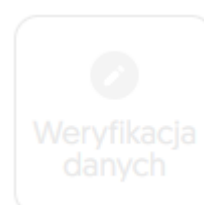
Krok oczekuje na podanie danych



Podano dane, dane oczekują na zakończenie weryfikacji



Dane zostały zweryfikowane



Podanie danych jest jeszcze niedostępne

## Krok Weryfikacja danych

Podanie danych do weryfikacji to krok, w którym podasz dane organizacji, dla której będzie wydany certyfikat, dane subskrybenta (osoby która reprezentuje organizację i będzie właścicielem certyfikatu) oraz dane upoważnienia subskrybenta do reprezentowania organizacji. Spośród podanych tu danych będzie możliwy w ostatnim kroku aktywacji certyfikatu wybór danych do certyfikatu.

Listę obsługiwanych dokumentów potwierdzających znajdziesz w [Informacje o wymaganych dokumentach](#).

Rozpoczęcie podawania danych do weryfikacji możesz poprzez **Dashboard**, wybierając opcję **Weryfikacja danych**:

The screenshot shows the Certum dashboard interface. On the left is a navigation menu with items: Dashboard, Certyfikaty, Domeny, Wyszukiwarka certyfikatów, and Sklep Certum. The main content area is divided into several sections:

- Cześć**: A greeting message and a Certum logo.
- Powiadomienia**: A notification section with tabs for 'Informacje', 'Problemy', 'Wygasające certyfikaty', and 'Nowe certyfikaty [1]'. It contains a message: 'Nie znaleziono zadań spełniających kryteria.' with a box icon.
- Przydatne informacje**: A section with a lightbulb icon and text explaining the activation process.
- Przydatne linki**: A list of links including 'Automatyczna weryfikacja subskrybenta', 'Pomoc, wymagane dokumenty', 'Generator CSR, PFX', and 'Nasze produkty'.
- Code Signing**: A section for a specific certificate with order number 'ORDER\_0000023456/pol8'. It features two buttons: 'Weryfikacja danych' (highlighted with a red box) and 'Aktywacja certyfikatu'. Below the buttons are fields for 'Alias', 'Produkt' (EV Code Signing 365 dni - wydanie), 'Status' (Wymagana aktywacja), 'Common name', and 'Data końca ważności certyfikatu'. A 'Szczegóły certyfikatu' link is at the bottom.

lub z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz przy danych subskrybenta opcję **Wypełnij dane**:

The screenshot shows the Certum dashboard interface. On the left is a navigation menu with items: Dashboard, Certyfikaty, Domeny, Wyszukiwarka certyfikatów, and Sklep Certum. The main content area is titled 'Certyfikat dla zamówienia ORDER/0000123456/po48'. Below the title are two main sections: 'Dane subskrybenta' and 'Dane organizacji'. The 'Dane subskrybenta' section shows a status 'Oczekuje na dane' and a blue button labeled 'Wypełnij dane' which is highlighted with a red rectangular box. To the right, there is a 'Szczegóły' section with a list of product details: 'Kategoria produktu: Code Signing', 'Produkt: EV Code Signing 365 dni - wydanie', and 'Data złożenia zamówienia'.

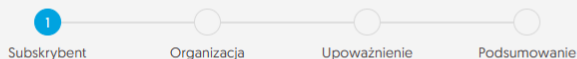
Kreator przeprowadzi Cię przez proces podawania danych. W jego pierwszym etapie wybierz podanie nowych danych. W przyszłości będzie możliwość ich użycia do wydania kolejnego certyfikatu.

The screenshot shows the 'Dane do weryfikacji' step in the Certum dashboard. The main heading is 'Dane do weryfikacji' with a circular icon containing a document and a checkmark. Below the heading is a paragraph: 'Wybierz jeden ze zweryfikowanych zestawów danych lub wprowadź nowe do weryfikacji. Spośród wskazanych danych, w kroku aktywacji certyfikatu będziesz miał możliwość wybrania danych do certyfikatu.' There are two radio button options: 'Podaj nowe dane' (which is selected) and another unselected option. A blue 'Kontynuuj' button is located at the bottom right of the main content area.

W kolejnym etapie podaj dane subskrybenta, czyli osoby, która reprezentuje organizację i będzie właścicielem certyfikatu. Imiona i nazwiska zapisz w formularzu tak, jak widnieją na dokumencie tożsamości subskrybenta.

Wybierz również metodę weryfikacji tożsamości subskrybenta spośród dostępnych:

- **Automatyczna weryfikacja tożsamości** – subskrybent otrzyma e-mail z linkiem do serwisu weryfikacji tożsamości z użyciem kamery komputera lub telefonu i dokumentu tożsamości
- **Załączenie dokumentu** – dodasz skan dokumentu tożsamości subskrybenta lub skan potwierdzenia tożsamości.



## Dane subskrybenta

Subskrybent to osoba, która będzie właścicielem certyfikatu: dane jej lub organizacji którą może reprezentować, będą dostępne do wyboru jako dane do certyfikatu. Po zapisaniu danych, subskrybent zostanie poproszony o weryfikację swojej tożsamości z użyciem **dokumentu tożsamości** jedną z dostępnych metod weryfikacji.

IMIĘ\*

Jan

NAZWISKO\*

Kowalski

### Metoda weryfikacji

Automatyczna weryfikacja tożsamości     Załączenie dokumentu do weryfikacji subskrybenta

ADRES E-MAIL SUBSKRYBENTA\*

jankowalski@twojafirma.pl

W przypadku **automatycznej weryfikacji tożsamości**, na podany tu adres e-mail subskrybent otrzyma link oraz instrukcję do rozpoczęcia procesu. Link zostanie wysłany po zapisaniu danych do weryfikacji.

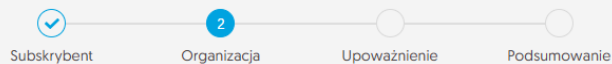
[Cofnij](#)

[Kontynuuj](#)

Po wypełnieniu powyższych danych, przejdź do kolejnego etapu czyli podania danych organizacji. W tym miejscu podaj dane organizacji oraz adres jej siedziby. Dane posłużą do zweryfikowania istnienia organizacji.

W tym miejscu wybierz również w jaki sposób Certum zweryfikuje istnienie organizacji:

- **Wskazanie rejestru** – Certum wyszuka po podanym numerze informacji o organizacji w publicznym rejestrze
- **Załączenie dokumentu** – dodasz dokument potwierdzający założenie organizacji.



## Dane organizacji

Wprowadź dane organizacji do weryfikacji jej istnienia. Spośród wskazanych danych, w kroku aktywacji certyfikatu będziesz miał możliwość wybrania danych do certyfikatu.

### Dane organizacji

ORGANIZACJA\*

Twoja firma

RODZAJ DZIAŁALNOŚCI\*

Prywatna

NUMER REJESTROWY\*

12345678

### Siedziba organizacji

KRAJ\*

Polska [PL]

WOJEWÓDZTWO\*

mazowieckie

MIEJSCOWOŚĆ\*

Warszawa

Po wypełnieniu wszystkich wymaganych danych, przejdź do ostatniego etapu kroku podawania danych do weryfikacji, czyli do określenia sposobu weryfikacji upoważnienia subskrybenta do reprezentowania organizacji.

Do wyboru są dwie metody:

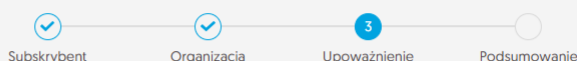
- **Subskrybent widnieje w rejestrze** – osoba podana jako subskrybent widnieje w jednym z podanych rejestrów jako reprezentant organizacji
- **Załączenie dokumentu** – dodasz dokument potwierdzający upoważnienie. Przykład takiego dokumentu możesz pobrać z odnośnika **Pobierz gotowe upoważnienie**.



Na metodę weryfikacji upoważnienia subskrybenta ma również wpływ wybrana metoda weryfikacji organizacji. Jeśli został tam podany numer rejestrowy i jego typ, Certum w pierwszej kolejności poszuka czy subskrybent widnieje w rejestrze, a samą metodę weryfikacji upoważnienia subskrybenta system automatycznie oznaczy jako **Subskrybent widnieje w rejestrze**. Nie jest to jednak przeszkodą by dodać dokument potwierdzający upoważnienie subskrybenta.



- Dashboard
- Certyfikaty
- Domeny
- Wyszukiwarka certyfikatów
- Sklep Certum



## Upoważnienie

Wybierz metodę weryfikacji upoważnienia subskrybenta do reprezentowania organizacji.

### Dane subskrybenta

Imię      Nazwisko  
Jan      Kowalski

### Metoda weryfikacji upoważnienia subskrybenta

- Subskrybent widnieje w KRS, GUS, CEIDG, DUNS lub LEI jako reprezentant organizacji       Załączenie dokumentu potwierdzającego upoważnienie

### Wybrany typ numeru rejestrowego

KRS  
12345678

[Cofnij](#)

[Kontynuuj](#)

Po wybraniu metody weryfikacji upoważnienia i przejściu dalej, zweryfikuj wprowadzone dane na ekranie podsumowania. Jeśli dane są poprawne, oznacz wymagane oświadczenia i zakończ krok podawania danych do weryfikacji.

Ekran sukcesu poinformuje Cię o zapisaniu danych do weryfikacji. Certum zajmie się ich weryfikacją. W tym czasie, jeśli chcesz dodać jeszcze jakiś dokument potwierdzający wprowadzone dane, możesz go dodać w szczegółach certyfikatu. Jest to również czas na wykonanie automatycznej weryfikacji tożsamości subskrybenta, jeśli taka metoda weryfikacji została wybrana. Zapraszamy do zapoznania się z instrukcją [automatycznej weryfikacji tożsamości](#).



- [Dashboard](#)
- [Certyfikaty](#)
- [Domeny](#)
- [Wyszukiwarka certyfikatów](#)
- [Sklep Certum](#)



## Sukces!

Dane zostały zapisane i przekazane do weryfikacji. Weryfikacja zajmuje zwykle od 1 do 7 dni. Pozytywna weryfikacja danych pozwoli przejść do kolejnego kroku aktywacji certyfikatu.

[Przejdź do dashboardu](#)

Pozytywna weryfikacja podanych danych pozwoli przejść do kroku **Aktywacji certyfikatu**.

## Krok Aktywacja certyfikatu

Aktywację certyfikatu możesz rozpocząć poprzez **Dashboard**, wybierając opcję **Aktywacja certyfikatu**:

- [Dashboard](#)
- [Certyfikaty](#)
- [Domeny](#)
- [Wyszukiwarka certyfikatów](#)
- [Sklep Certum](#)

### Cześć

Zalogowałeś się do panelu produktów bezpieczeństwa, gdzie możesz je aktywować, sprawdzić status i zarządzać nimi.



### Przydatne informacje

Proces aktywacji certyfikatu składa się zaleźnie od typu certyfikatu, z dostarczenia danych organizacji i subskrybenta certyfikatu, podania domeny lub adresu mailowego do umieszczenia w certyfikacie i ich weryfikacji oraz podania kluczy. Wszystkie wymagane przez produkt kroki są prezentowane na kafelku produktu. Każdy z kroków możesz wykonać w dogodnym dla siebie czasie, jednak pamiętaj, że ukończenie wszystkich z nich i ich pozytywna weryfikacja przez zespół Certum jest konieczna do wydania certyfikatu.

### Przydatne linki

- [Automatyczna weryfikacja subskrybenta](#)
- [Pomoc, wymagane dokumenty](#)
- [Generator CSR, PFX](#)
- [Nasze produkty](#)

### Powiadomienia

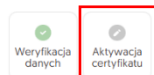
[Informacje](#)   [Problemy](#)   [Wygasające certyfikaty](#)   [Nowe certyfikaty \[1\]](#)



Nie znaleziono zadań spełniających kryteria.

### Code Signing

Numer zamówienia ORDER/0000123456/pc48



Alias  
-  
Produkt  
**EV Code Signing 365 dni - wydanie**  
Status  
**W weryfikacji**  
Common name  
-  
Data końca ważności certyfikatu  
-  
[Szczegóły certyfikatu](#)

lub analogicznie jak w poprzednim kroku: z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz opcję **Aktywuj certyfikat**.

W tym kroku wybierzesz pola do certyfikatu oraz wygenerujesz parę kluczy.

Wybierz pola, które chcesz umieścić w certyfikacie. Niektóre pola są wymagane i ich odznaczenie nie jest możliwe.

Po dokonaniu wyboru przejdź do generowania pary kluczy.

Dla certyfikatów Code Signing dostępnymi metodami generacji kluczy jest **Generowanie pary kluczy na karcie** – klucze zostaną zapisane na karcie kryptograficznej.

Wybierając metodę generowania pary kluczy na karcie, wybierz również algorytm i długość klucza. Twój wybór powinien zależeć od algorytmu i długości klucza wspieranej przez aplikację, w której używasz certyfikatu lub rekomendację np. Twojego działu IT.

Po wybraniu metody generowania pary kluczy na karcie, wybierz algorytm i długość klucza.

**Certum**  
by *ORFECO*

Dashboard  
Certyfikaty  
Domeny  
Wyszukiwarka certyfikatów  
Sklep Certum

Wybór danych do certyfikatu   **2**   Metoda generacji   Generacja kluczy   Podsumowanie

## Wybór metody generowania kluczy

Generacja za pomocą aplikacji Certum SignService pozwoli zapisać klucze na karcie kryptograficznej.

### Metoda generacji pary kluczy

Generowanie pary kluczy na karcie

ALGORYTM KLUCZA I DŁUGOŚĆ KLUCZA

RSA 3072

Metoda CSR pozwoli uzyskać certyfikat wraz z kluczem w formie do przenoszenia i instalacji z pliku. Pamiętaj, by zapisać klucz prywatny, który wygenerowałeś wraz z CSR.

1 Wygenerowanie kluczy na karcie spowoduje, że wydany certyfikat zostanie zainstalowany na karcie kryptograficznej i jej podłączenie do komputera będzie wymagane zawsze, gdy certyfikat jest używany. Wspierane są tylko karty Certum.

Cofnij   Kontynuuj

Po przejściu dalej, upewnij się, że posiadasz kartę włożoną do czytnika, czytnik podłączony do komputera, a sama karta ma zainicjalizowany profil zwykły z nadanym kodem PIN. W procesie wymagane jest również posiadanie zainstalowanej na komputerze aplikacji proCertum CardManager, w której możesz również sprawdzić status karty i kodów PIN i PUK.

Zapraszamy do zapoznania się z instrukcją [jak nadać kod PUK i PIN dla profilu zwykłego karty](#).

- [Dashboard](#)
- [Certyfikaty](#)
- [Domeny](#)
- [Wyszukiwarka certyfikatów](#)
- [Sklep Certum](#)

- ✓ Wybór danych do certyfikatu
- ✓ Metoda generacji
- 3 Generacja kluczy
- Podsumowanie

## Generacja kluczy

W celu wygenerowania kluczy, zastosuj instrukcję dostępną poniżej.

[Pobierz aplikację Certum SignService](#)

1. Pobierz i zainstaluj aplikację **Certum SignService**.
2. Pobierz i zainstaluj aplikację **proCertum CardManager**, jeśli jej nie posiadasz lub jest nieaktualna.
3. Podłącz czytnik do komputera i włóż kartę do czytnika.
4. Otwórz aplikację **proCertum CardManager** i sprawdź czy profil zwykły karty jest zainicjalizowany. Jeśli profil nie jest zainicjalizowany, aplikacja poprosi Cię o nadanie kodów PIN i PUK.
5. Rozpocznij generację kluczy przyciskiem **Wygeneruj klucze**.
6. Zaakceptuj komunikat z przeglądarki o zgodę na uruchomienie aplikacji Certum SignService.
7. Gdy pojawi się okno aplikacji Certum SignService, wprowadź PIN do profilu zwykłego karty.
8. Oczekaj na wygenerowanie kluczy, może to zająć do kilku minut.

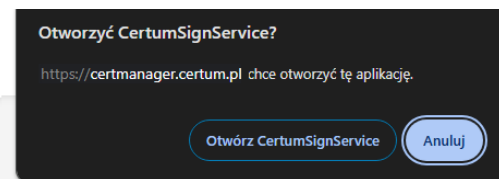
i Po zakończeniu generacji, zostaniesz przeniesiony do kolejnego okna procesu.

[Cofnij](#)

**Wygeneruj klucze**

Do wygenerowania kluczy na karcie potrzebujesz również zainstalowaną na komputerze aplikację Certum SignService. Aplikacja Certum SignService po uruchomieniu generowania kluczy, poprosi o zgodę na uruchomienie się i podanie kodu PIN profilu zwykłego karty w celu wygenerowania na niej kluczy.

- [Dashboard](#)
- [Certyfikaty](#)



- ✓ Wybór danych do certyfikatu
- ✓ Metoda generacji
- 3 Generacja kluczy
- Podsumowanie



Po wpisaniu kodu PIN rozpocznie się proces generowania klucza na karcie. Może to zająć do kilkudziesięciu sekund. Po wygenerowaniu kluczy, proces przejdzie do kolejnego etapu.

Przejdź na ekran podsumowania i sprawdź wszystkie dane. Oznacz oświadczenia jeśli są wymagane i zakończ aktywację certyfikatu.

Ekran sukcesu poinformuje Cię o przekazaniu certyfikatu do wydania. Wydany certyfikat można będzie pobrać z wiadomości e-mail o utworzeniu certyfikatu lub z widoku szczegółów certyfikatu: w dogodnym kodowaniu **PEM** lub **DER** lub zainstalować na karcie, również z poziomu szczegółów certyfikatu.

W widoku szczegółów certyfikatu możesz również pobrać certyfikaty pośrednie dla wydanego certyfikatu.