

Aktywacja certyfikatu Open Source Code Signing w chmurze

Wer. 1.0

assecO

 **Certum**
by assecO

Spis treści

1. Opis produktu	3
2. Aktywacja certyfikatu	3
Krok Weryfikacja danych	4
Krok Aktywacja certyfikatu.....	8

1. Opis produktu

Certyfikat Standard Code Signing w chmurze to certyfikat przechowywany na karcie wirtualnej w usłudze SimplySign.

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.

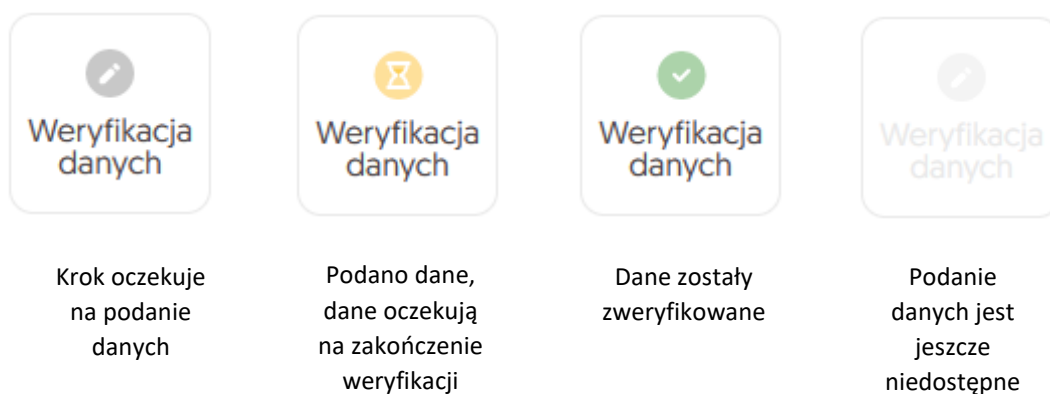
Cyfrowe podpisywanie kodu sprawia, że korzystanie z aplikacji jest bezpieczne, co przekłada się na większe zaufanie do Twojej marki i poszerzenie grona klientów.

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 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 Weryfikacja danych

Podanie danych do weryfikacji to krok, w którym podasz dane subskrybenta (osoby, która będzie właścicielem certyfikatu). Spośród podanych tu danych będzie możliwy w ostatnim kroku aktywacji certyfikatu wybór danych do certyfikatu.

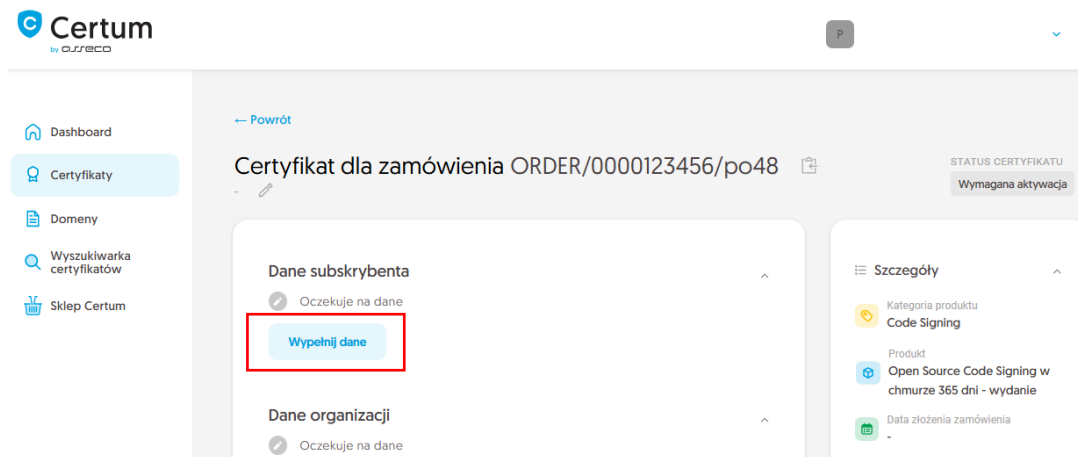
Listę obsługiwanych dokumentów potwierdzających znajdziesz w [Informacje o wymaganych dokumentach](#).

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

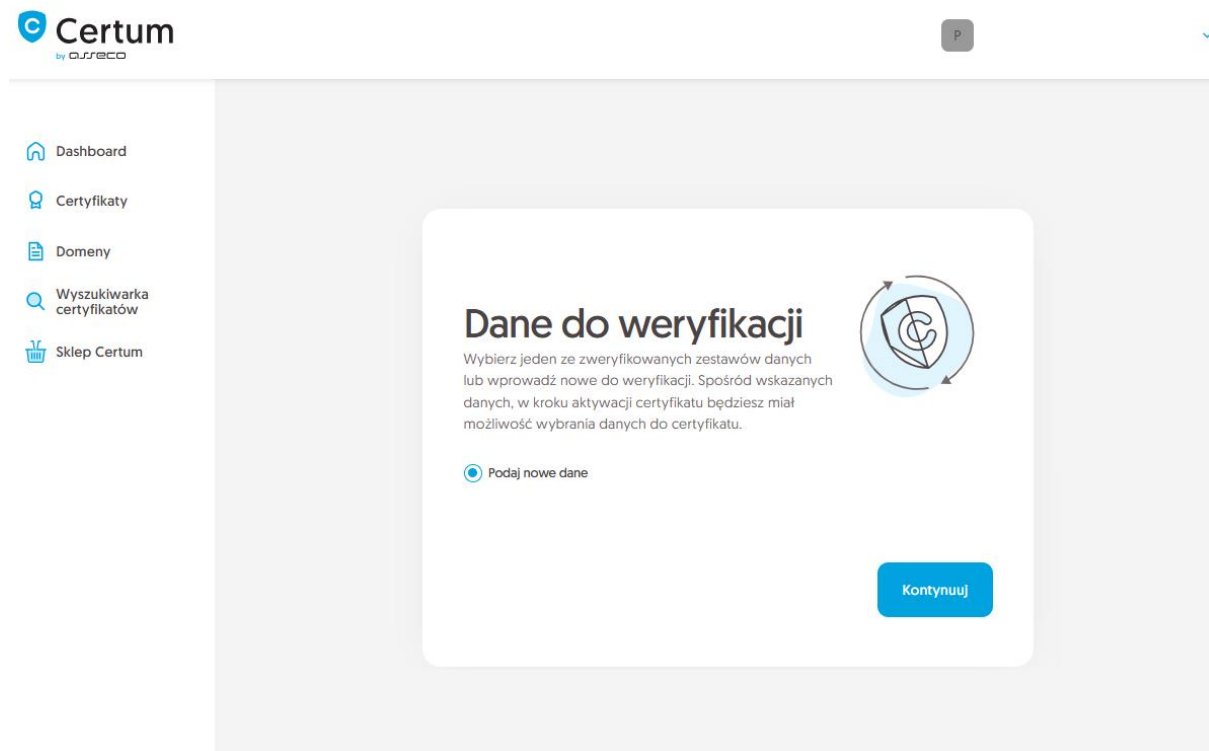
The screenshot shows the Certum dashboard interface. On the left is a navigation menu with items: Dashboard, Certyfikaty, Domeny, Wyszukiwarka certyfikatów, and Sklep Certum. The main content area is divided into several sections:

- Cześć**: A welcome message stating the user is logged into the security products panel and can activate or manage certificates.
- Powiadomienia**: A notification section with tabs for 'Informacje', 'Problemy', 'Wygasające certyfikaty', and 'Nowe certyfikaty [1]'. It displays a message: 'Nie znaleziono zadań spełniających kryteria.' (No tasks meeting the criteria were found).
- Code Signing**: A section for a specific certificate with the order number 'CIB29/000023456/po48'. It features two buttons: 'Weryfikacja danych' (highlighted with a red box) and 'Aktywacja certyfikatu'. Below the buttons, details for the certificate are listed:
 - Alias: -
 - Produkt: Open Source Code Signing w chmurze 365 dni - wydanie
 - Status: Wymagana aktywacja
 - Common name: -
 - Data końca ważności certyfikatu: -
- Przydatne informacje**: A section providing details about the activation process, including a note that the process depends on the certificate type and organization data, and a list of 'Przydatne linki' (Useful links) such as 'Automatyczna weryfikacja subskrybenta', 'Pomoc, wymagane dokumenty', and 'Nasze produkty'.

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



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.

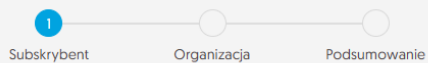


W kolejnym etapie podaj dane subskrybenta, czyli osoby, która będzie właścicielem certyfikatu. Imiona i nazwiska zapisz w formularzu tak, jak widnieją na dokumencie tożsamości subskrybenta.

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.

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



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@twojadomena.pl

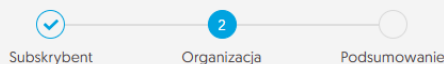
W przypadku **automatycznej weryfikacji tożsamości**, na podany tu adres e-mail subskrybent otrzyma link oraz instrukcję do rozpoczęcia procesu. Link zostanie wysłany po zapisaniu danych do weryfikacji.

[Cofnij](#)

[Kontynuuj](#)

Po wypełnieniu powyższych danych, przejdź do kolejnego etapu, czyli podania danych organizacji. Dla certyfikatu Open Source podaj dane adresowe subskrybenta.

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



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*

Open Source Developer

Siedziba organizacji

KRAJ*

Polska [PL]

WOJEWÓDZTWO*

mazowieckie

MIEJSCOWOŚĆ*

Warszawa

Metoda weryfikacji

Załączenie potwierdzenia istnienia organizacji

Dokumenty [0]

[Informacje o wymaganych dokumentach](#)

Po wypełnieniu wszystkich wymaganych danych, przejdź do podsumowania.

Zweryfikuj wprowadzone dane na ekranie podsumowania. Jeśli dane są poprawne, oznacz oświadczenia jeśli są wymagane 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.



Powiadomienia

Informacje Problemy Wygasające certyfikaty Nowe certyfikaty [1]



Nie znaleziono zadań spełniających kryteria.

Przydatne informacje

Proces aktywacji certyfikatu składa się, zależnie 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.

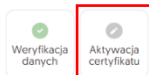
Przydatne linki

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

< ● ● ● >

Code Signing

Numer zamówienia ORDER/0000123456/pc48



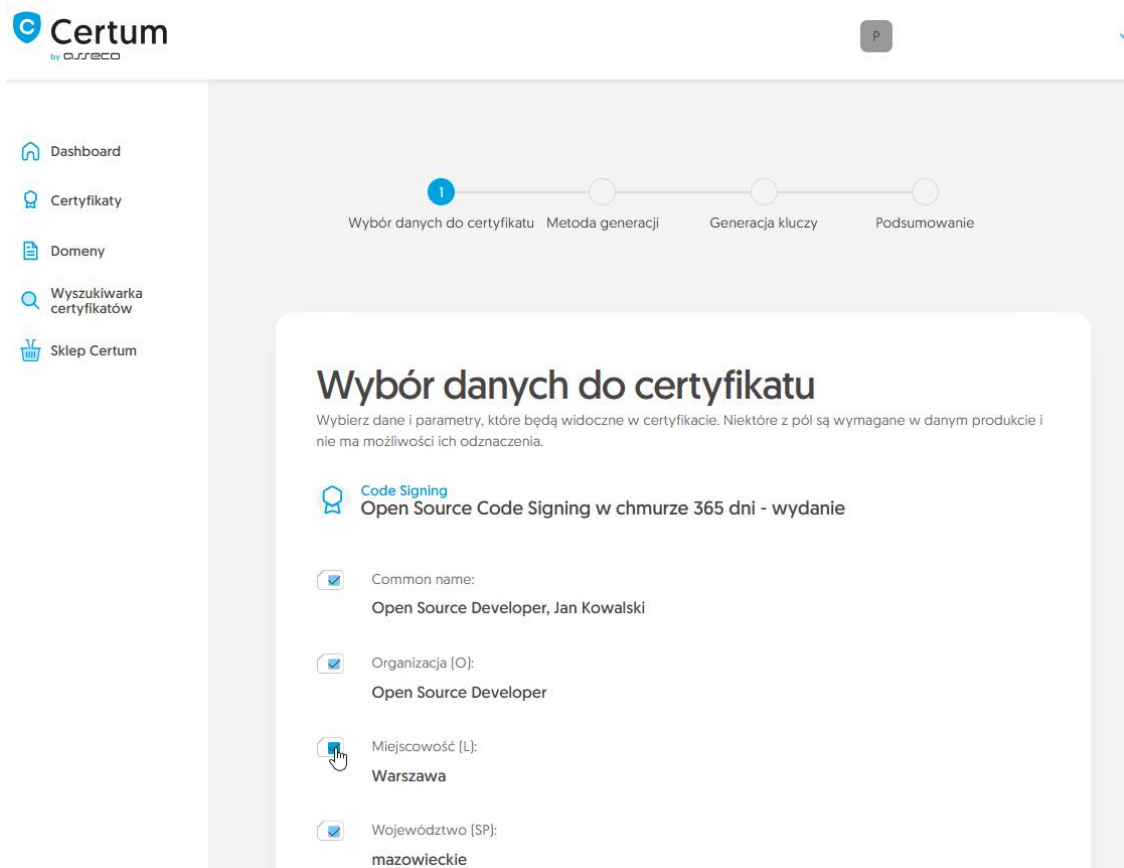
Alias
-
Produkt
Open Source Code Signing w chmurze 365 dni - wydanie
Status
W weryfikacji
Common name
-
Data końca ważności certyfikatu
-

[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.








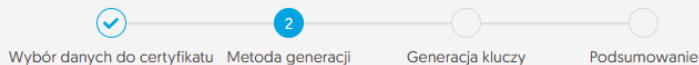
Po dokonaniu wyboru przejdź do generowania pary kluczy.

Dla certyfikatów Code Signing w chmurze dostępnymi metodami generacji kluczy jest metoda **Certyfikat w chmurze** – klucze zostaną zapisane na wirtualnej karcie kryptograficznej w usłudze SimplySign.

Wybierając metodę generowania pary kluczy w chmurze, 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.

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



Wybór metody generowania kluczy


Dla certyfikatów przechowywanych w chmurze generacja kluczy odbędzie się automatycznie.

Metoda generacji pary kluczy

Certyfikat w chmurze

ALGORYTM KLUCZA I DŁUGOŚĆ KLUCZA






RSA 3072 ▼

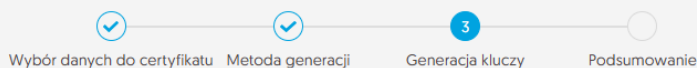
 W kolejnym kroku podasz lub zadeklarujesz do założenia konto w usłudze SimplySign, która służy do przechowywania certyfikatów Certum w chmurze.

[Cofnij](#)

[Kontynuuj](#)

W kolejnym etapie zdecyduj, czy istnieje już konto SimplySign, na którym ma zostać zainstalowany certyfikat, czy też chcesz, aby założyć dla tego certyfikatu nowe konto SimplySign. W obu przypadkach podaj adres e-mail, który będzie służył jako login do usługi SimplySign i umożliwi dostęp do wystawionego certyfikatu.

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



Konto SimplySign

Certyfikaty przechowywane w usłudze SimplySign (w chmurze) wymagają podania identyfikatora konta do którego mają zostać przypisane. Wprowadź adres e-mail konta SimplySign, na którym będzie używany certyfikat po jego wydaniu.

ADRES KONTA SIMPLYSIGN*

Wprowadź adres e-mail konta SimplySign

Jeśli konto SimplySign nie istnieje, zostanie ono dla Ciebie założone. Certyfikat po wydaniu zostanie automatycznie zainstalowany na koncie w usłudze SimplySign.



[Cofnij](#)

[Kontynuuj](#)

Po podaniu adresu e-mail konta SimplySign, 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 zostanie zainstalowany na koncie SimplySign podanym w poprzednim kroku. Zapoznaj się z [instrukcją instalacji aplikacji SimplySign](#) oraz z [instrukcją aktywacji aplikacji SimplySign](#).

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