

Aktywacja certyfikatu Standard Code Signing w chmurze

Wer. 1.9

assecO

 **Certum**
by assecO

Spis treści

1. Opis produktu	3
2. Aktywacja certyfikatu	3
Krok Weryfikacja danych	4
Wybór wariantu danych do weryfikacji	5
Podsumowanie kroku Weryfikacja danych	10
Krok Aktywacja certyfikatu.....	11

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

Jako **klient**, możesz rozpocząć proces aktywacji certyfikatu z poziomu **Twojego konta** w sklepie, w zakładce **Produkty bezpieczeństwa**.

Jako **partner**, proces aktywacji certyfikatu rozpoczynasz z poziomu **Dashboardu**, wybierając produkt, który chcesz zamówić.

Proces składa się z kilku kroków:

- **Weryfikacja danych** – podanie danych subskrybenta i/lub 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
nie dostępne

Krok Weryfikacja danych

Podanie danych do weryfikacji to krok, w którym, zależnie od wybranego wariantu wydania, 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.

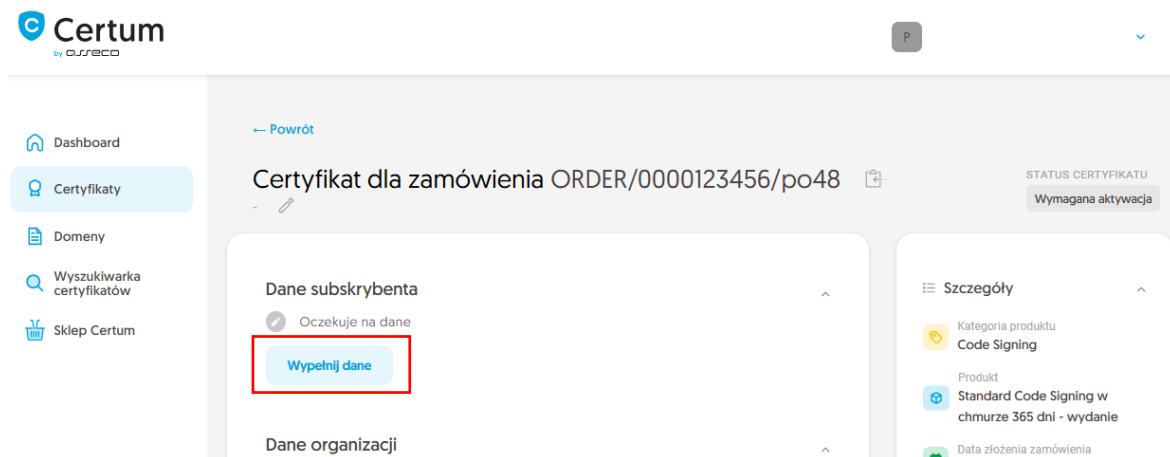
Listę obsługiwanych dokumentów potwierdzających znajdziesz w [Informacje o wymaganych dokumentach](#).

Jako **klient**, rozpocząć podawanie 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 section with a 'Zalogowałeś się do panelu produktów bezpieczeństwa, gdzie możesz je aktywować, sprawdzić status i zarządzać nimi.' message and a Certum logo.
- Powiadomienia**: A notification section with tabs for 'Informacje', 'Problemy', 'Wygasające certyfikaty', and 'Nowe certyfikaty [1]'. It displays a message: 'Nie znaleziono zadań spełniających kryteria.' with a box icon.
- Code Signing**: A section for a specific certificate. It shows a 'Weryfikacja danych' button highlighted with a red box, and an 'Aktywacja certyfikatu' button. Below the buttons are fields for 'Alias', 'Produkt' (Standard Code Signing w chmurze 365 dni - wydanie), 'Status' (Wymagana aktywacja), 'Common name', and 'Data końca ważności certyfikatu'. A 'Szczegóły certyfikatu' link is at the bottom.
- Przydatne informacje**: A section with a lightbulb icon and text explaining the activation process. It includes a 'Przydatne linki' section with links to 'Automatyczna weryfikacja subskrybenta', 'Pomoc, wymagane dokumenty', 'Generator CSR, FFX', and 'Nasze produkty'.

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



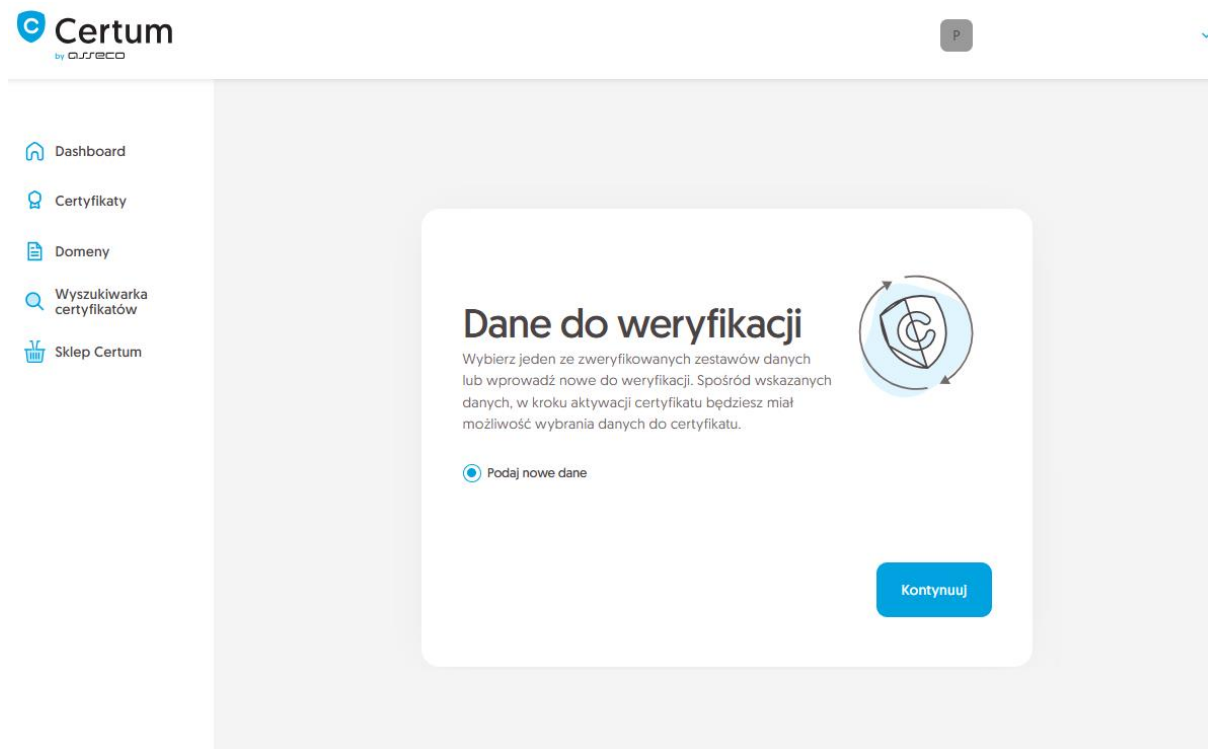
Jako **partner**, rozpocząć krok weryfikacji danych możesz z poziomu **Dashboardu**, wybierając opcję nowego zamówienia. Po wybraniu typu produktu i podaniu szczegółów zamówienia, będziesz mógł podać dane do wykorzystania w pierwszym kroku wydawania certyfikatu.

Wybór wariantu danych do weryfikacji

Wybierz jeden z trzech wariantów podania danych do weryfikacji:

- **Osoba fizyczna** – w certyfikacie umieszczone są dane subskrybenta, weryfikowana jest tożsamość subskrybenta, a jego dane adresowe podawane są w polach na dane organizacji. W Common name certyfikatu umieszczone jest imię i nazwisko subskrybenta
- **Organizacja** – w certyfikacie umieszczone są dane organizacji, weryfikowana jest tożsamość subskrybenta, organizacja oraz upoważnienie subskrybenta do reprezentowania organizacji. W Common name certyfikatu umieszczona jest nazwa organizacji
- **Sponsor** – w certyfikacie umieszczone są dane subskrybenta i organizacji, weryfikowana jest tożsamość subskrybenta, organizacja oraz upoważnienie subskrybenta do reprezentowania organizacji. W Common name certyfikatu umieszczone jest imię i nazwisko subskrybenta.






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.

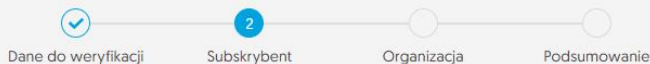


W kolejnym etapie podaj dane subskrybenta, czyli osoby, która reprezentuje organizację i będzie właścicielem certyfikatu. Imiona i nazwiska zapisz w formularzu tak, jak widnieją na dokumencie tożsamości subskrybenta.

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.

-  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 w wariantcie **osoba fizyczna**, podaj dane adresowe subskrybenta. Przejdź dalej do [podsumowania](#).

P

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

Dane do weryfikacji Subskrybent **3** Organizacja Podsumowanie

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*

Siedziba organizacji

KRAJ*

WOJEWÓDZTWO*

MIEJSCOWOŚĆ*

Jako osoba fizyczna, nie reprezentujesz żadnej organizacji. Wprowadź dane adresowe subskrybenta, które zostaną umieszczone w certyfikacie.

[Cofnij](#) [Kontynuuj](#)

Dla certyfikatów w wariantach **organizacja** i **sponsor** 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

Siedziba organizacji

KRAJ*

Polska [PL]

WOJEWÓDZTWO*

mazowieckie

MIEJSCOWOŚĆ*

Warszawa

Metoda weryfikacji

Wskazanie rejestru
 Załączenie potwierdzenia istnienia organizacji

WSKAZANIE NUMERU REJESTROWEGO*

KRS

Po wypełnieniu wszystkich wymaganych danych, przejdź do ostatniego etapu kroku podawania danych do weryfikacji, czyli do określenia sposobu weryfikacji upoważnienia subskrybenta do reprezentowania organizacji. Etap jest wymagany dla wariantów **organizacja** i **sponsor**.

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.

Po wybraniu metody weryfikacji upoważnienia przejdź dalej.

Podsumowanie kroku Weryfikacja danych

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
Standard 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.

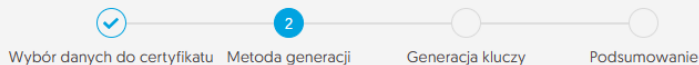
Po dokonaniu wyboru, przejdź do generowania pary kluczy.

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 rekomendacją 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

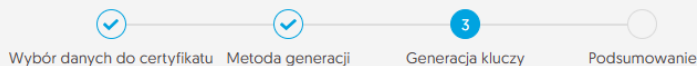
 W kolejnym kroku podasz lub zadeklarujesz do założenia konto w usłudze SimplySign, która służy do przechowywania certyfikatów Certum w chmurze.

[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.