



Aktywacja certyfikatu Standard Code Signing w chmurze

Wer. 1.7

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 welcome message stating the user is logged into the security products panel.
- Powiadomienia**: A notification section with a table header (Zdarzenie, Produkt, Data powiadomienia) and a central icon of an open box. Below the table, it says "Brak powiadomień do wyświetlenia."
- Code Signing**: A section for a specific product. It shows the order number "ORDER/0000123456/po9" and two buttons: "Weryfikacja danych" (highlighted with a red box) and "Aktywacja certyfikatu". Below the buttons, it lists:
 - Produkt: Standard Code Signing w chmurze 365 dni - wydanie
 - Status: Wymagana aktywacja
 - Common name: -
 - Data końca ważności certyfikatu: -
- Przydatne informacje**: A section with a lightbulb icon and text explaining the activation process.
- Przydatne linki**: A section with a link icon and a list of links:
 - Automatyczna weryfikacja subskrybenta
 - Pomoc, wymagane dokumenty
 - Generator CSR, PFX
 - Nasze produkty

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

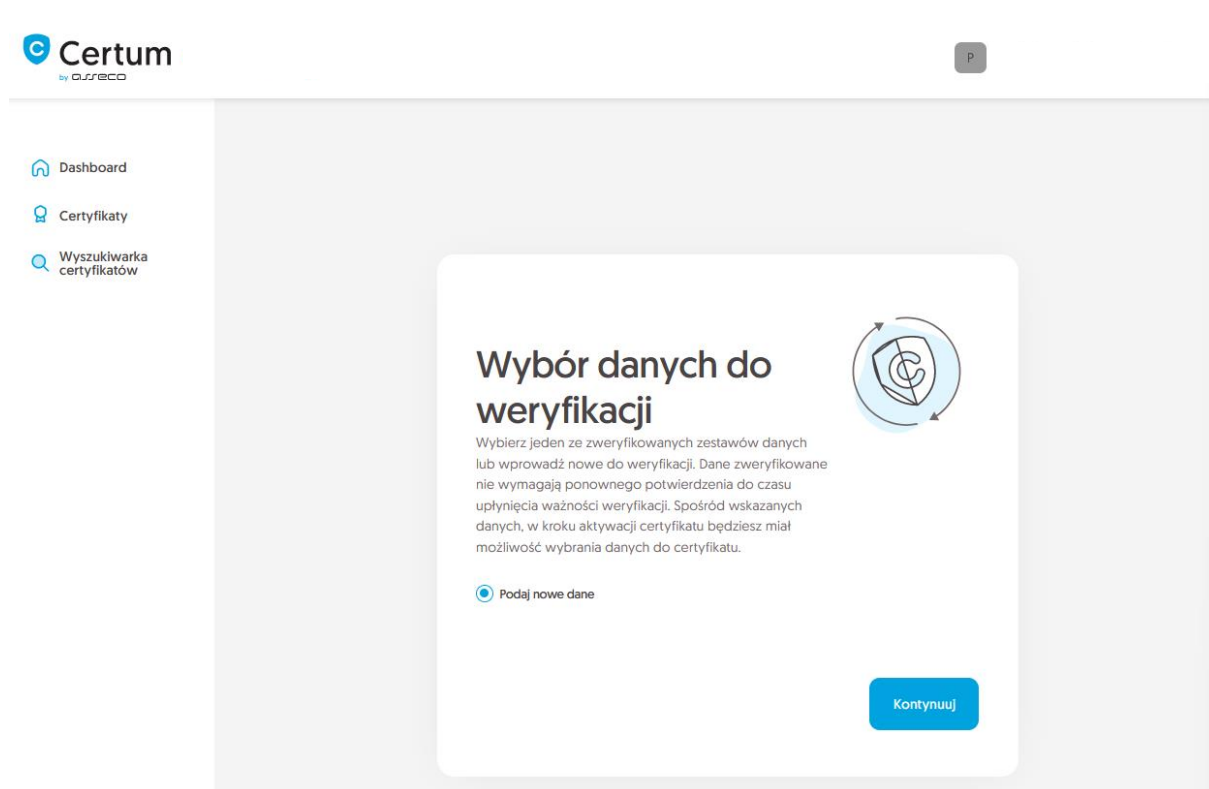
Jako **partner**, rozpocząć krok weryfikacji danych możesz z poziomu **Dashboardu**, wybierając opcję nowego zamówienia. Po wybraniu typu produktu i podaniu szczegółów zamówienia, będziesz mógł podać dane do wykorzystania w pierwszym kroku wydawania certyfikatu.

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.



Certum
by OFRACO

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów

Wybór danych do weryfikacji

Wybierz jeden ze zweryfikowanych zestawów danych lub wprowadź nowe do weryfikacji. Dane zweryfikowane nie wymagają ponownego potwierdzenia do czasu upłynięcia ważności weryfikacji. Spośród wskazanych danych, w kroku aktywacji certyfikatu będziesz miał możliwość wybrania danych do certyfikatu.




Podaj nowe dane

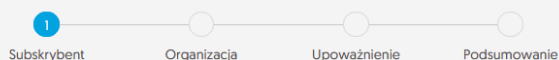
Kontynuuj

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
-  Wyszukiwarka certyfikatów



Dane Subskrybenta do weryfikacji

Subskrybent to osoba, która będzie właścicielem certyfikatu: dane jej lub powiązanej z nią organizacji którą może reprezentować, będą dostępne do wyboru jako dane do certyfikatu, zależnie od zakupionego typu produktu. Po zapisaniu danych do weryfikacji, 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*

jankowski@twojadomena.pl

W przypadku **automatycznej weryfikacji tożsamości**, na podany tu adres e-mail Subskrybent otrzyma link oraz instrukcje 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](#).

Certum
by CJSECO

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów

Wybór danych do weryfikacji Subskrybent **Organizacja** Podsumowanie

Dane do weryfikacji 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*
Jan Kowalski

Siedziba organizacji

KRAJ*
Polska

WOJEWÓDZTWO*
mazowieckie

MIEJSCOWOŚĆ*
Warszawa

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 do weryfikacji 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

WOJEWÓDZTWO*

mazowieckie

MIEJSCOWOŚĆ*

Warszawa

Metoda weryfikacji

Wskazanie rejestru Załączenie potwierdzenia istnienia organizacji

WSKAZANIE NUMERU REJESTROWEGO*

KRS

NUMER REJESTROWY*

12345678

[Cofnij](#)

[Kontynuuj](#)

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.

Certum
by GUSSECO

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów

Wybór danych do weryfikacji Subskrybent Organizacja **Upoważnienie** Podsumowanie

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

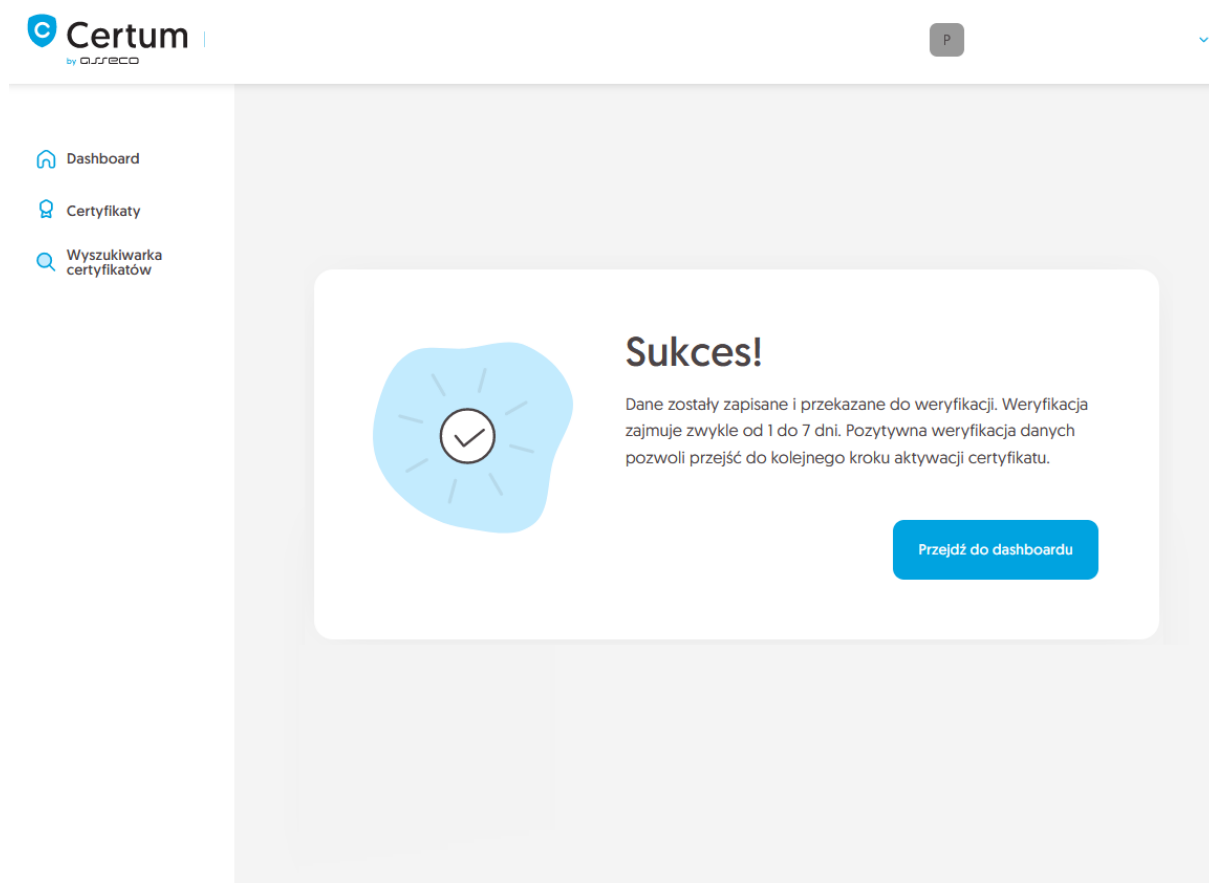
[Cofnij](#) [Kontynuuj](#)

Po wybraniu metody weryfikacji upoważnienia 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](#).

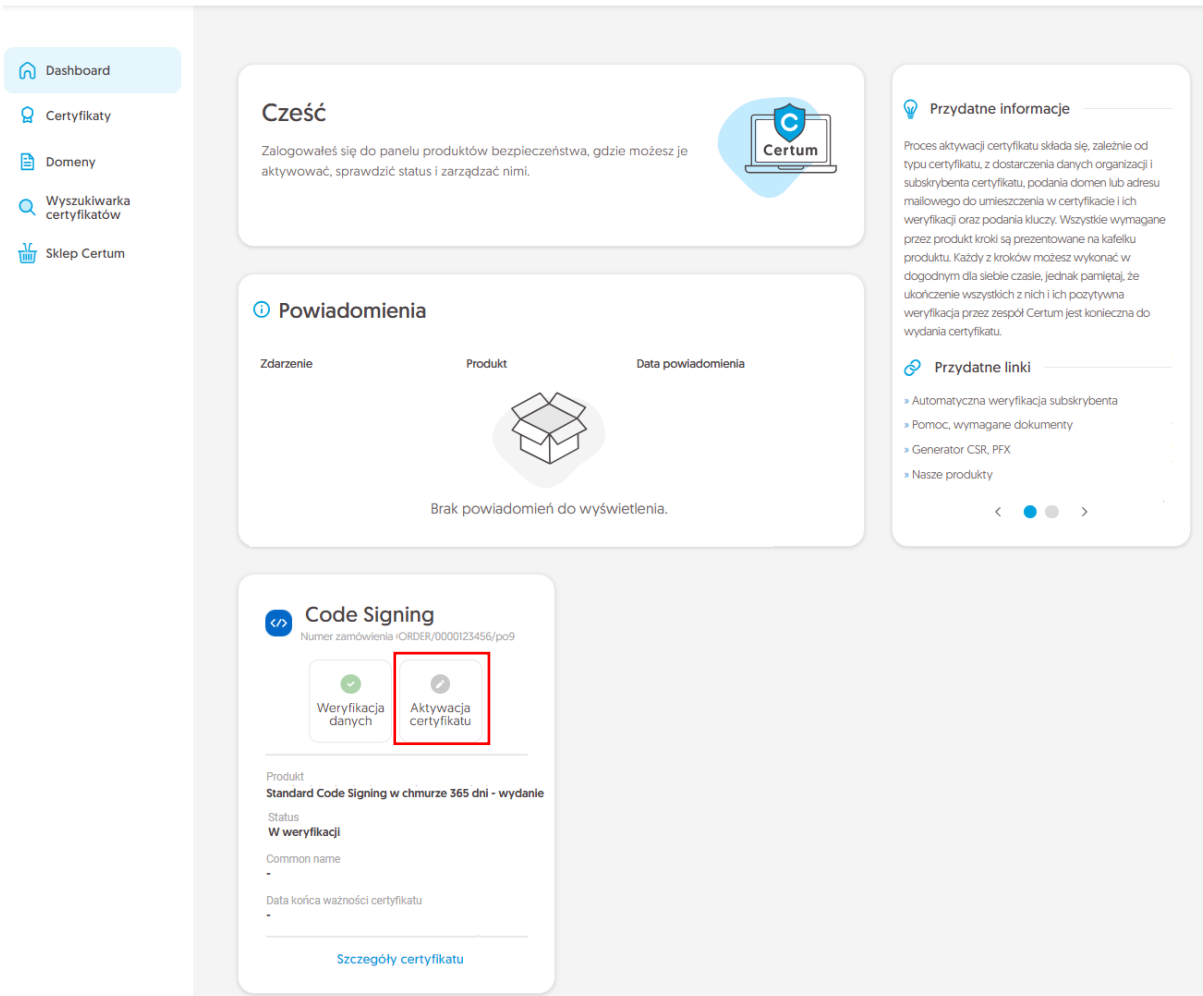


The screenshot shows the Certum by asseco dashboard. On the left, there is a navigation menu with three items: 'Dashboard' (home icon), 'Certyfikaty' (certificate icon), and 'Wyszukiwarka certyfikatów' (magnifying glass icon). The main content area features a large white card with a blue circular icon containing a white checkmark. To the right of the icon, the heading 'Sukces!' is displayed in bold. Below the heading, a paragraph of text states: '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.' At the bottom right of the card, there is a blue button with the text '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**:

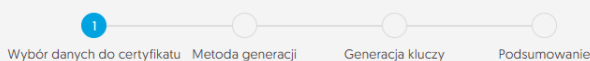


lub analogicznie jak w poprzednim kroku: z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz opcję **Aktywuj certyfikat**.

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.

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



Wybór danych do certyfikatu

Wybierz dane i parametry, które będą widoczne w certyfikacie. Niektóre z pól są wymagane w danym produkcie i nie ma możliwości ich odznaczenia.

 Code Signing
Standard Code Signing w chmurze 365 dni - wydanie

Common name:
Jan Kowalski

Organizacja [O]:
Twoja firma

Miejscowość [L]:
Warszawa





Województwo [SP]:
województwo

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
-  Wyszukiwarka certyfikatów
-  Sklep Certum

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

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

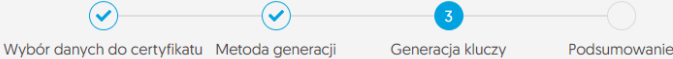
 W kolejnym kroku podasz lub zadeklarujesz do założenia konto w usłudze SimplySign, która służy do przechowywania certyfikatów Certum w chmurze.

[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*

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. Certum zweryfikuje ostatecznie dane w certyfikacie i po pozytywnej weryfikacji, wyda go. Wydany certyfikat zostanie automatycznie 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.