

# Aktywacja certyfikatu Standard Code Signing w chmurze

Wer. 1.5

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 Generacja klucza .....	11
Krok Aktywacja certyfikatu .....	14

## 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.

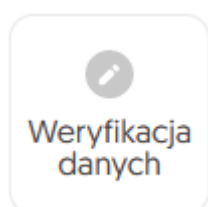
Cyfrowe podpisywanie kodu sprawia, że korzystanie z aplikacji jest bezpieczne, co przekłada się na większe zaufanie do Twojej marki i poszerzenie grona klientów.

## 2. Aktywacja certyfikatu

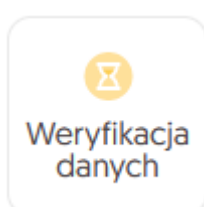
Rozpoczęcie procesu aktywacji będzie możliwe z poziomu **Twojego konta** w sklepie, w zakładce **Produkty bezpieczeństwa**. Proces składa się z kilku kroków:

- **Weryfikacja danych** – podanie danych Subskrybenta i/lub organizacji oraz ich weryfikacja
- **Generacja klucza** – wygenerowanie kluczy
- **Aktywacja certyfikatu** – wybór pól do certyfikatu i przekazanie go do wydania.

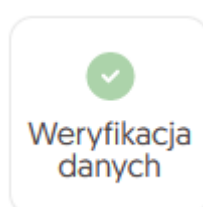
Każdy z kroków w miarę postępu aktywacji będzie przechodził przez kolejne statusy:



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, 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](#).

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

The screenshot shows the Certum dashboard with the following elements:

- Header:** Certum logo and 'Produkty bezpieczeństwa' (Security Products).
- Left Sidebar:** Navigation menu with 'Dashboard' (selected), 'Certyfikaty' (Certificates), and 'Wyszukiwarka certyfikatów' (Certificate Search).
- Main Content Area:**
  - Cześć (Hello):** A welcome message and a Certum logo.
  - Aktualności (News):** A table with columns: Zdarzenie (Event), Produkt (Product), and Data wystąpienia (Occurrence Date).
  - Code Signing:** A section for order 'ORDER/0000123456/pot5'. It features three steps: 'Weryfikacja danych' (Data Verification, highlighted with a red box), 'Generacja klucza' (Key Generation), and 'Aktywacja certyfikatu' (Certificate Activation). Below the steps, it shows:
    - Produkt: Standard Code Signing w chmurze 365 dni - wydanie
    - Status: Wymagana aktywacja
    - Common name: -
    - Data końca ważności certyfikatu: -
    - Link: Szczegóły certyfikatu
  - Przydatne informacje (Useful information):** A section explaining the activation process and listing additional links:
    - Automatyczna weryfikacja Subskrybenta
    - Pomoc, wymagane dokumenty
    - Generator CSR, PFX
    - Nasze produkty

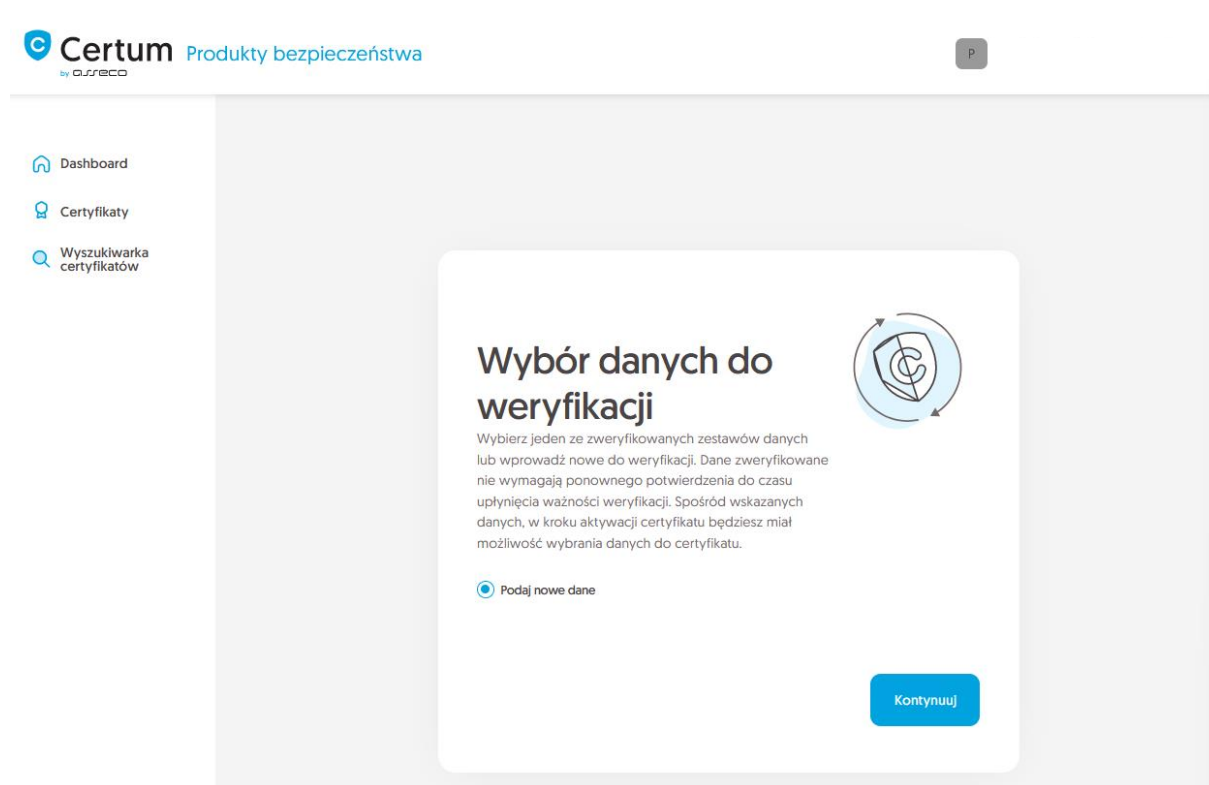
lub z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz przy danych Subskrybenta opcję **Wypełnij dane**:

### 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.

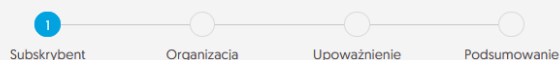


W kolejnym etapie podaj dane Subskrybenta, czyli osoby, która reprezentuje organizację i będzie właścicielem certyfikatu. Imiona i nazwiska zapisz w formularzu tak, jak widnieją na dokumencie tożsamości Subskrybenta.

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
-  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\*

jankowalski@twojdomena.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](#).

## 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\*

Warszawą



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**.



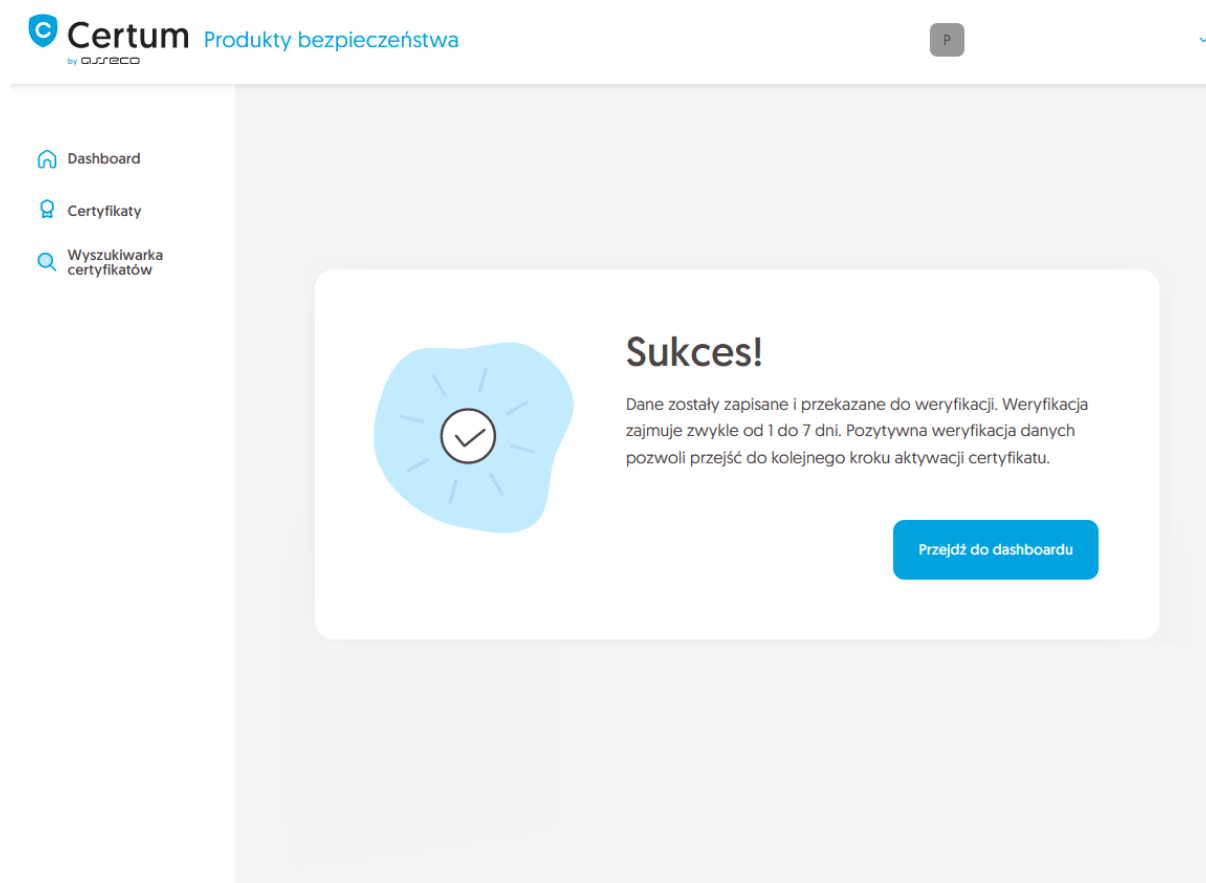
Na metodę weryfikacji upoważnienia Subskrybenta ma również wpływ wybrana metoda weryfikacji organizacji. Jeśli został tam podany numer rejestrowy i jego typ, Certum w pierwszej kolejności poszuka czy Subskrybent widnieje w rejestrze, a samą metodę weryfikacji upoważnienia Subskrybenta system automatycznie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

Po wybraniu metody weryfikacji upoważnienia przejdź dalej.

### Podsumowanie kroku Weryfikacja danych

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](#).



Pozytywna weryfikacja podanych danych pozwoli przejść do kroku wygenerowania kluczy.


### Krok Generacja klucza

Rozpoczęcie generacji pary kluczy możesz poprzez **Dashboard**, wybierając opcję **Generacja klucza**:

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów

### Cześć

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



### Przydatne informacje

Proces aktywacji produktu składa się, zależnie od typu produktu, z dostarczenia danych Organizacji i Subskrybenta certyfikatu, podania domen 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

### Aktualności

Zdarzenie	Produkt	Data wystąpienia

### Code Signing

Numer zamówienia ORDER/0000123456/po15

Weryfikacja danych

**Generacja klucza**

Aktywacja certyfikatu

Produkt: Standard Code Signing w chmurze 365 dni - wydanie

Status: W weryfikacji

Common name: -

Data końca ważności certyfikatu: -

[Szczegóły certyfikatu](#)




lub analogicznie jak w przypadku kroku **Weryfikacja danych**: z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz opcję **Wygeneruj klucze**.

W tym kroku wygenerujesz parę kluczy do certyfikatu.

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
-  Wyszukiwarka certyfikatów

## Wybór metody generowania kluczy


Wybierz jedną z dostępnych metod generacji pary kluczy. Generacja za pomocą aplikacji Certum SignService pozwoli zapisać klucze na karcie kryptograficznej. 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.

Kontynuuj

W kolejnym etapie zdecyduj, czy posiadasz już konto SimplySign, na którym zostanie 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
-  Wyszukiwarka certyfikatów

1 — 2  
 Generacja kluczy Podsumowanie

## 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 chcesz używać certyfikatu po jego wydaniu.

ADRES KONTA SIMPLYSIGN\*

jankowski@twojdomena.pl

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

 **SimplySign**  
by delfico

[Cofnij](#)

[Kontynuuj](#)

Po podaniu adresu e-mail konta SimplySign, przejdź dalej.




Zweryfikuj wprowadzone dane na ekranie podsumowania. Jeśli dane są poprawne, zakończ krok generacji kluczy.

Ekran sukcesu poinformuje Cię o zakończeniu kroku generacji kluczy. Możesz przejść do ostatniego kroku, czyli **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 wybierz pola, które chcesz umieścić w certyfikacie. Niektóre pola są wymagane i ich odznaczenie nie jest możliwe.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów

Wybór danych do certyfikatu Podsumowanie

## 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:  
Twoja firma



Organizacja (O):  
Twoja firma



Miejscowość (L):  
Warszawa



Województwo (SP):  
mazowieckie



Kraj (C):  
Polska

### Okres ważności certyfikatu



Pełny okres ważności certyfikatu



Skrócona data końca ważności

Kontynuuj

Po dokonaniu wyboru przejdź na ekran podsumowania i sprawdź wszystkie wybrane dane. Oznacz wymagane oświadczenia 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 uzyskania dostępu do certyfikatu w chmurze](#) oraz informacją o [aplikacjach wymaganych do użytkowania certyfikatu w chmurze](#).

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