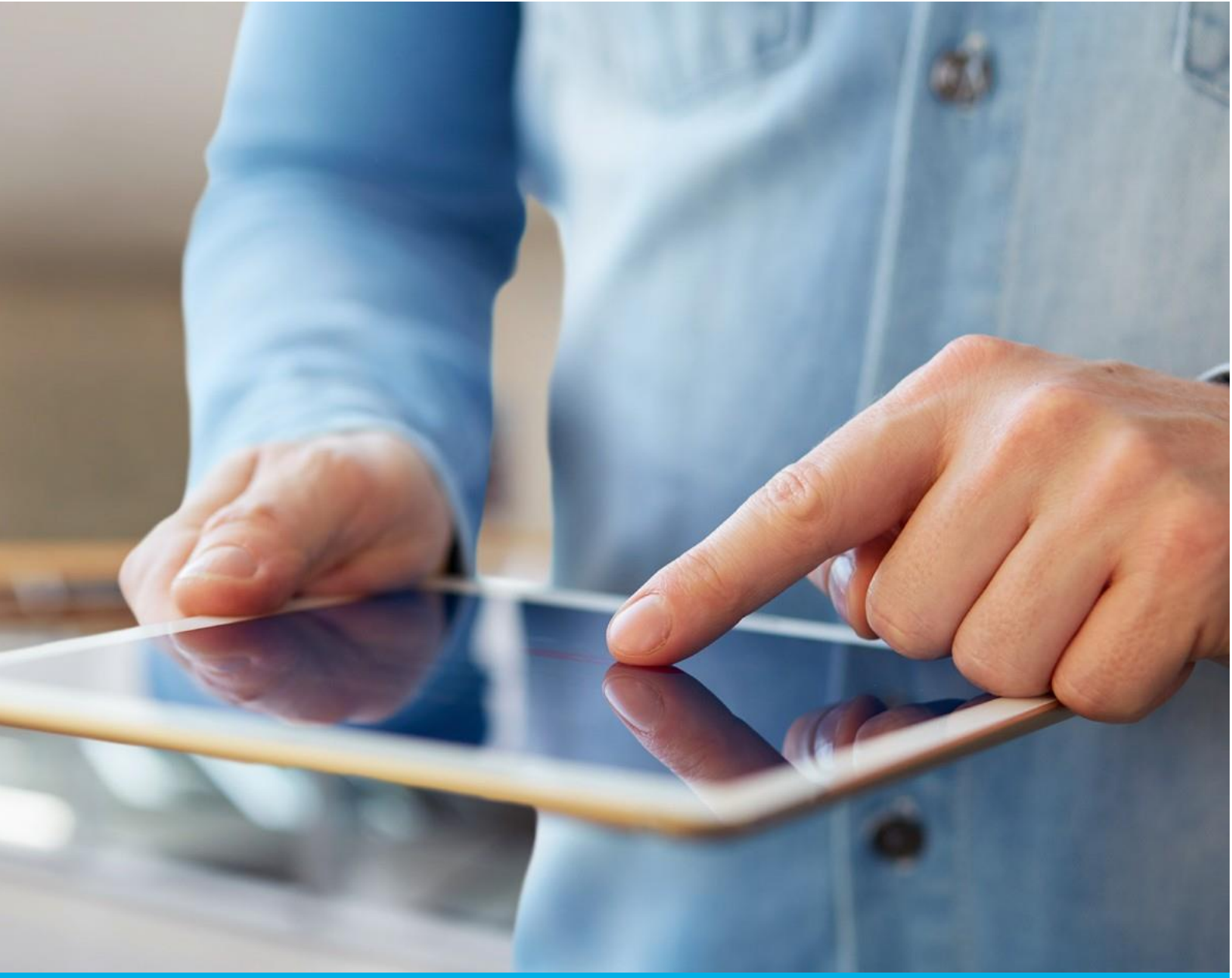


Aktywacja certyfikatu Standard Code Signing na karcie kryptograficznej

Wer. 2.9

asseco

Certum by asseco

Spis treści

certum.pl
infolinia@certum.pl

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.

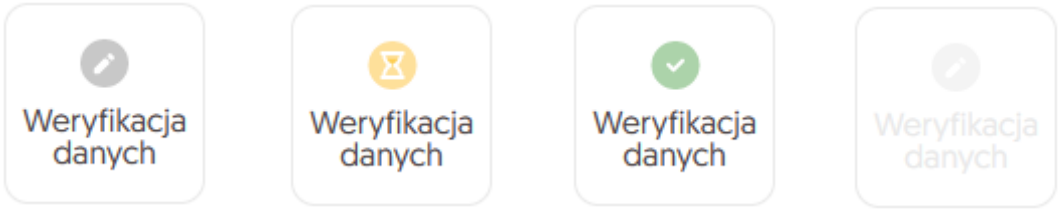
Cyfrowe podpisywanie kodu sprawia, że korzystanie z aplikacji jest bezpieczne, co przekłada się na większe zaufanie do Twojej marki i poszerzenie grona klientów.

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/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

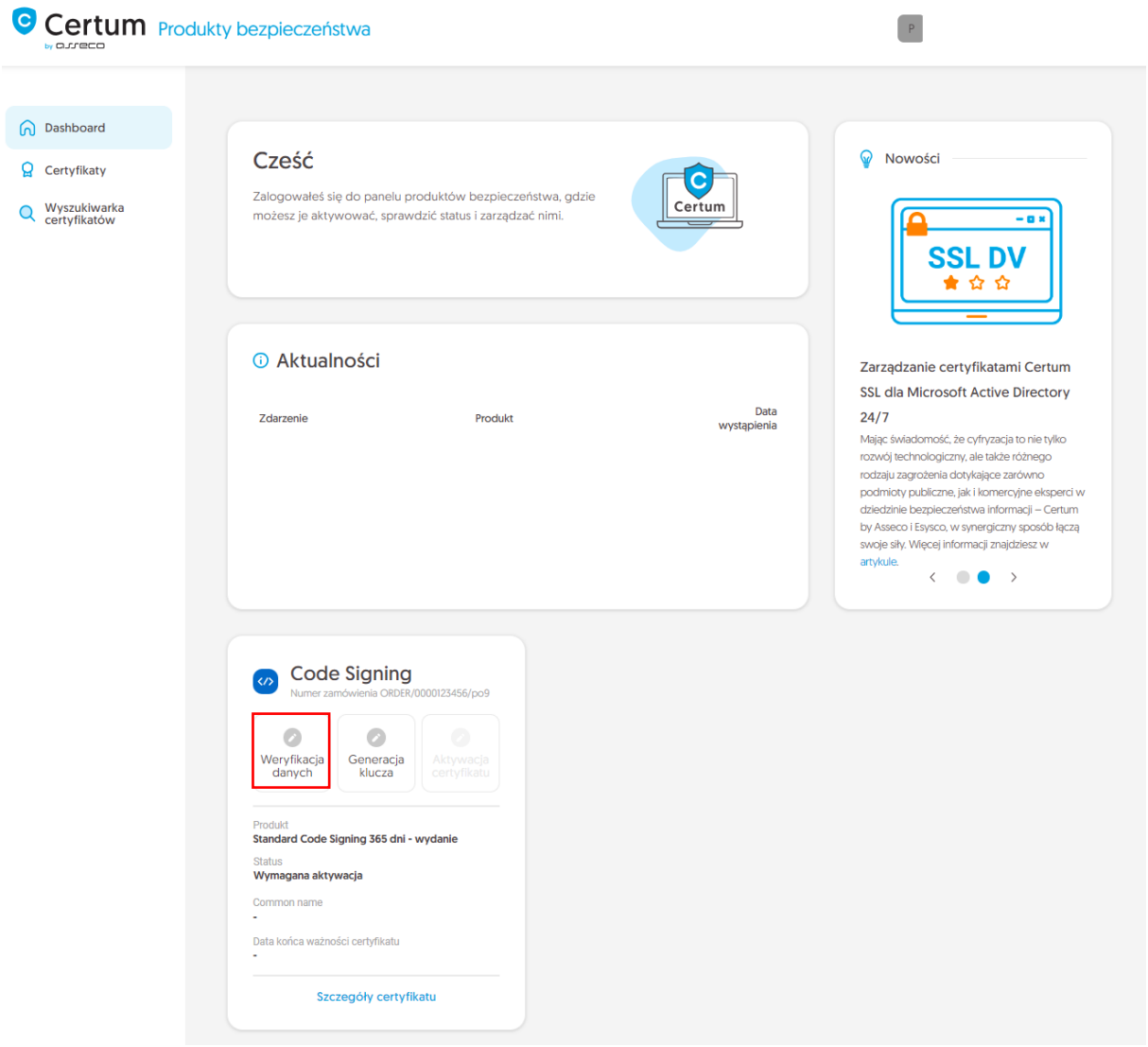
certum.pl
infolinia@certum.pl

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.

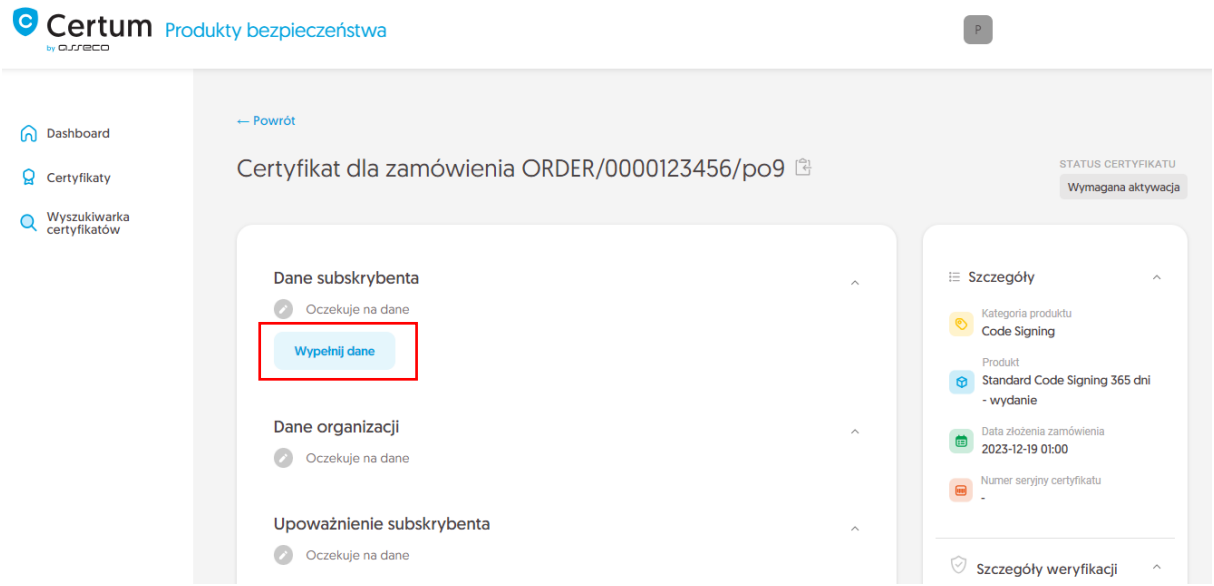
Listę obsługiwanych dokumentów potwierdzających znajdziesz w Informacje o wymaganych dokumentach.

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



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

certum.pl
infolinia@certum.pl



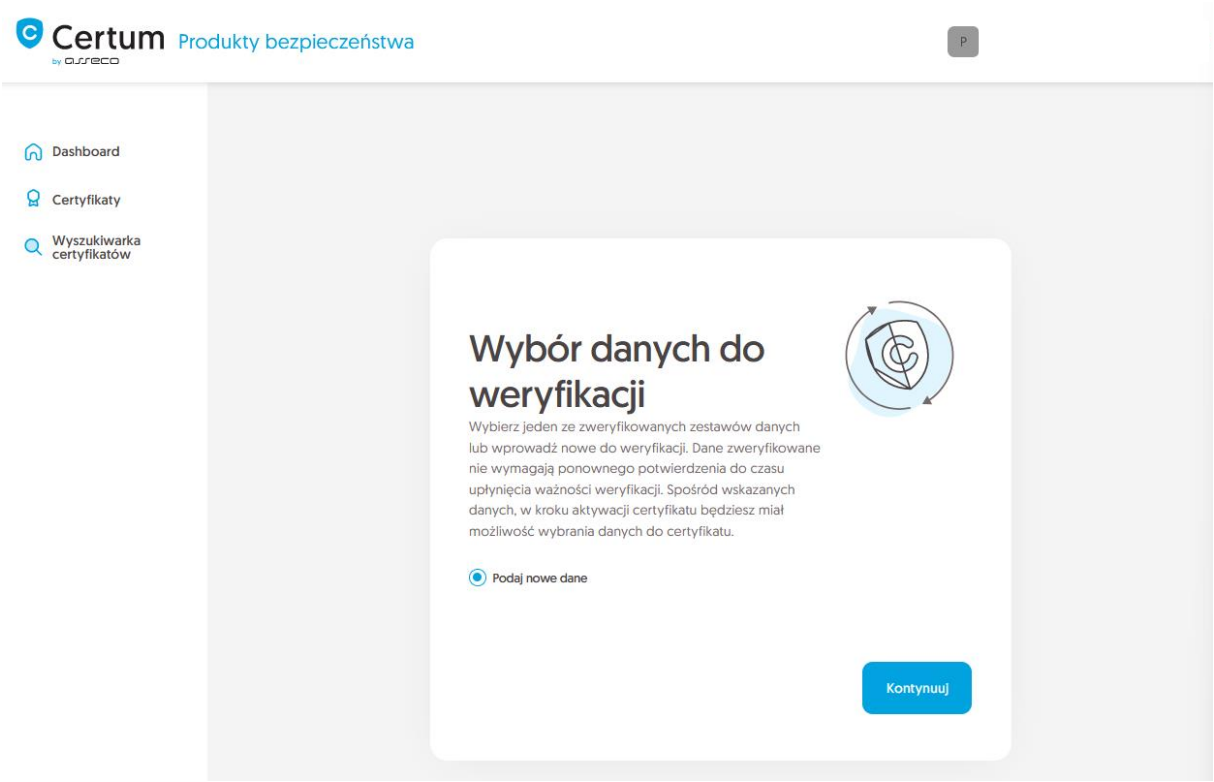
Wybór wariantu danych do weryfikacji

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.

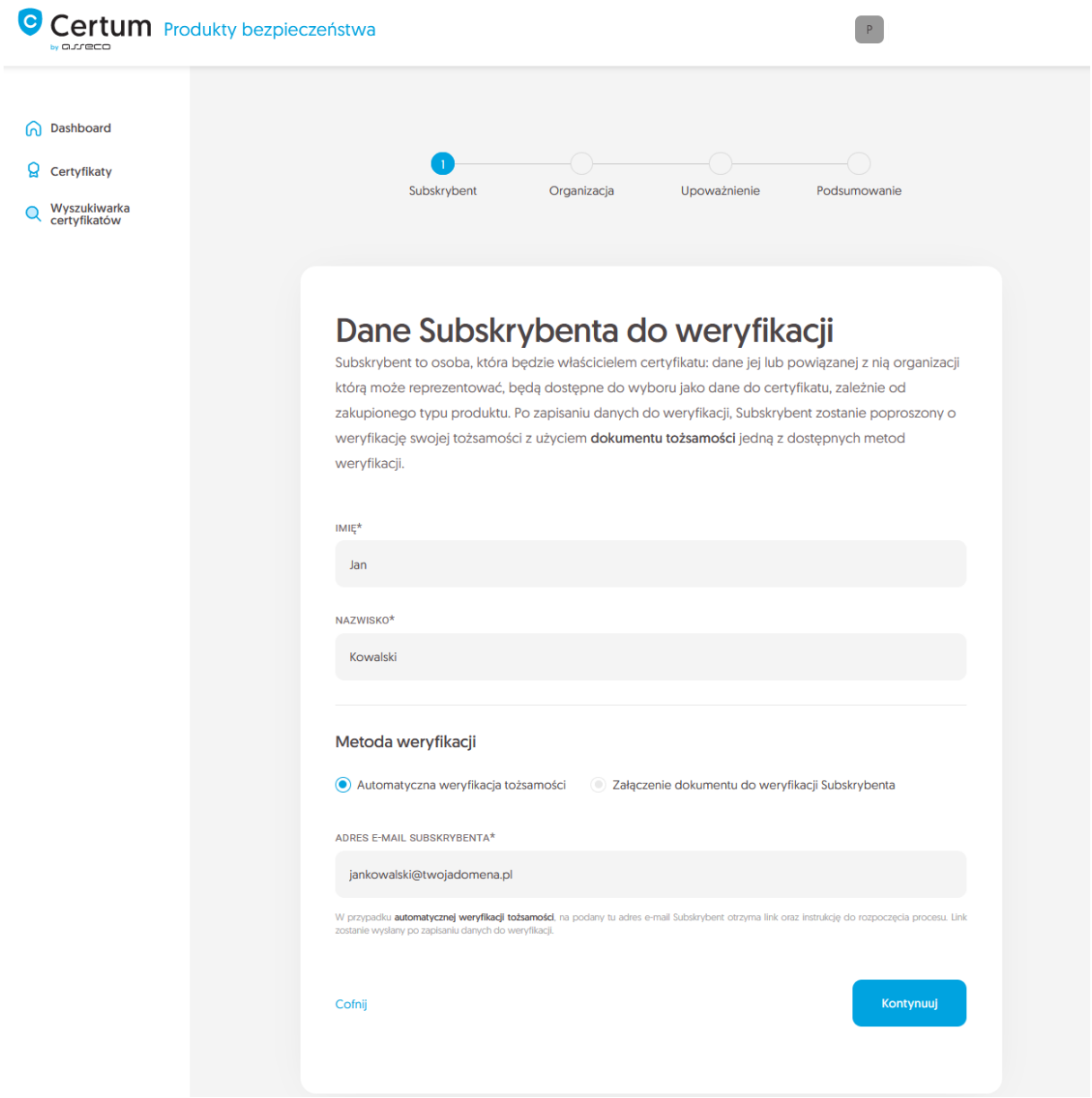
certum.pl
infolinia@certum.pl



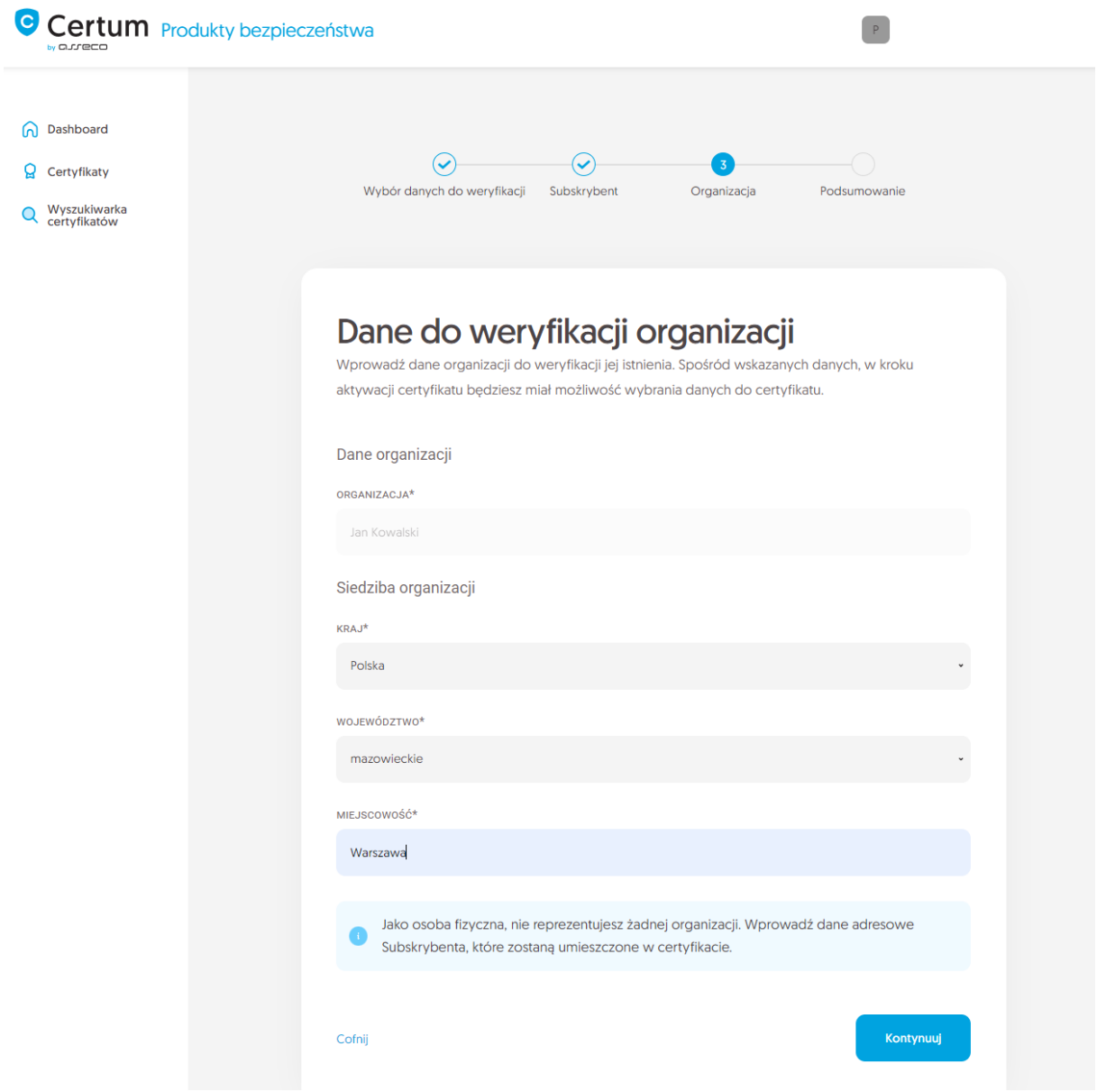
W kolejnym etapie podaj dane Subskrybenta, czyli osoby, która reprezentuje organizację i będzie właścicielem certyfikatu. Imiona i nazwiska zapisz w formularzu tak, jak widnieją na dokumencie tożsamości Subskrybenta.

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.



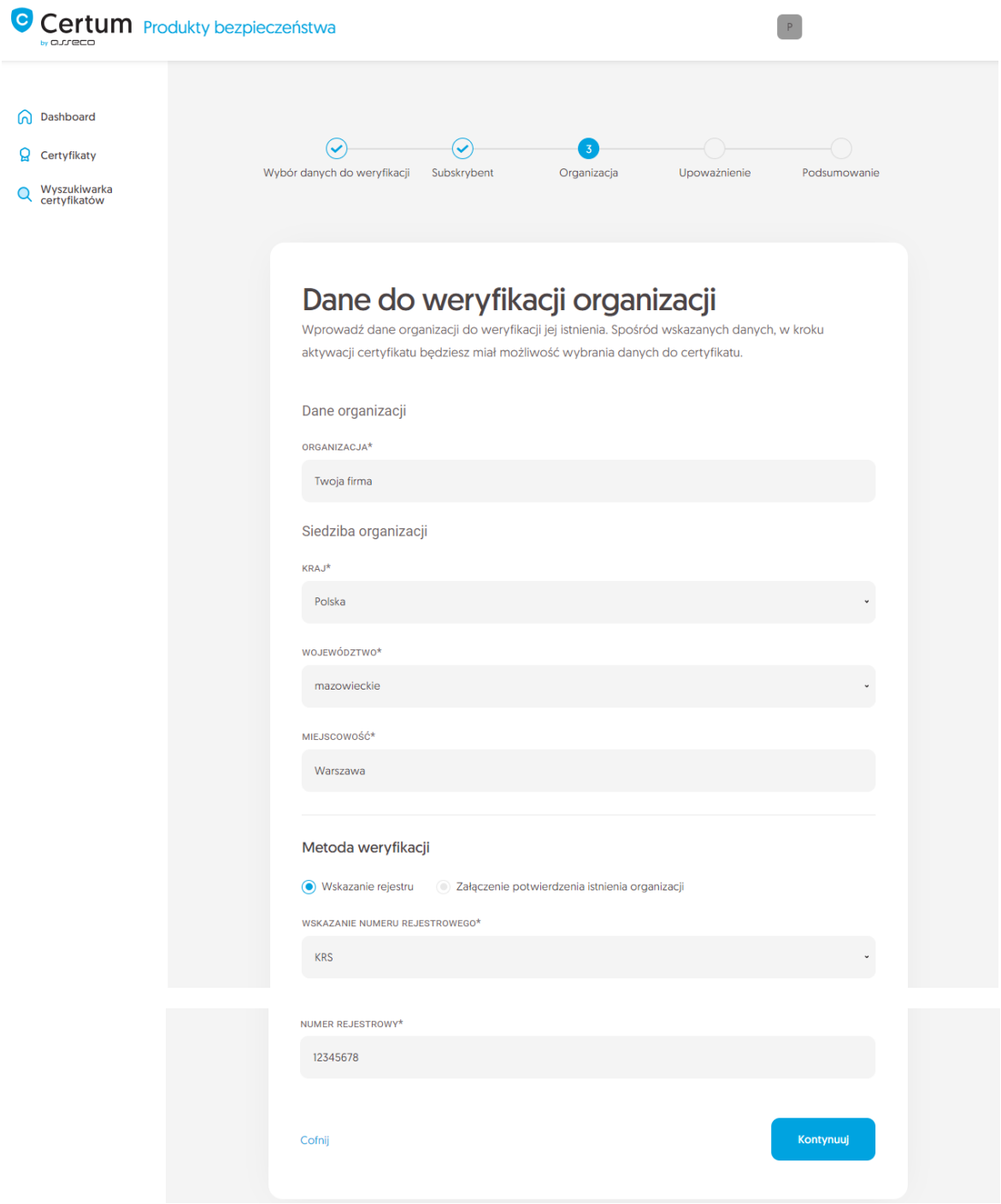
Po wypełnieniu powyższych danych, przejdź do kolejnego etapu czyli podania danych organizacji. Dla certyfikatu w wariancie **osoba fizyczna**, podaj dane adresowe Subskrybenta. Przejdź dalej do podsumowania.



Dla certyfikatów w wariancie **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 istnieje organizacji:

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



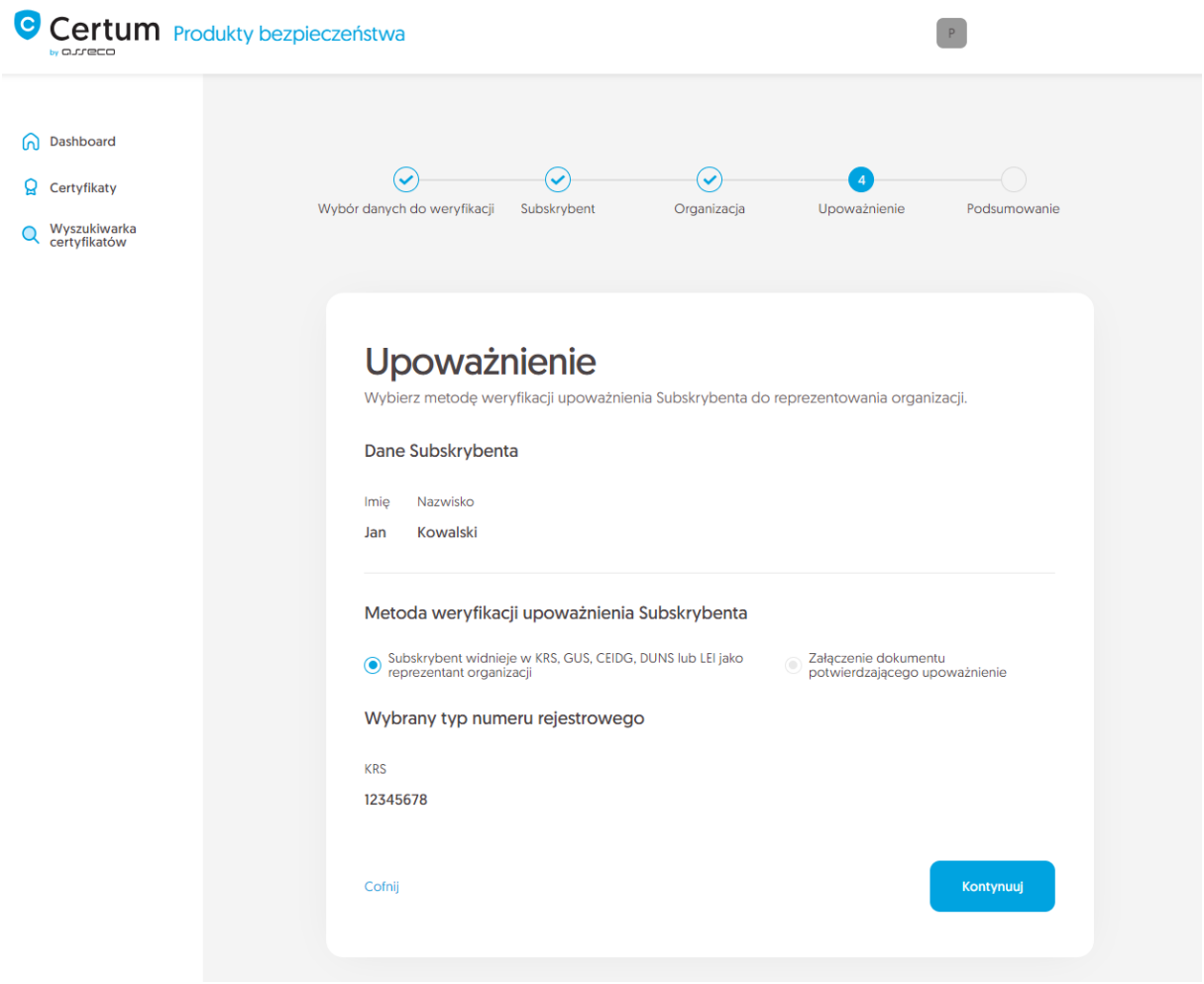
Po wypełnieniu wszystkich wymaganych danych, przejdź do ostatniego etapu kroku podawania danych do weryfikacji, czyli do określenia sposobu weryfikacji upoważnienia Subskrybenta do reprezentowania organizacji. Etap jest wymagany dla wariantów **organizacja** i **sponsor**.

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**.

certum.pl
infolinia@certum.pl

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.

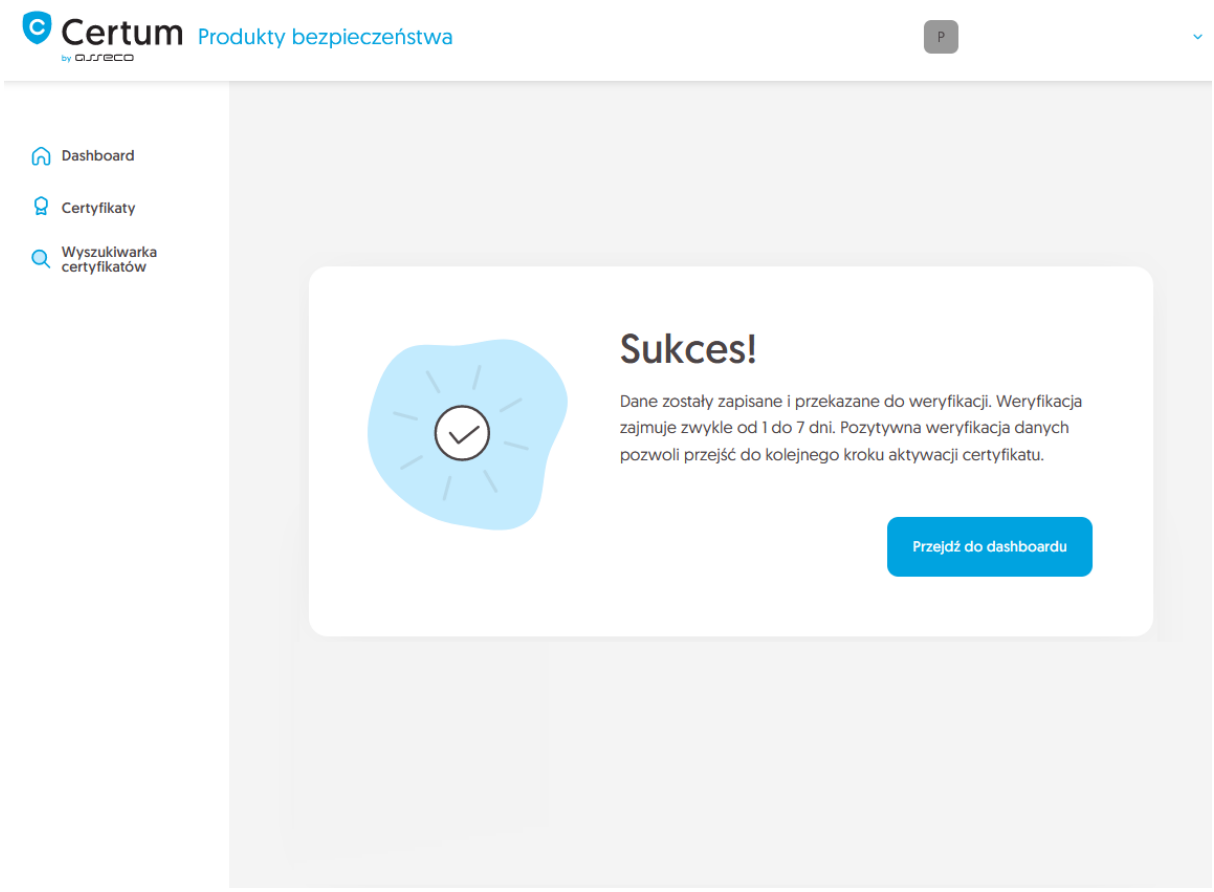


Po wybraniu metody weryfikacji upoważnienia przejdź dalej.

Podsumowanie kroku Weryfikacja danych

Zweryfikuj wprowadzone dane na ekranie podsumowania. Jeśli dane są poprawne, oznacz wymagane oświadczenia i zakończ krok podawania danych do weryfikacji.

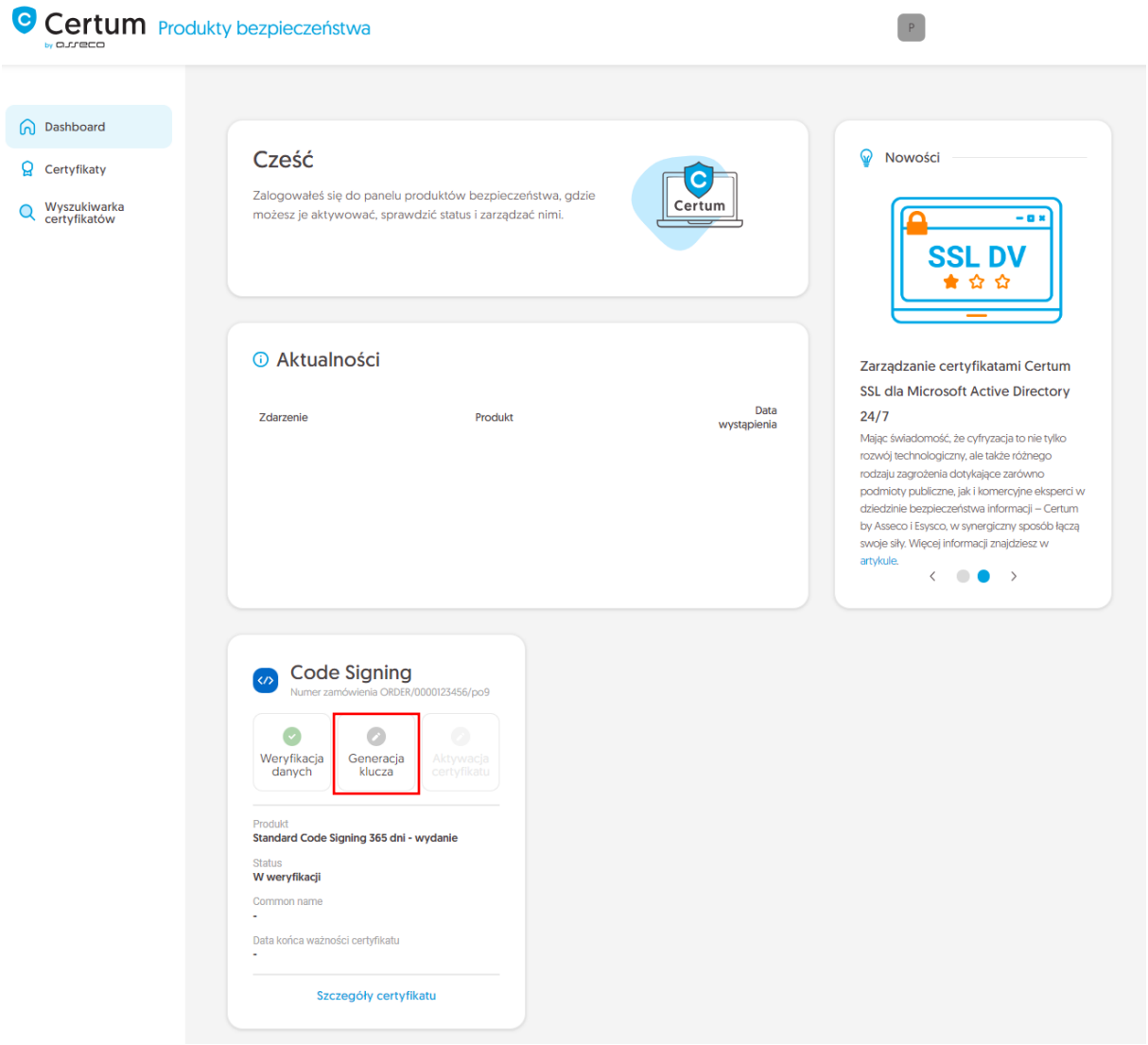
Ekran sukcesu poinformuje Cię o zapisaniu danych do weryfikacji. Certum zajmie się ich weryfikacją. W tym czasie, jeśli chcesz dodać jeszcze jakiś dokument potwierdzający wprowadzone dane, możesz go dodać w szczegółach certyfikatu. Jest to również czas na wykonanie automatycznej weryfikacji tożsamości 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:**



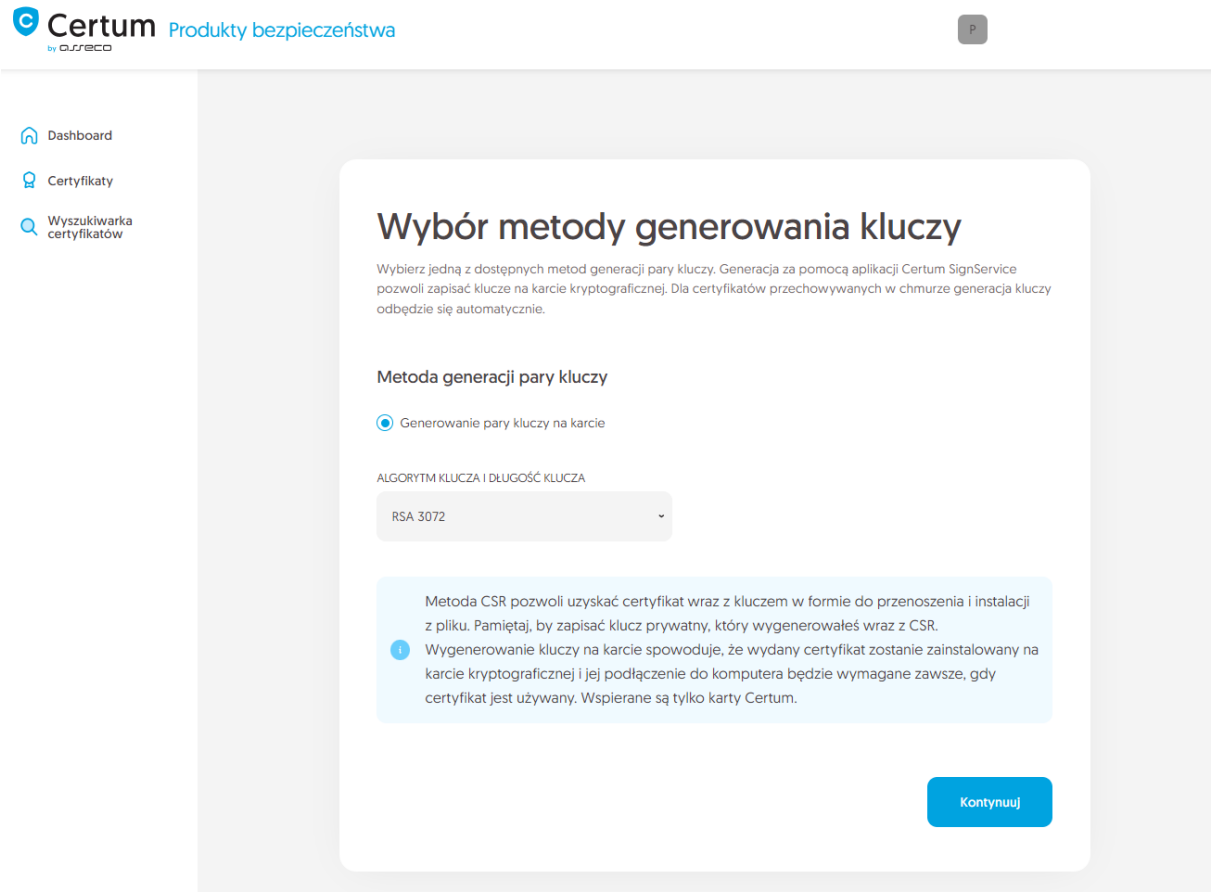
lub analogicznie jak w przypadku kroku **Weryfikacja danych**: z listy **Certyfikaty** – wybierz certyfikat który chcesz aktywować i w szczegółach wybierz opcję **Wygeneruj klucze**.

W tym kroku wygenerujesz parę kluczy do certyfikatu.

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

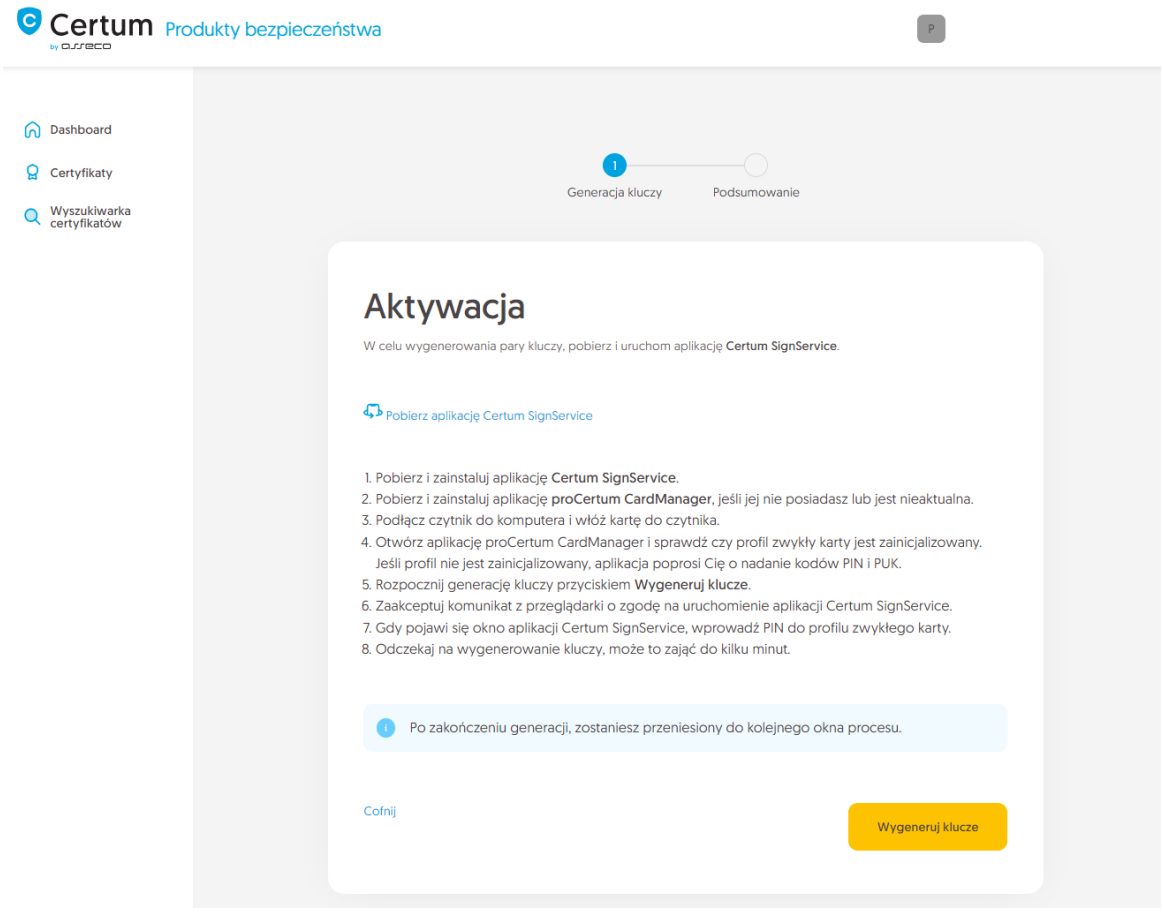
Wybierając metodę generowania pary kluczy na karcie, wybierz również algorytm i długość klucza. Twój wybór powinien zależeć od algorytmu i długości klucza wspieranej przez aplikację, w której używasz certyfikatu lub rekomendację np. Twojego działu IT.

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

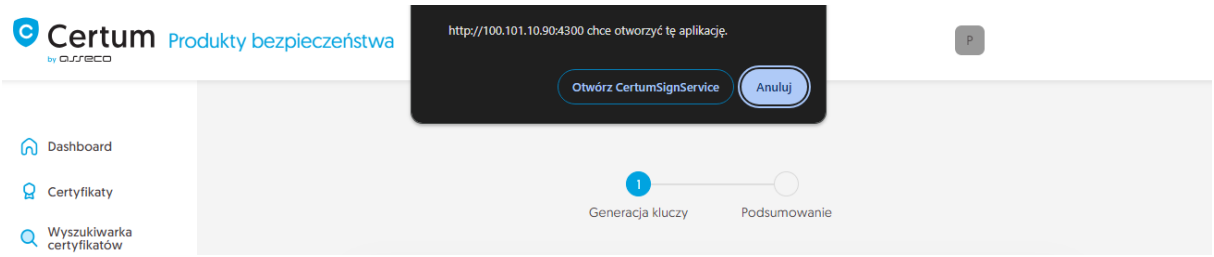


Po przejściu dalej, upewnij się, że posiadasz kartę włożoną do czytnika, czytnik podłączony do komputera, a sama karta ma zainicjalizowany profil zwykły z nadanym kodem PIN. W procesie wymagane jest również posiadanie zainstalowanej na komputerze aplikacji proCertum CardManager, w której możesz również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

Zapraszamy do zapoznania się z instrukcją jak nadać kod PUK i PIN dla profilu zwykłego karty.



Do wygenerowania kluczy na karcie potrzebujesz również zainstalowaną 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.



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.

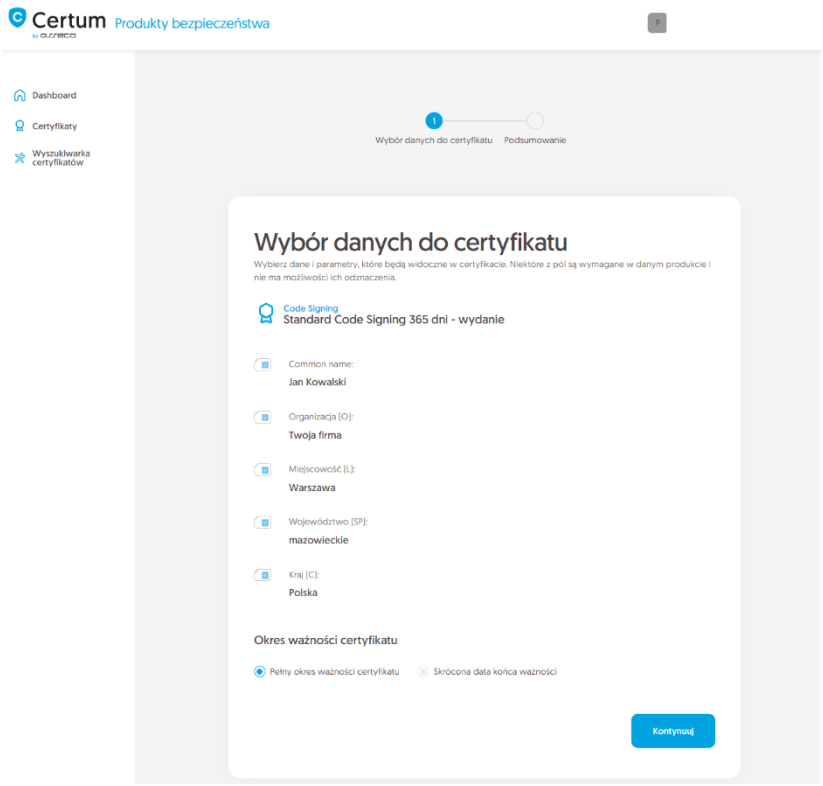
Zweryfikuj wprowadzone dane na ekranie podsumowania. Jeśli dane są poprawne, zakończ krok generacji kluczy.

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.



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 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 Twojego certyfikatu.