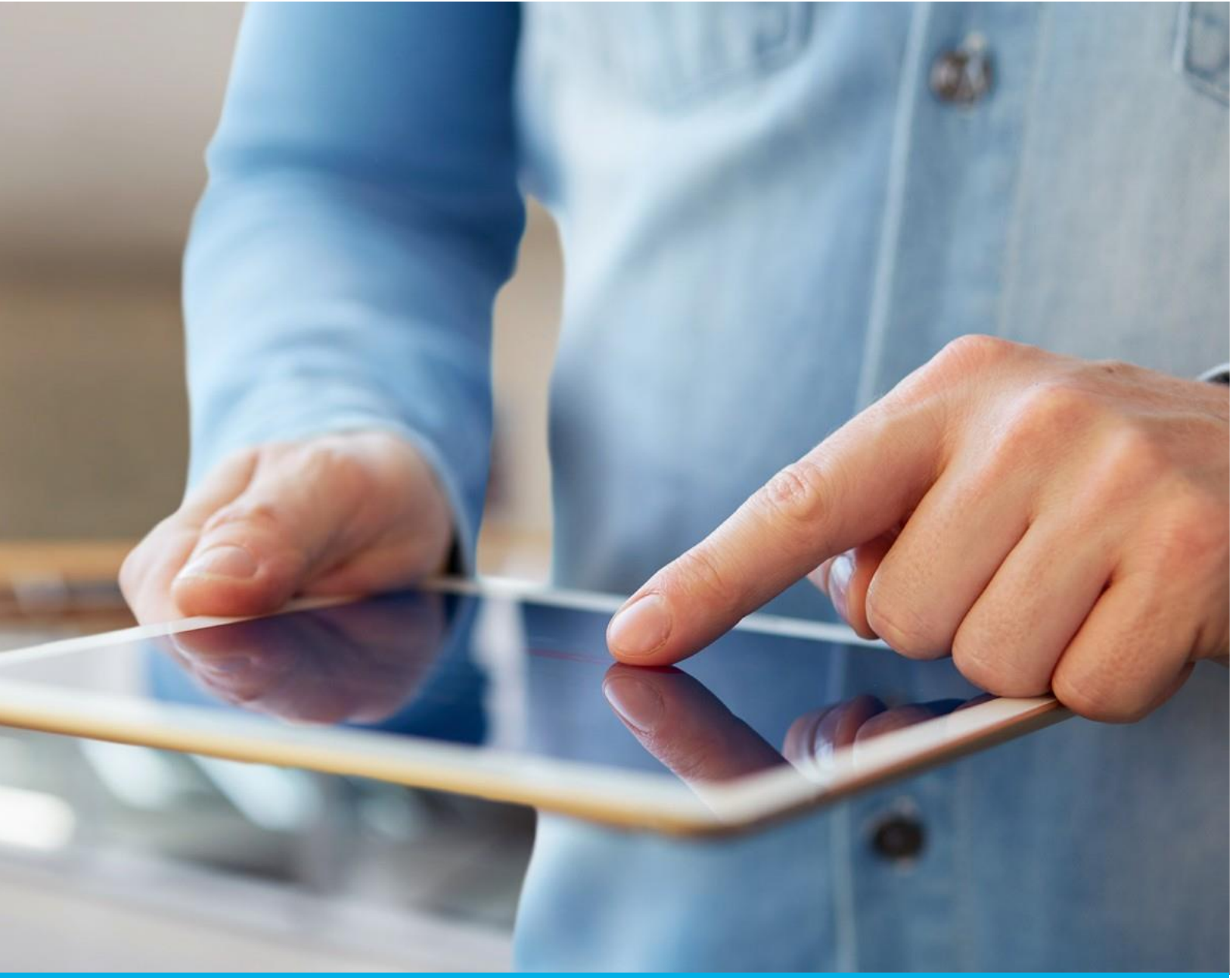


Aktywacja certyfikatu Certum S/MIME Sponsor

Wer. 1.5

asseco

Certum by asseco

Spis treści

1. Opis produktu 3
2. Aktywacja certyfikatu 3
Krok Weryfikacja danych 4
Krok Weryfikacja e-mail 9
Metoda CSR 11
Metoda generowania kluczy na karcie kryptograficznej 12
Podanie adresu e-mail 15
Krok Aktywacja certyfikatu 16

certum.pl
infolinia@certum.pl

1. Opis produktu

Certum S/MIME to certyfikaty stosowane do podpisywania wiadomości e-mail. Umożliwiają one szyfrowanie treści wiadomości, co zapewnia prywatność i poufność poczty elektronicznej.

Dzięki cyfrowemu podpisowi, potwierdzają adres email lub tożsamość nadawcy i gwarantują integralność przesyłanej treści.

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 organizacji oraz ich weryfikacja
- **Weryfikacja e-mail** – wygenerowanie kluczy i podanie e-mail oraz jego weryfikacja
- **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

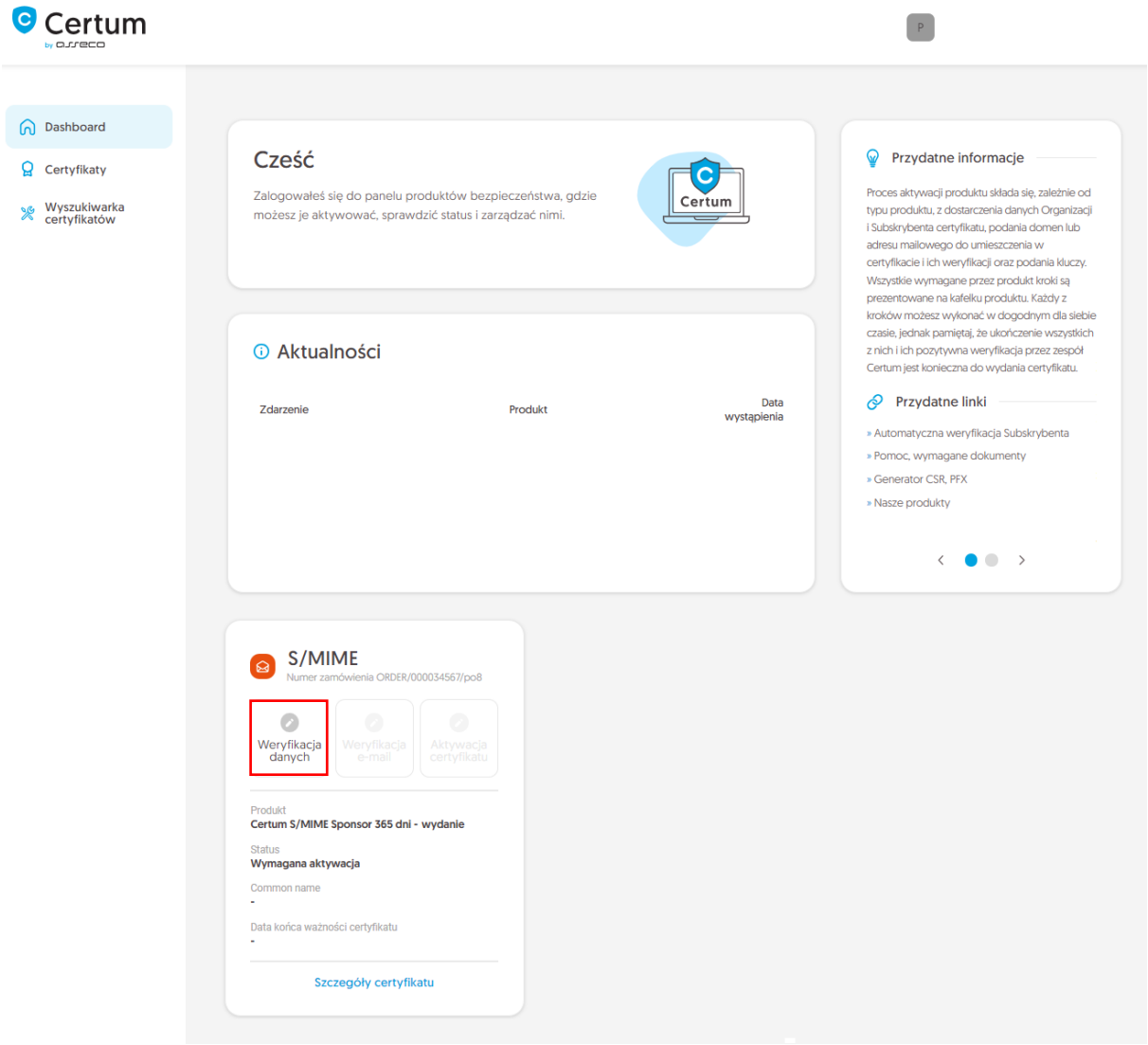
certum.pl
infolinia@certum.pl

Krok Weryfikacja danych

Podanie danych do weryfikacji to krok, w którym 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.

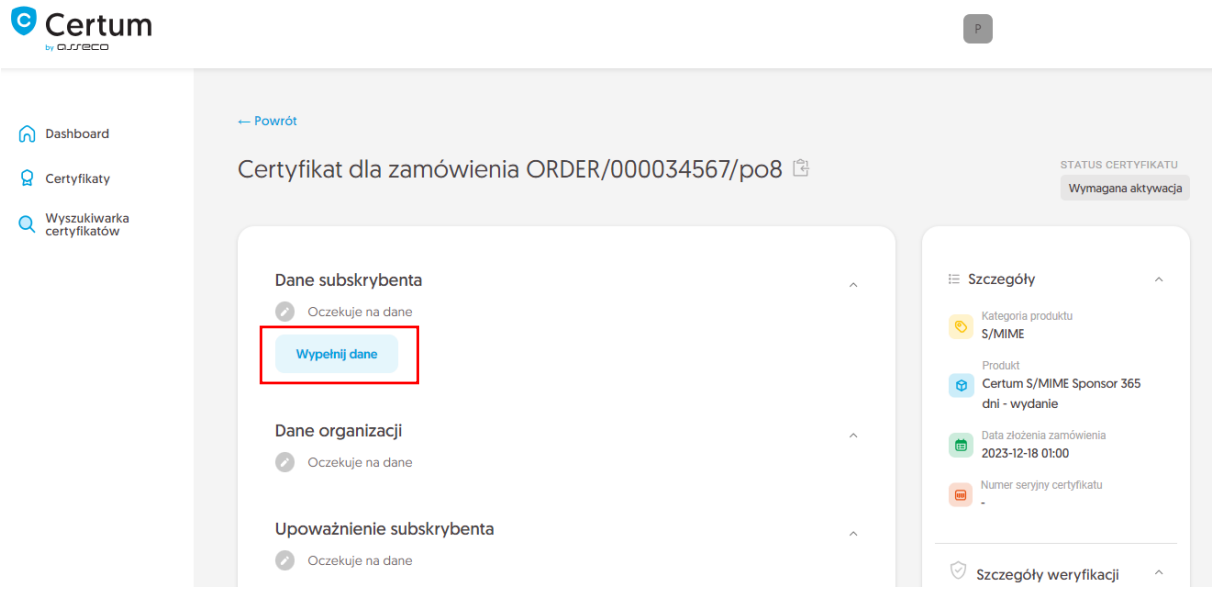
Listę obsługiwanych dokumentów potwierdzających znajdziesz w Informacje o wymaganych dokumentach.

Jako klient, rozpocząć podawanie danych do weryfikacji możesz poprzez **Dashboard**, wybierając opcję **Weryfikacja danych:**



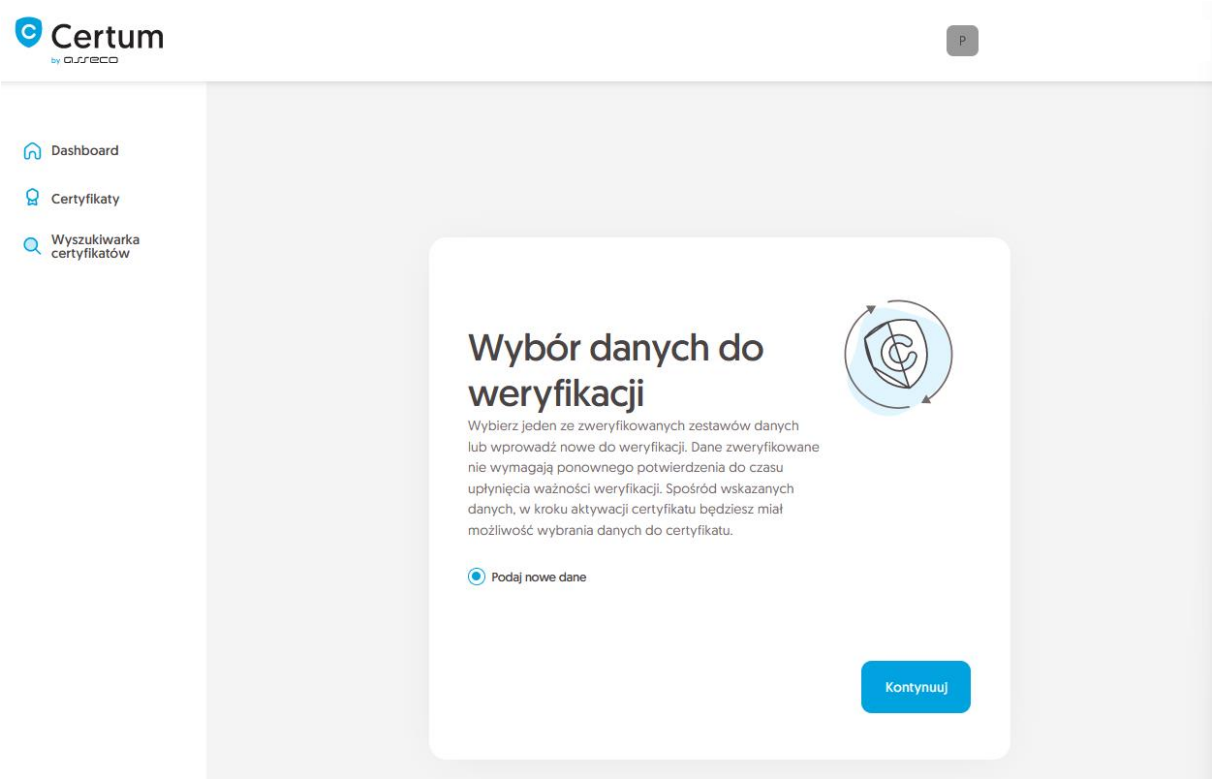
lub z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz przy danych subskrybenta opcję **Wypełnij dane**:

certum.pl
infolinia@certum.pl



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.

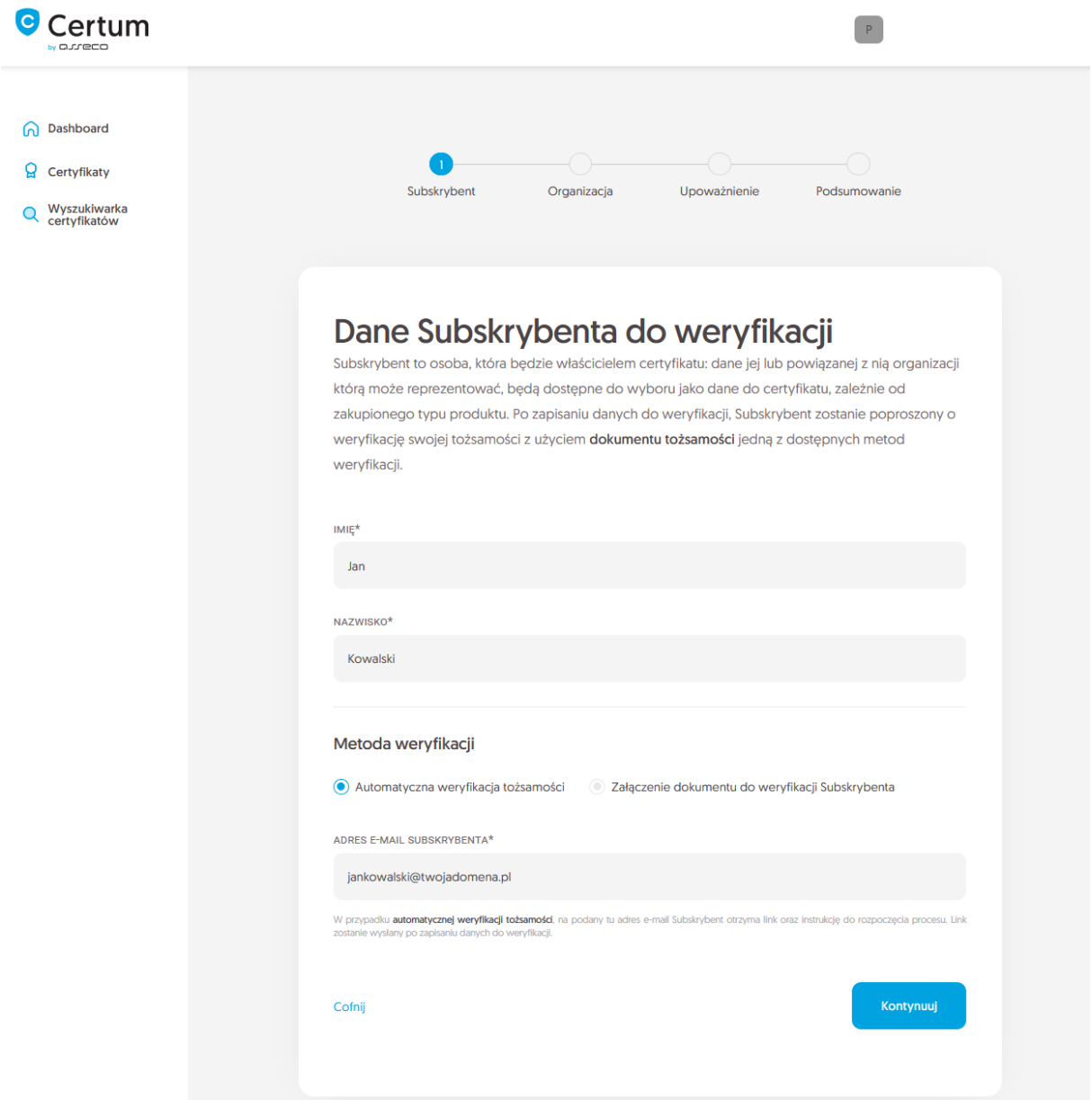
Kreator przeprowadzi Cię przez proces podawania danych. W jego pierwszym etapie wybierz podanie nowych danych. W przyszłości będzie możliwość ich użycia do wydania kolejnego certyfikatu.



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:

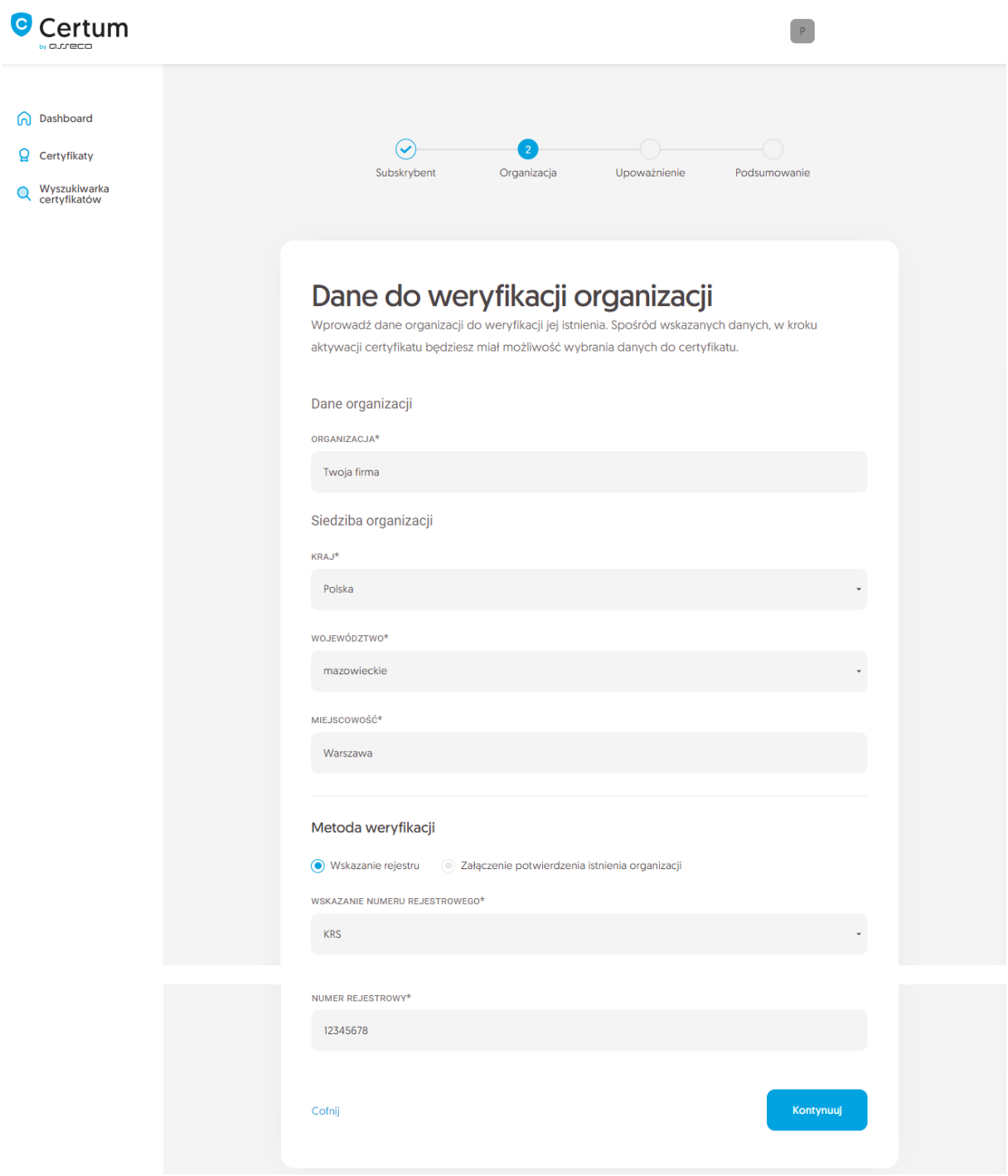
- **Automatyczna weryfikacja tożsamości** – subskrybent otrzyma e-mail z linkiem do serwisu weryfikacji tożsamości z użyciem kamery komputera lub telefonu i dokumentu tożsamości
- **Załączenie dokumentu** – dodasz skan dokumentu tożsamości subskrybenta lub skan potwierdzenia tożsamości.



Po wypełnieniu powyższych danych, przejdź do kolejnego etapu, czyli podania danych organizacji. W tym miejscu 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.

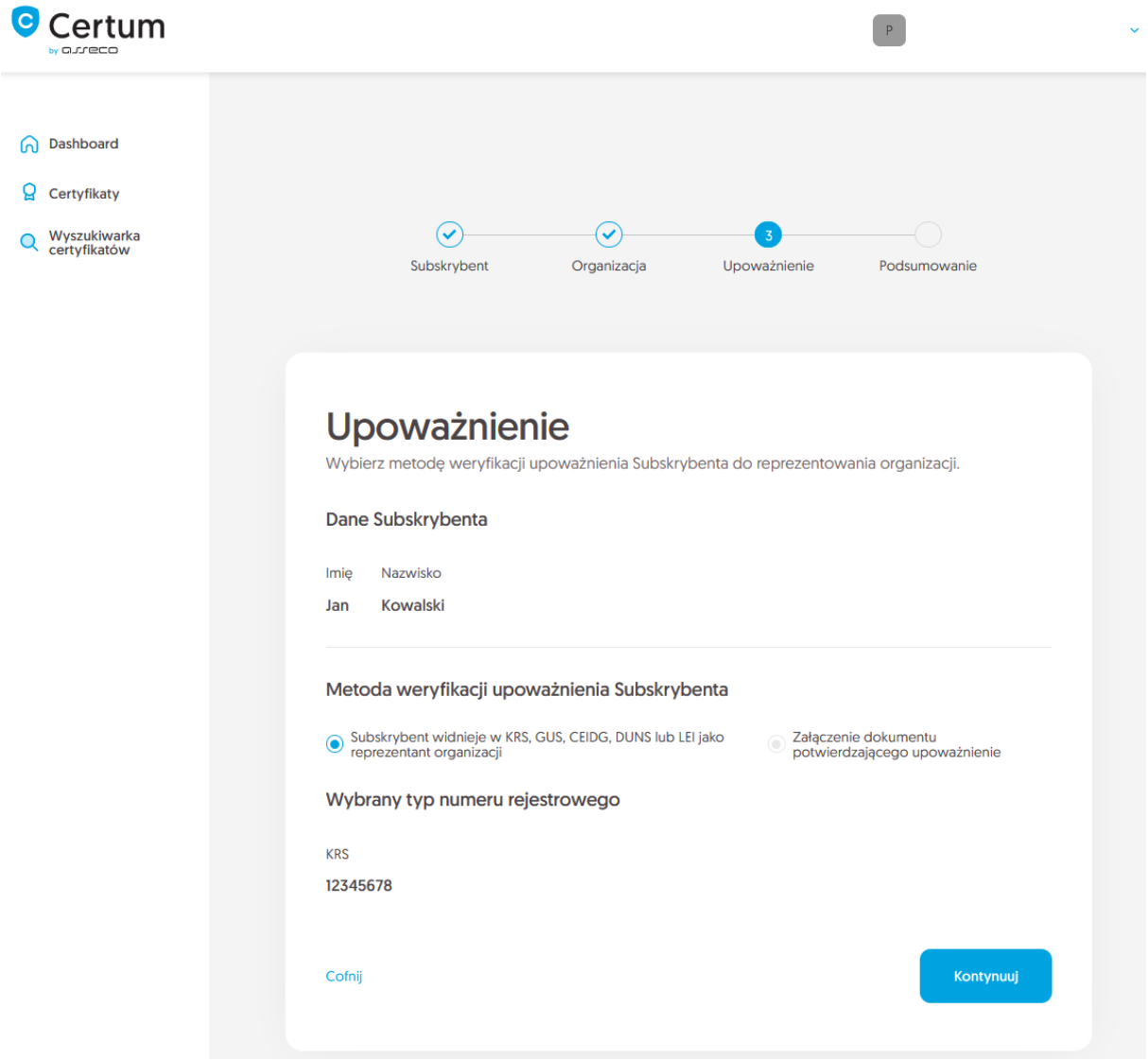


Po wypełnieniu wszystkich wymaganych danych, przejdź do ostatniego etapu kroku podawania danych do weryfikacji, czyli do określenia sposobu weryfikacji upoważnienia subskrybenta do reprezentowania organizacji.

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**.

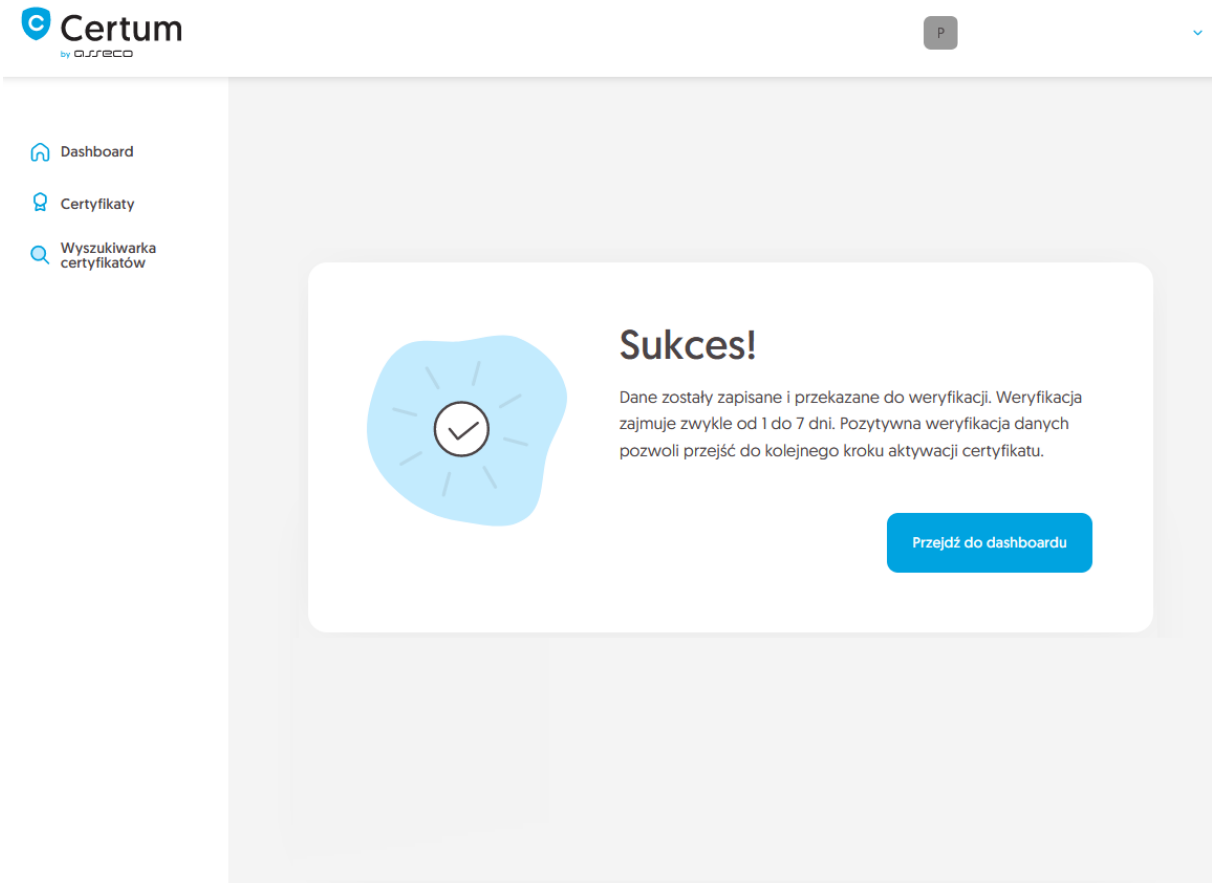
Na metodę weryfikacji upoważnienia subskrybenta ma również wpływ wybrana metoda weryfikacji organizacji. Jeśli został tam podany numer rejestrowy i jego typ, Certum w pierwszej kolejności poszuka czy subskrybent widnieje w rejestrze, a samą metodę weryfikacji upoważnienia subskrybenta system automatycznie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



Po wybraniu metody weryfikacji upoważnienia i przejściu dalej, 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.

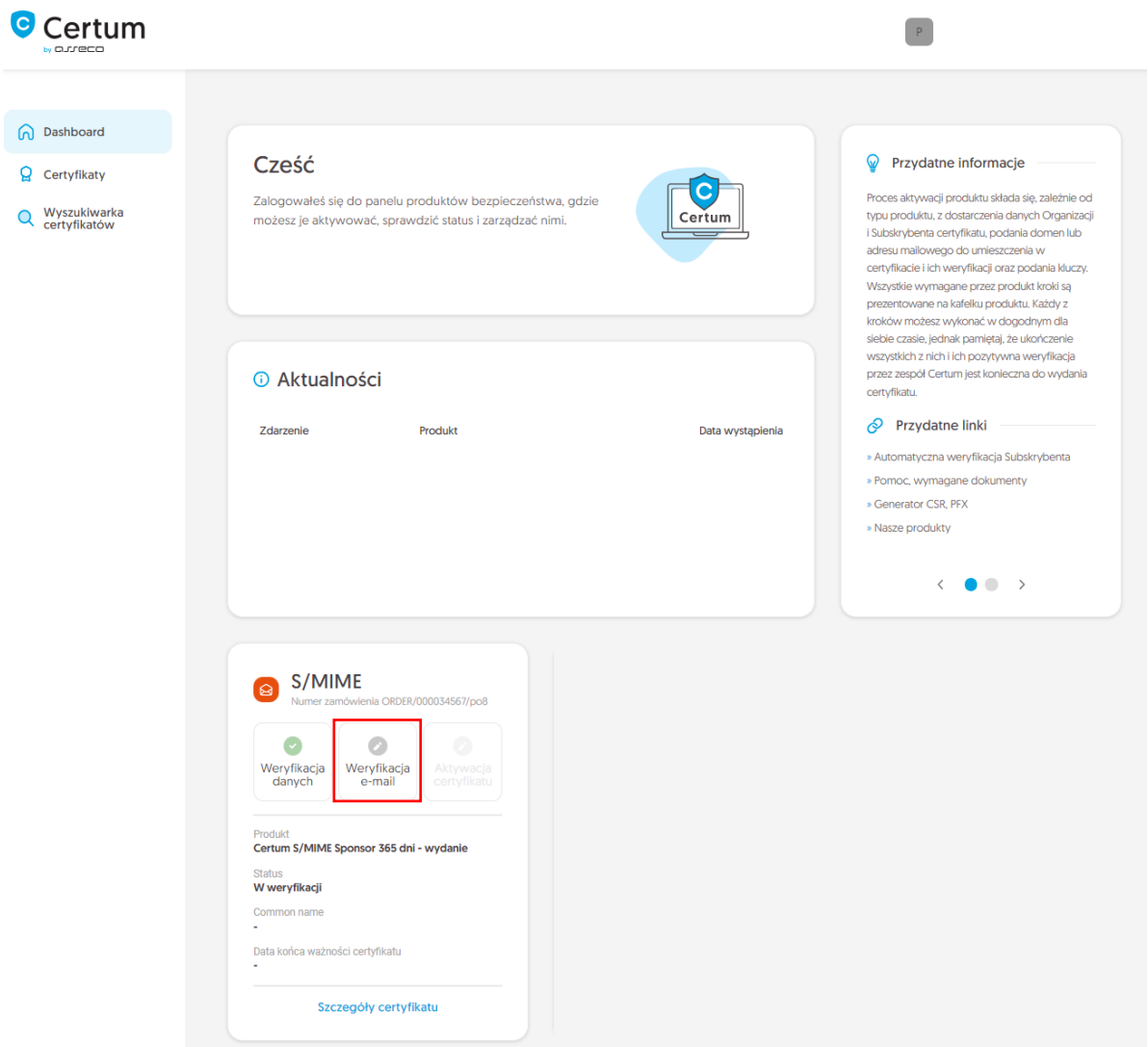
certum.pl
infolinia@certum.pl



Pozytywna weryfikacja podanych danych pozwoli przejść do kroku wygenerowania kluczy i podania adresu e-mail.

Krok Weryfikacja e-mail

Rozpoczęcie generacji pary kluczy i podania e-mail możesz poprzez **Dashboard**, wybierając opcję **Weryfikacja e-mail:**



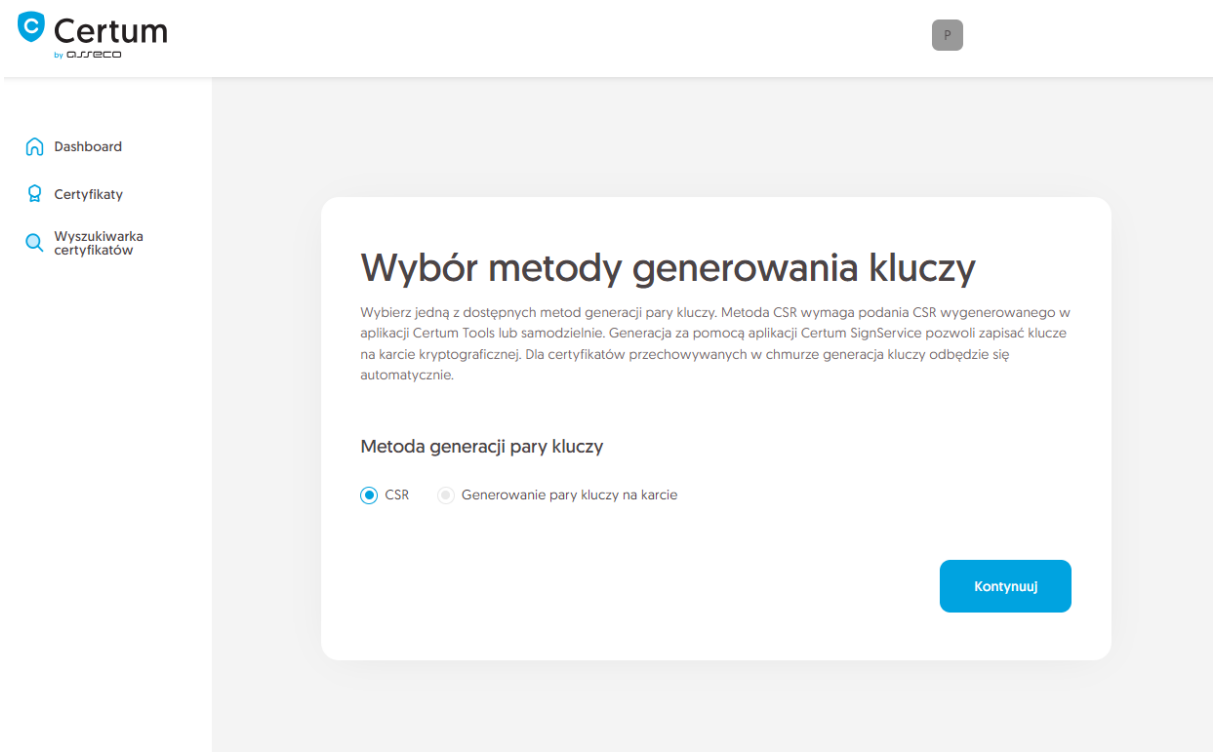
lub analogicznie jak w przypadku kroku **Weryfikacja danych**: z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz opcję **Podaj adres e-mail**.

W tym kroku wygenerujesz parę kluczy oraz podasz adres e-mail do umieszczenia w certyfikacie.

Dla certyfikatów S/MIME dostępnymi metodami generacji kluczy są:

- **CSR** – żądanie podpisania certyfikatu, wygenerowane poprzez generator np. Certum Tools lub aplikację/serwer, na którym będzie zainstalowany certyfikat
- **Generowanie pary kluczy na karcie** – klucze zostaną zapisane na karcie kryptograficznej.

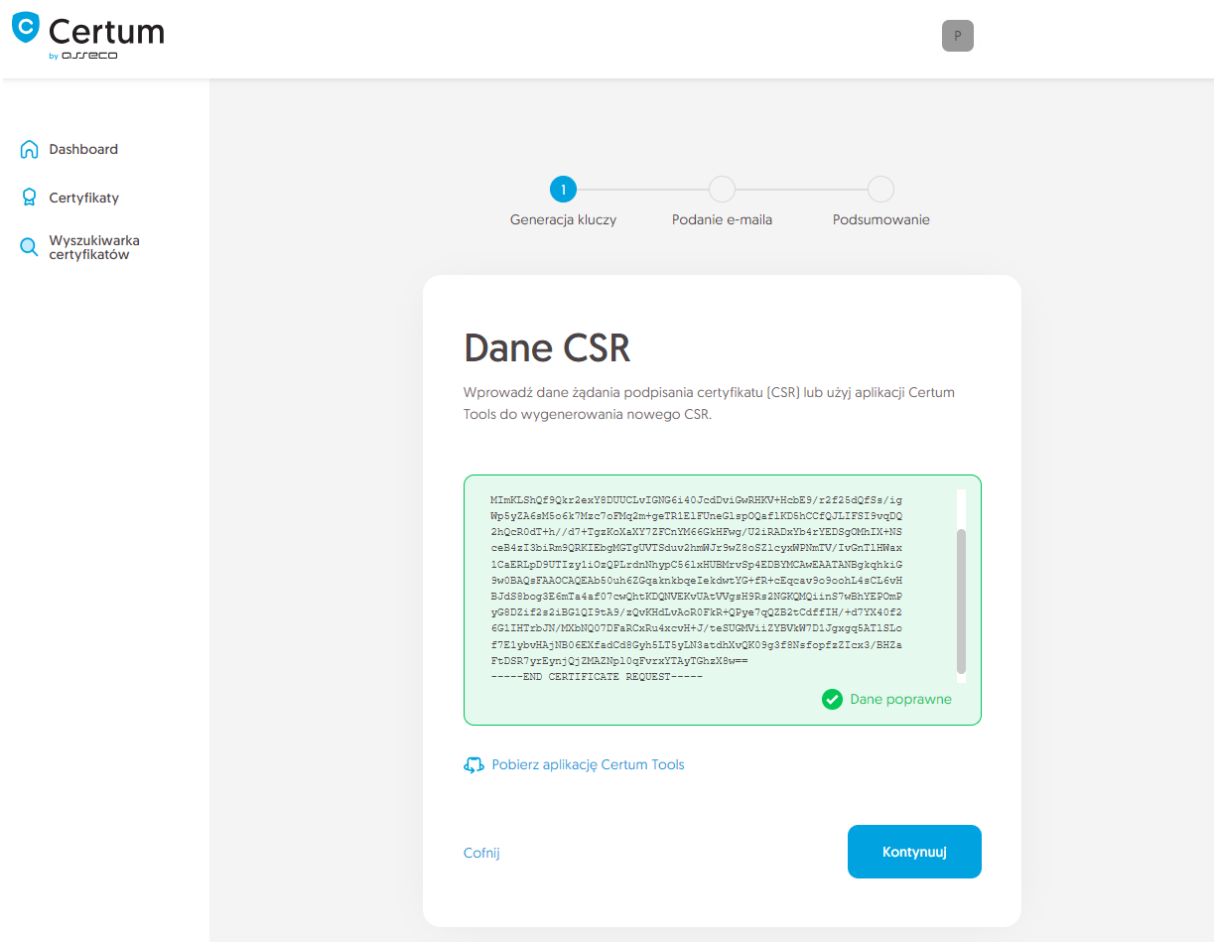
Wybierając metodę generowania pary kluczy na karcie, wybierz również algorytm i długość klucza. Twój wybór powinien zależeć od algorytmu i długości klucza wspieranej przez aplikację, w której używasz certyfikatu lub rekomendację np. Twojego działu IT.



Metoda CSR

Po wybraniu metody CSR, możesz przejść dalej do podania CSR. Na tym etapie będziesz mógł pobrać aplikację Certum Tools do wygenerowania CSR lub dostarczyć własny.

Po przejściu dalej, wklej posiadany CSR. Po wklejeniu CSR, zostanie on zweryfikowany czy jest poprawny. W razie wystąpienia błędu CSR, pojawi się o tym informacja w komunikacie błędu.

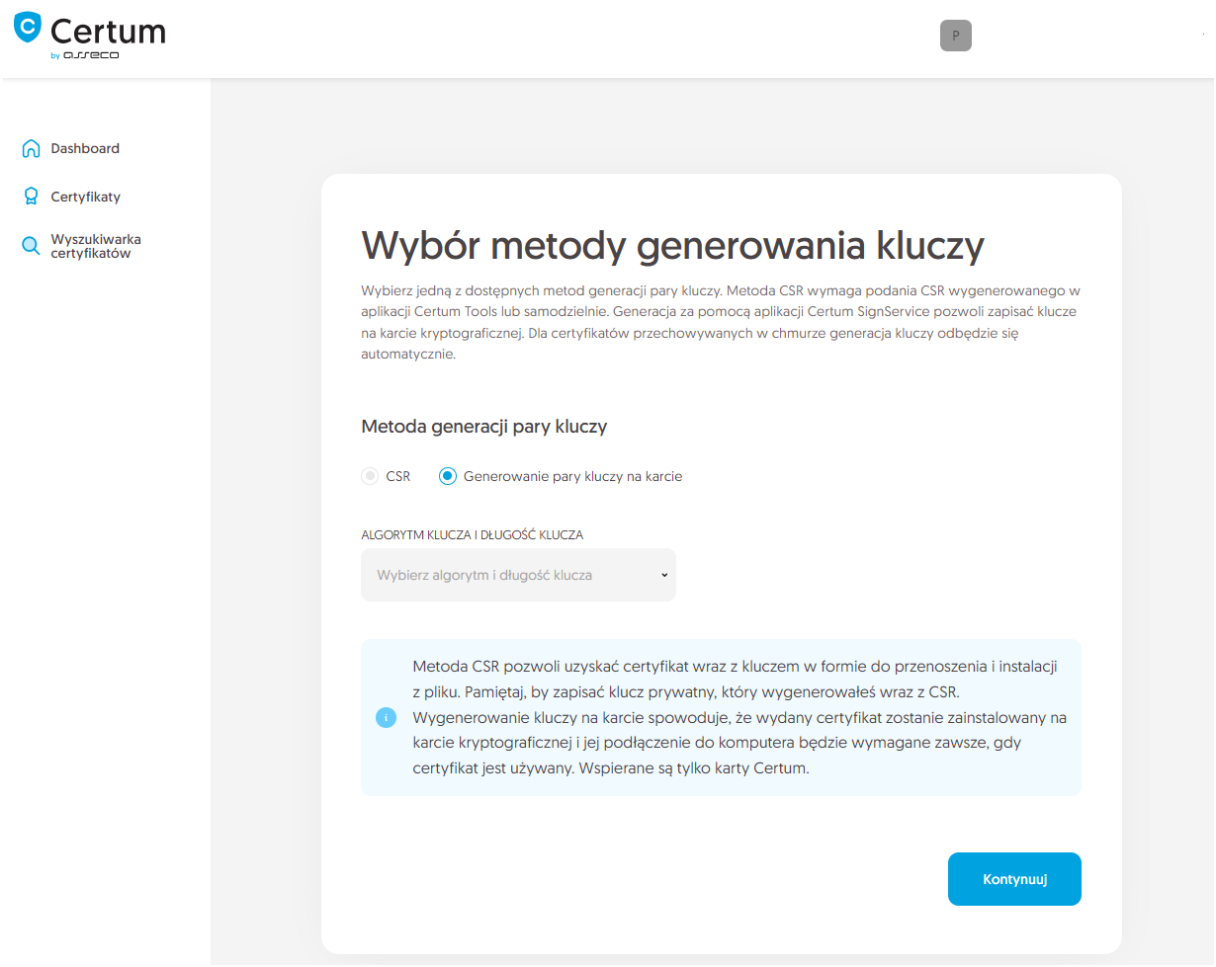


Pamiętaj, aby w przypadku wygenerowania CSR w generatorze, zapisać i zachować klucz prywatny. Będzie on niezbędny do zainstalowania certyfikatu po jego wydaniu.

Podanie prawidłowego CSR i przejście dalej pozwoli podać e-mail do certyfikatu.

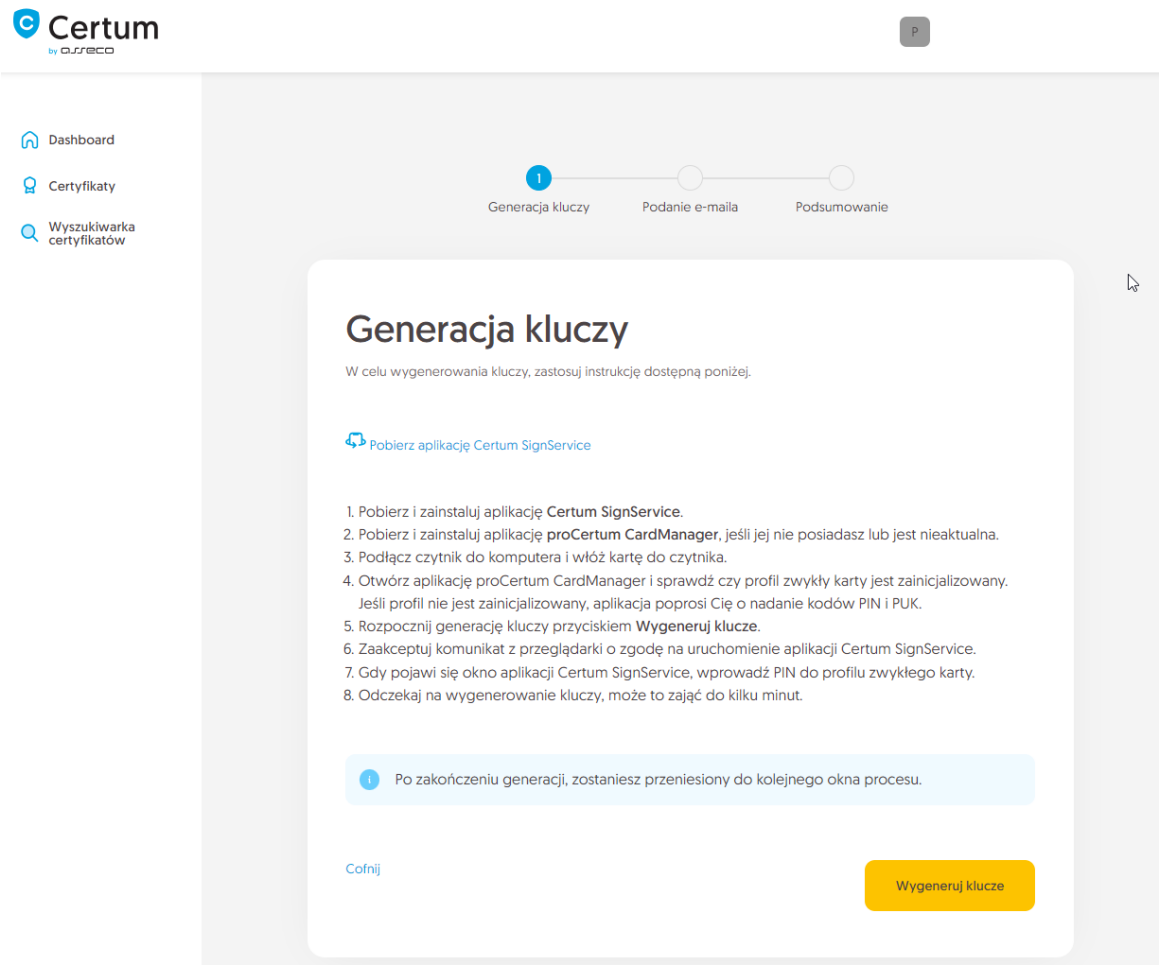
Metoda generowania kluczy na karcie kryptograficznej

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

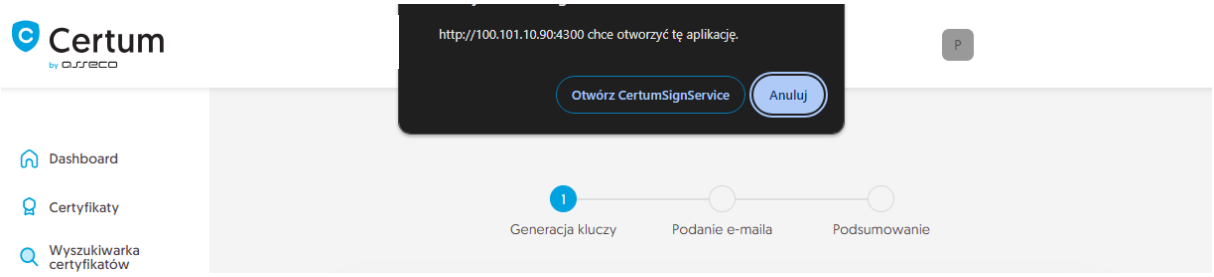


Po przejściu dalej, upewnij się, że posiadasz kartę włożoną do czytnika, czytnik podłączony do komputera, a sama karta ma zainicjalizowany profil zwykły z nadanym kodem PIN. W procesie wymagane jest również posiadanie zainstalowanej na komputerze aplikacji proCertum CardManager, w której możesz również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

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



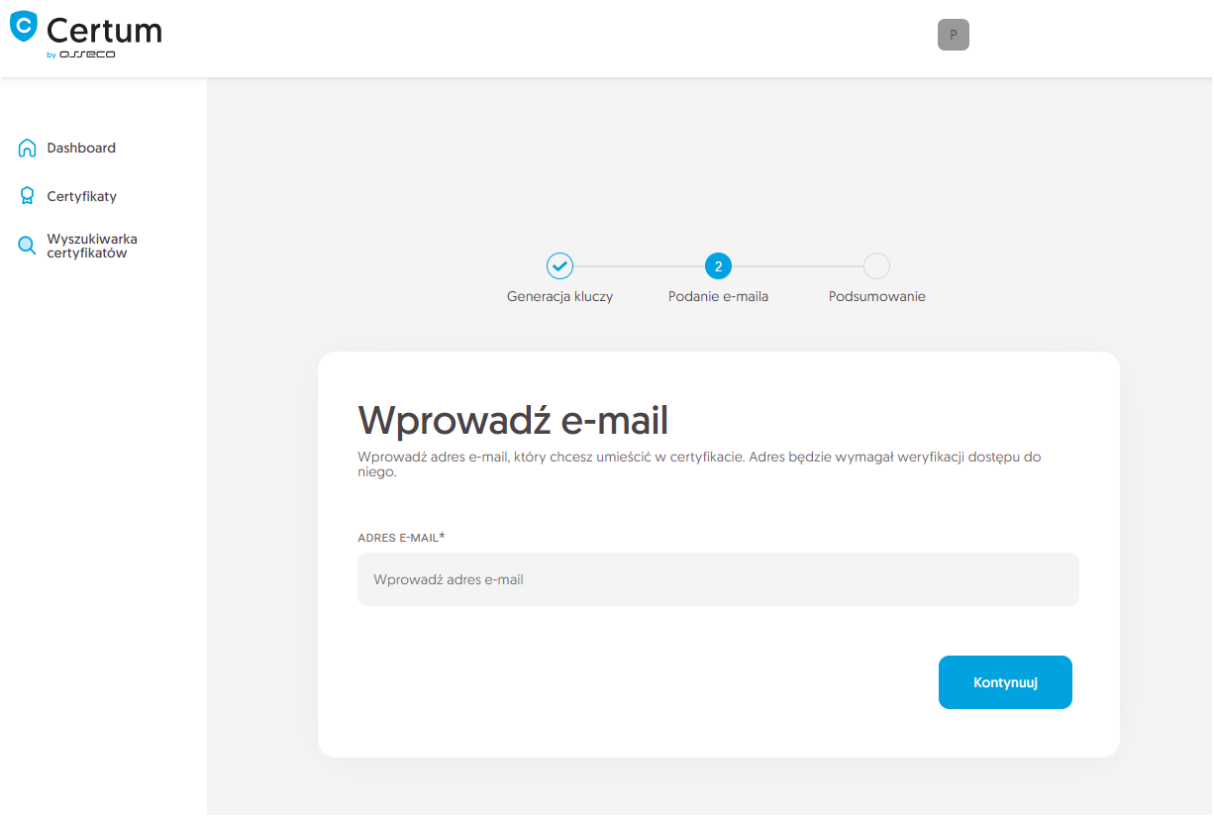
Do wygenerowania kluczy na karcie potrzebujesz również zainstalowaną na komputerze aplikację Certum SignService. Aplikacja Certum SignService po uruchomieniu generowania kluczy, poprosi o zgodę na uruchomienie się i podanie kodu PIN profilu zwykłego karty w celu wygenerowania na niej kluczy.



Po wpisaniu kodu PIN rozpocznie się proces generowania klucza na karcie. Może to zająć do kilkudziesięciu sekund. Wygenerowanie klucza pozwoli podać e-mail do certyfikatu.

Podanie adresu e-mail

Wprowadź adres e-mail i przejdź do podsumowania.



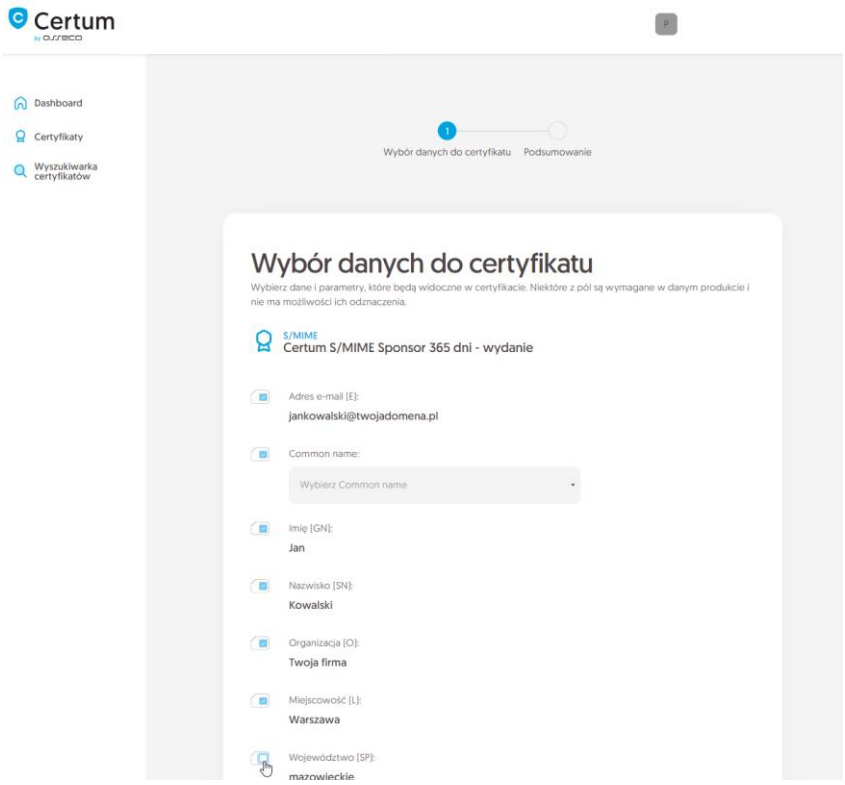
Zweryfikuj wprowadzone dane na ekranie podsumowania. Jeśli dane są poprawne, zakończ krok podawania adresu e-mail.

Ekran sukcesu poinformuje Cię o zapisaniu adresu e-mail. Przeprowadź jego weryfikację. Po ukończeniu weryfikacji adresu e-mail jego status powinien zmienić się na „zweryfikowano”, co pozwoli 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 Common name certyfikatu oraz 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 oświadczenia jeśli są wymagane i zakończ aktywację certyfikatu.

Ekran sukcesu poinformuje Cię o przekazaniu certyfikatu do wydania. 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 wydanego certyfikatu.

Jeśli potrzebujesz pliku PFX, możesz skorzystać z generatora Certum Tools.