

Aktywacja certyfikatu Certum S/MIME Sponsor

Wer. 1.4

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

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.

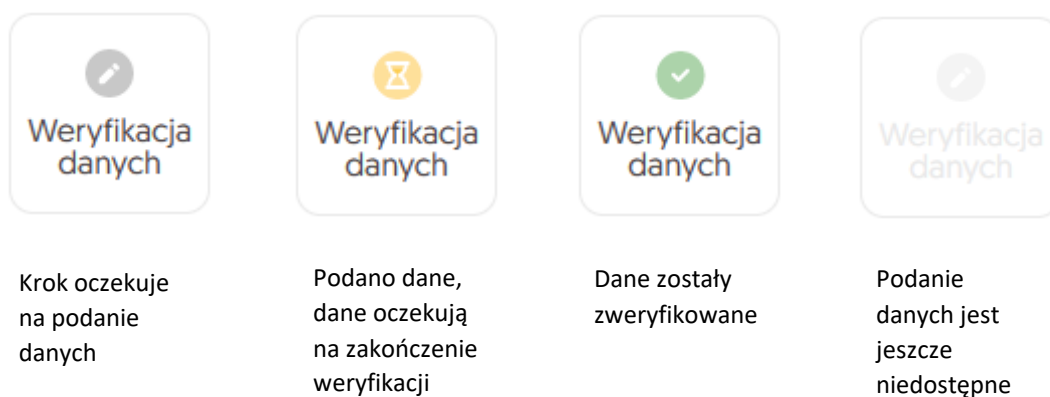
Dzięki cyfrowemu podpisowi, potwierdzają adres email lub tożsamość nadawcy i gwarantują integralność przesyłanej treści.

2. Aktywacja certyfikatu

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 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 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](#).

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

The screenshot shows the Certum dashboard interface. On the left is a sidebar with navigation links: Dashboard, Certyfikaty, and Wyszukiwarka certyfikatów. The main content area is divided into several sections. At the top, there's a 'Cześć' (Hello) message and a 'Przydatne informacje' (Useful information) section. Below that is an 'Aktualności' (News) section with a table of events. The bottom section is titled 'S/MIME' and contains three buttons: 'Weryfikacja danych' (highlighted with a red box), 'Weryfikacja e-mail', and 'Aktywacja certyfikatu'. Below these buttons, there's a summary of the product: 'Certum S/MIME Sponsor 365 dni - wydanie', status 'Wymagana aktywacja', and a link to 'Szczegóły certyfikatu'.

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

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.

Certum Produkty bezpieczeństwa

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów

Subskrybent Organizacja Upoważnienie Podsumowanie

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@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. 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 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.

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 Produkty bezpieczeństwa

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów

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

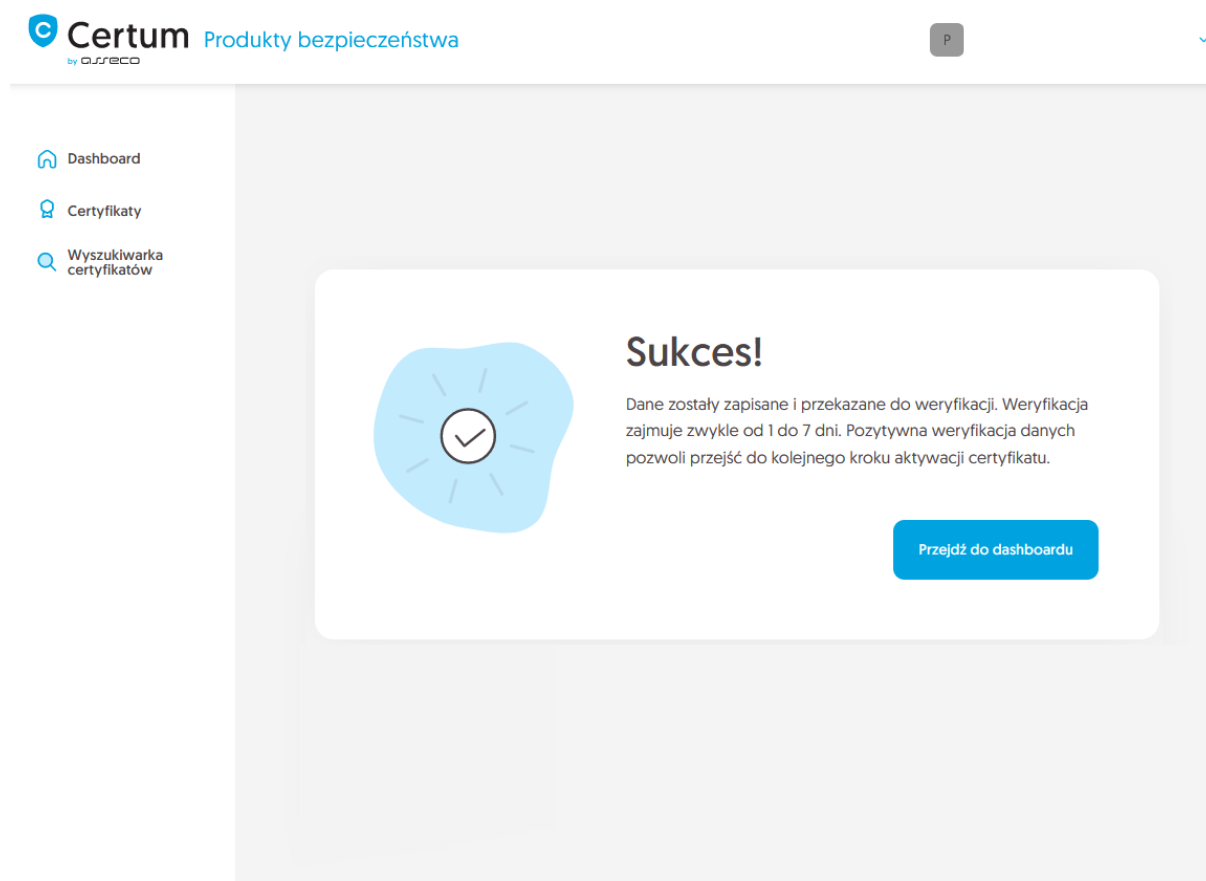
Wybrany typ numeru rejestrowego

KRS
12345678

Cofnij Kontynuuj

Po wybraniu metody weryfikacji upoważnienia i przejściu dalej, zweryfikuj wprowadzone dane na ekranie podsumowania. Jeśli dane są poprawne, oznacz wymagane oświadczenia i zakończ krok podawania danych do weryfikacji.

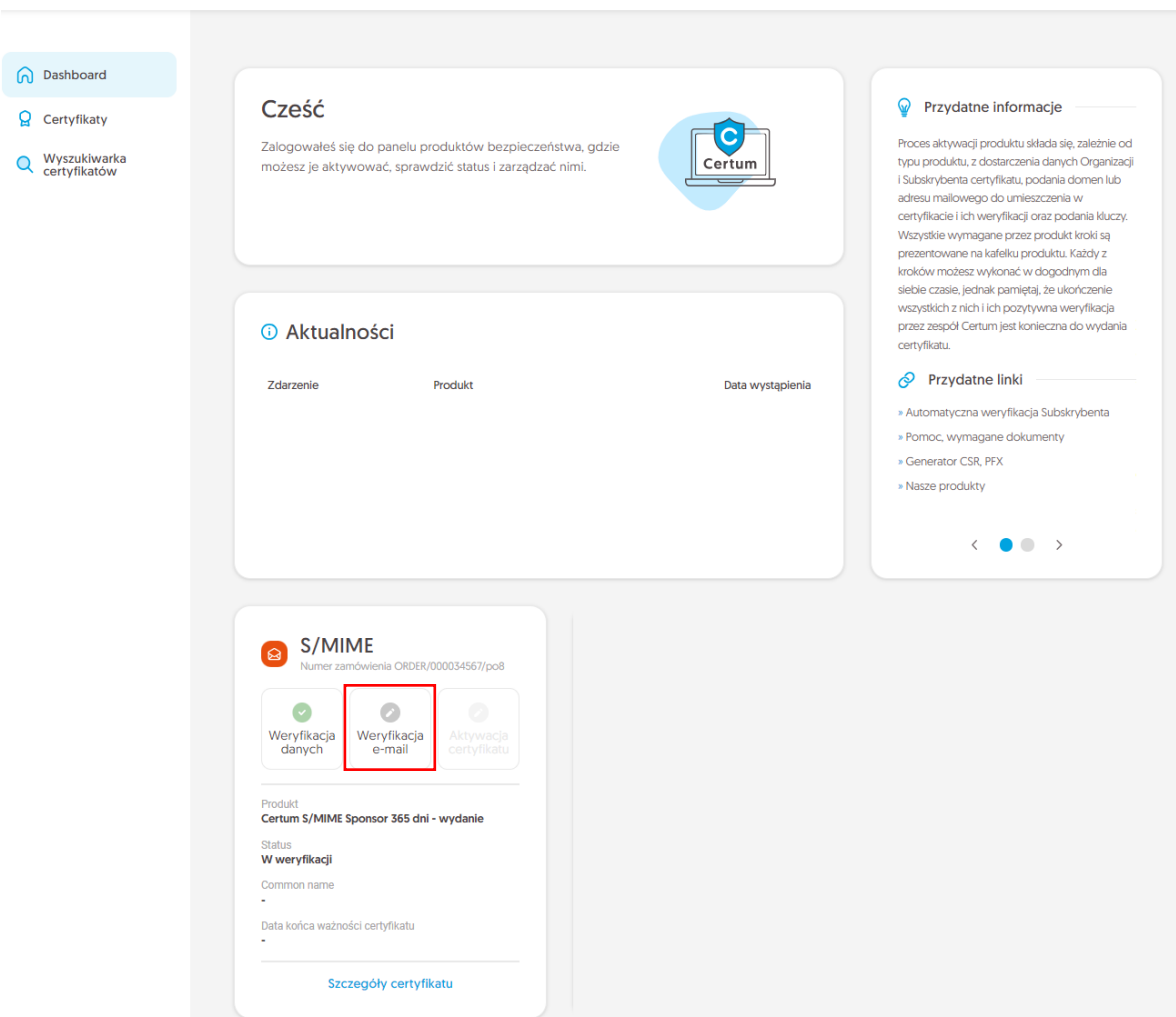
Ekran sukcesu poinformuje Cię o zapisaniu danych do weryfikacji. Certum zajmie się ich weryfikacją. W tym czasie, jeśli chcesz dodać jeszcze jakiś dokument potwierdzający wprowadzone dane, możesz go dodać w szczegółach certyfikatu. Jest to również czas na wykonanie automatycznej weryfikacji tożsamości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



Cześć

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

Aktualności

Zdarzenie	Produkt	Data wystąpienia

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

S/MIME
Numer zamówienia ORDER/000034567/poB

Weryfikacja danych Weryfikacja e-mail Aktywacja certyfikatu

Produkt
Certum S/MIME Sponsor 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 **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.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów

Wybór metody generowania kluczy

Wybierz jedną z dostępnych metod generacji pary kluczy. Metoda CSR wymaga podania CSR wygenerowanego w aplikacji Certum Tools lub samodzielnie. 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




☒ CSR ☐ Generowanie pary kluczy na karcie

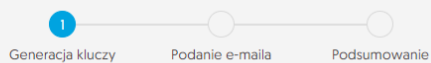
[Kontynuuj](#)

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.


-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów



Dane CSR

Wprowadź dane żądania podpisania certyfikatu (CSR) lub użyj aplikacji Certum Tools do wygenerowania nowego CSR.

```
MIImKLSHQf9Qkr2exY8DUUCLvIGN6i40JodDviGwSHV+HcbE3/r2f25dQfSe/ig
Wp5y2A6M5o6k7Moc7oFMq2m+geTR1E1FUneG1spOQaf1KDShCCfQJLIFSIswgDQ
2hQcR0dt+h//d7+TgeKMaXV72PcnYM66GkHPwg/U2iRAADxYb4rYEDSgQmIX+MS
ceB4eT3b1Rw9QRKIIEbgMGTgUVISduv2hmWJc9w28oSL1cywPDeTV/IwGcTlHWax
1CaERlpDSUTiIry1i0eQPLrdnNkypC561wHUBMrvSp4EDBYMCAwEAATAMBgkqhkiG
9w0BAQsFAAOCAQEh50uh6ZGaknkbqeTekdvsYQ+FR+cEgcav9o9oohL4sCL6vH
BJdS8bog3E6mTe4ef07cwQhtKDQNVKvUItVUgsH9Ra2NGWQM1inS7wBhYEPomP
yGSD2if2e2iBG1QI9tA9/sQvKHdLwAoR0FkR+QPye7gQ2S2+CdfH/+d7YK40F2
6G1IHTzbJN/MKbNQ07DFaRCxRu4kcvH+/teSUDQW7i2YBVKW7D17gwgq5A1LSLo
f7E1ybvHAjNB06EMFadC48Gyh5LT5yLN3ardhXvQK09g3f8Nsfopfa2Icw3/BHZA
FtDSR7yrEynjQjZMAZnp10qFvznYTAyTghzX9w==
-----END CERTIFICATE REQUEST-----
```

 Dane poprawne

 Pobierz aplikację Certum Tools

[Cofnij](#)

[Kontynuuj](#)






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.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów

Wybór metody generowania kluczy

Wybierz jedną z dostępnych metod generacji pary kluczy. Metoda CSR wymaga podania CSR wygenerowanego w aplikacji Certum Tools lub samodzielnie. 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

☐ CSR ☒ Generowanie pary kluczy na karcie

ALGORYTM KLUCZA I DŁUGOŚĆ KLUCZA

Wybierz algorytm i długość klucza ▼




Metoda CSR pozwoli uzyskać certyfikat wraz z kluczem w formie do przenoszenia i instalacji z pliku. Pamiętaj, by zapisać klucz prywatny, który wygenerowałeś wraz z CSR.

i Wygenerowanie kluczy na karcie spowoduje, że wydany certyfikat zostanie zainstalowany na karcie kryptograficznej i jej podłączenie do komputera będzie wymagane zawsze, gdy certyfikat jest używany. Wspierane są tylko karty Certum.

Kontynuuj

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](#).

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów


- 1 Generacja kluczy
- Podanie e-maila
- Podsumowanie

Generacja kluczy

W celu wygenerowania kluczy, zastosuj instrukcję dostępną poniżej.

 [Pobierz aplikację Certum SignService](#)




1. Pobierz i zainstaluj aplikację **Certum SignService**.
2. Pobierz i zainstaluj aplikację **proCertum CardManager**, jeśli jej nie posiadasz lub jest nieaktualna.
3. Podłącz czytnik do komputera i włóż kartę do czytnika.
4. Otwórz aplikację **proCertum CardManager** i sprawdź czy profil zwykły karty jest zainicjalizowany.
Jeśli profil nie jest zainicjalizowany, aplikacja poprosi Cię o nadanie kodów PIN i PUK.
5. Rozpocznij generację kluczy przyciskiem **Wygeneruj klucze**.
6. Zaakceptuj komunikat z przeglądarki o zgodę na uruchomienie aplikacji Certum SignService.
7. Gdy pojawi się okno aplikacji Certum SignService, wprowadź PIN do profilu zwykłego karty.
8. Odczekaj na wygenerowanie kluczy, może to zająć do kilku minut.

 Po zakończeniu generacji, zostaniesz przeniesiony do kolejnego okna procesu.

[Cofnij](#)

Wygeneruj klucze

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.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów

- 1 Generacja kluczy
- Podanie e-maila
- Podsumowanie

http://100.101.10.90:4300 chce otworzyć tę aplikację.

Otwórz CertumSignService

Anuluj



The image shows a Windows-style dialog box titled "Certum SignService". Inside the dialog, there is a logo consisting of a blue icon of a computer monitor with a quill pen writing on it, followed by the text "Certum SignService" in a large, bold, black font, and "by GISECO" in a smaller blue font below it. Below the logo, the title "Generacja nowej pary kluczy" is centered. There are two sections: "Dane karty" and "Dane klucza". The "Dane karty" section contains two fields: "Nazwa czytnika:" with the value "ACS ACR39U ICC Reader 0" and "Numer karty:" with the value "2268 9624 6429 8967". The "Dane klucza" section contains two fields: "Algorytm:" with the value "RSA" and "Wielkość:" with the value "2048". Below these sections, there is a label "PIN profilu zwykłego:" followed by a text input field. Below the input field, the text "[od 4 do 8 znaków]" is displayed. Further down, there are two lines of bold text: "W zależności od algorytmu i wielkości klucza generacja może potrwać do kilku minut" and "W trakcie operacji nie wyjmuj karty z czytnika". At the bottom right, there are two buttons: "Ok" and "Anuluj".

Certum SignService

 **Certum SignService**
by GISECO

Generacja nowej pary kluczy

Dane karty

Nazwa czytnika: ACS ACR39U ICC Reader 0
Numer karty: 2268 9624 6429 8967

Dane klucza

Algorytm: RSA
Wielkość: 2048

PIN profilu zwykłego:
[od 4 do 8 znaków]

**W zależności od algorytmu i wielkości klucza
generacja może potrwać do kilku minut**




W trakcie operacji nie wyjmuj karty z czytnika

Ok Anuluj

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.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów



Wprowadź e-mail

Wprowadź adres e-mail, który chcesz umieścić w certyfikacie. Adres będzie wymagał weryfikacji dostępu do niego.

ADRES E-MAIL*

Wprowadź adres e-mail

Kontynuuj

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.

Certum Produkty bezpieczeństwa

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.

S/MIME
Certum S/MIME Sponsor 365 dni - wydanie

Adres e-mail [E]:
jankowski@twojadomena.pl

Common name:
Wybierz Common name

Imię [GN]:
Jan

Nazwisko [SN]:
Kowalski

Organizacja [O]:
Twoja firma

Miejscowość [L]:
Warszawa

Województwo [SP]:
mazowieckie

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. 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.

Jeśli potrzebujesz pliku PFX, możesz skorzystać z generatora [Certum Tools](https://certum.pl/certum-tools).