

Aktywacja certyfikatu EV Code Signing na karcie kryptograficznej

Wer. 2.8

assecO

 **Certum**
by assecO

Spis treści

1. Opis produktu	3
2. Aktywacja certyfikatu	3
Krok Weryfikacja danych.....	4
Krok Generacja klucza	10
Krok Aktywacja certyfikatu	14

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.

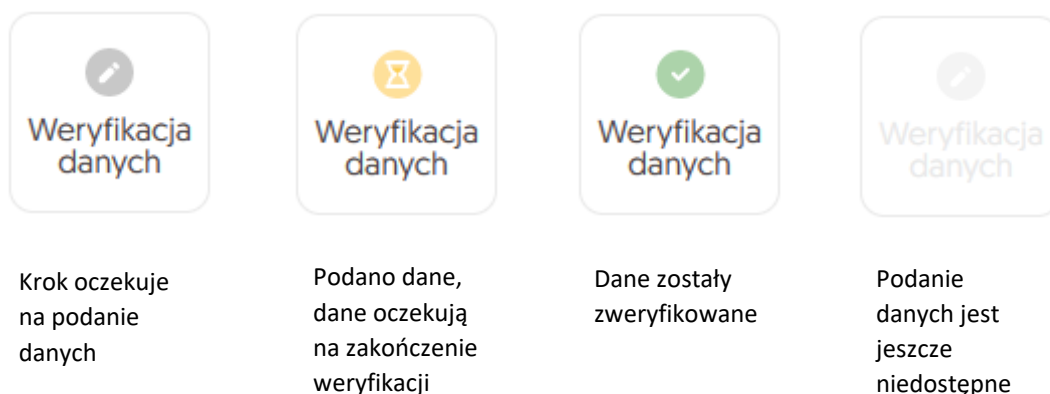
Cyfrowe podpisywanie kodu sprawia, że korzystanie z aplikacji jest bezpieczne, co przekłada się na większe zaufanie do Twojej marki i poszerzenie grona klientów.

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 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 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 has a header with the Certum logo and 'Produkty bezpieczeństwa'. Below this, there are three main sections:

- Cześć**: A welcome message stating that the user has logged into the security products panel and can activate, check status, and manage certificates.
- Aktualności**: A table with columns for 'Zdarzenie' (Event), 'Produkt' (Product), and 'Data wystąpienia' (Occurrence date).
- Nowości**: A news section titled 'Zarządzanie certyfikatami Certum SSL dla Microsoft Active Directory 24/7', discussing digitalization and security.

At the bottom, there is a 'Code Signing' section for order 'ORDER/0000123456/po14'. It contains three buttons: 'Weryfikacja danych' (highlighted with a red box), 'Generacja klucza', and 'Aktywacja certyfikatu'. Below these buttons, details for the 'EV Code Signing 365 dni - wydanie' product are shown, including the status 'Wymagana aktywacja' and fields for 'Common name' and 'Data końca ważności certyfikatu'.

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

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów

← Powrót

Certyfikat dla zamówienia ORDER/0000123456/po14

STATUS CERTYFIKATU
Wymagana aktywacja

Dane subskrybenta
Oczekuje na dane
Wypełnij dane

Dane organizacji
Oczekuje na dane

Upoważnienie subskrybenta
Oczekuje na dane

Szczegóły
Kategoria produktu
Code Signing
Produkt
EV Code Signing 365 dni - wydanie
Data złożenia zamówienia
2023-01-05 01:00
Numer seryjny certyfikatu
-
Szczegóły weryfikacji

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.

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.

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.

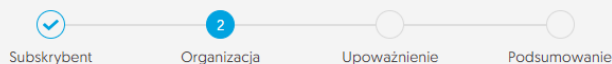
[Cofnij](#) [Kontynuuj](#)

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.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów



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

RODZAJ DZIAŁALNOŚCI*

Prywatna

NUMER REJESTROWY*

12345678

Siedziba organizacji

KRAJ*

Polska

WOJEWÓDZTWO*

mazowieckie

MIEJSCOWOŚĆ*

Warszawa

KOD POCZTOWY*

10-100

ADRES*

Jana Kochanowskiego 1

Miejsce rejestracji 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.

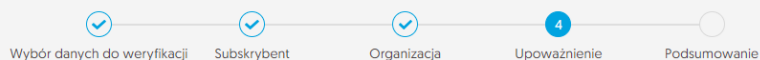
Do wyboru są dwie metody:

- **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.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów



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

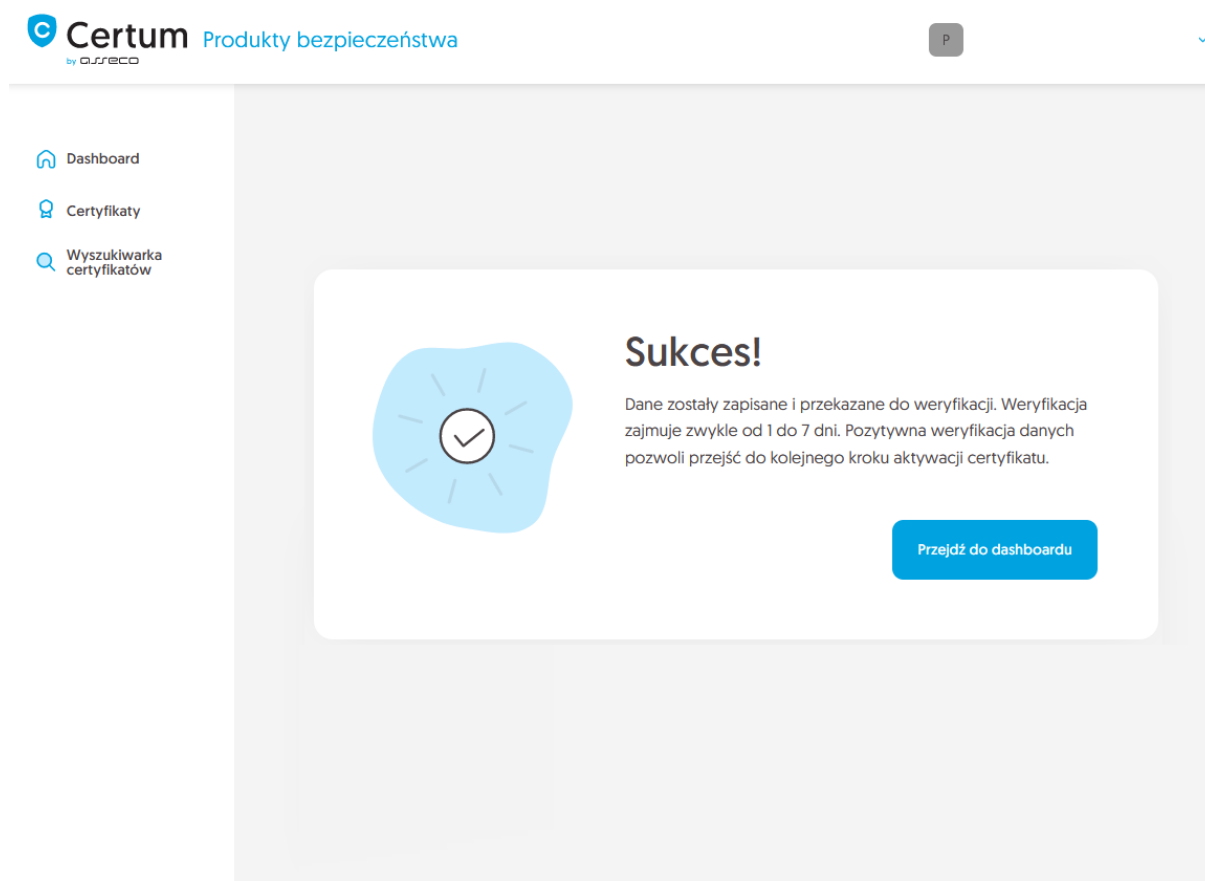
KRS
12345678

[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.


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.



Aktualności

Zdarzenie	Produkt	Data wystąpienia

Code Signing

Numer zamówienia ORDER/0000123456/po14

Weryfikacja danych

Generacja klucza

Aktywacja certyfikatu

Produkt
EV Code Signing 365 dni - wydanie

Status
W weryfikacji

Common name
-

Data końca ważności certyfikatu
-

[Szczegóły certyfikatu](#)

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




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.

-  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

- ☒ Generowanie pary kluczy na karcie

ALGORYTM KLUCZA I DŁUGOŚĆ KLUCZA




RSA 3072

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. 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 Podsumowanie

Aktywacja

W celu wygenerowania pary kluczy, pobierz i uruchom aplikację **Certum SignService**.

 [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. Oczekaj 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

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

Otwórz CertumSignService

Anuluj

1 Generacja kluczy Podsumowanie



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. 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.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów

1 —————

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
EV Code Signing 365 dni - wydanie



Common name:
Twoja firma



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. 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.