Instrukcja przygotowania wniosku o certyfikat CEPiK dla kart CryptoCard Graphite

v3.3

Certyfikat Systemu CEPiK (certyfikat TLS) na karcie kryptograficznej jest niezbędny, aby skorzystać z aplikacji dostępowych Systemu CEPiK 2.0, wykorzystujących przeglądarkę internetową lub aplikacje firm trzecich. Użytkownicy musza posiadać swoje imienne certyfikaty, które jednoznacznie ich identyfikują w systemie CEPiK 2.0.

Obecnie system CEPiK 2.0 umożliwia wnioskowanie o certyfikat przy pomocy dwóch metod:

Metoda 1 (**zalecana**) - wygenerowanie własnych kluczy na karcie kryptograficznej i przygotowanie elektronicznego wniosku o certyfikat w postaci pliku PKCS#10/CSR, przesłanie go do systemu CEPiK w celu wygenerowania certyfikatu, który zostaje po jakimś czasie odesłany zwrotnie w pliku PKCS#12/PFX i następnie zaimportowanie go na kartę, w której wygenerowano parę kluczy na starcie tej metody.

> *Ta metoda nie stawia praktycznie żadnych wymagań na środowisko komputera Użytkownika a interakcje z systemem CEKPiK ograniczają się do przesyłania pocztą elektroniczną dwóch plików (wniosku o certyfikat i zwrotnie wystawionego certyfikatu).*
>
> *UWAGA:*
> *Wnioskując tą metodą należy postępować zgodnie z zasadami opisanymi na stronie http://www.cepik.gov.pl/si-cepik-2.0/certyfikaty-skp, dotyczącymi składania wniosku o wydanie certyfikatu dla operatora dla karty kryptograficznej **w pliku** („1. PRZYGOTOWANIE WNIOSKU CERTYFIKACYJNEGO operatora (w pliku)"), czyli:*
>
> - *Wypełnić, wydrukować i wysłać podpisany wniosek papierowy do Centralnego Ośrodka Informatyki w Łodzi*
> - *Wygenerować zgodnie z poniższą instrukcją elektroniczne „zgłoszenie certyfikacyjne" CSR w formacie PKCS#10 i przesłać ja w załączniku maila na adres cc.coi@coi.gov.pl*
> - *Po akceptacji papierowego wniosku i otrzymaniu wiadomości na adres e-mail wskazany we wniosku certyfikacyjnym należy postępować zgodnie z instrukcją w wiadomości, w szczególności wykonać import certyfikatu na kartę kryptograficzną zgodnie z poniższą instrukcją*

Metoda 2 – zdalne wygenerowanie i zapisanie na karcie certyfikatu za pomocą procedury online na portalu CEPIK. W czasie tego procesu generowana jest para kluczy, system CEPIK generuje certyfikat do tych kluczy i importuje ten certyfikat na kartę użytą w tym procesie, która jest włożona do czytnika podłączonego do komputera Użytkownika.

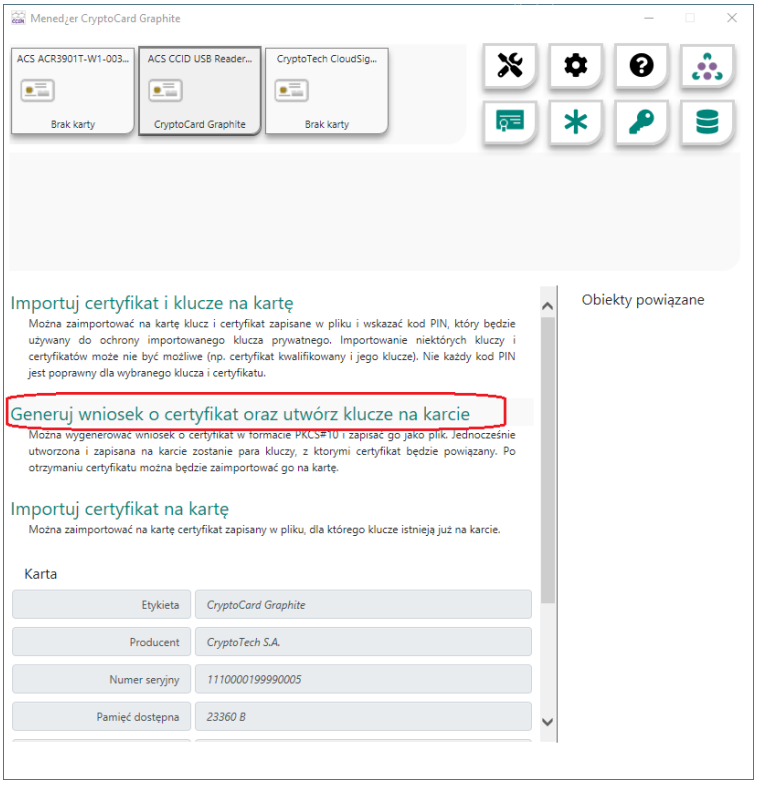
> *Nowe karty CC Graphite jeszcze nie są obsługiwane przez system CEPIK w tej metodzie, a sama metoda obsługi online karty przez przeglądarkę napotyka na kolejne problemy lub ograniczenia w aktualnych wersjach przeglądarek internetowych lub systemach operacyjnych. W wielu przypadkach albo nie jest ona łatwa do osiągnięcia albo zupełnie niemożliwa do wykorzystania przy określonej konfiguracji lokalnego komputera Użytkownika CEPiK.*

Przed rozpoczęciem generowanie wniosku należy zainstalować pakiet oprogramowania **CryptoCard Suite dla kart CryptoCard Graphite** oraz posiadać w lokalnym systemie poprawnie działający czytnik kart elektronicznych (niektóre modele czytników mogą wymagać dedykowanych sterowników ich producentów, ale najczęściej sterowniki są automatycznie zapewniane przez system Windows lub usługę Windows Update).

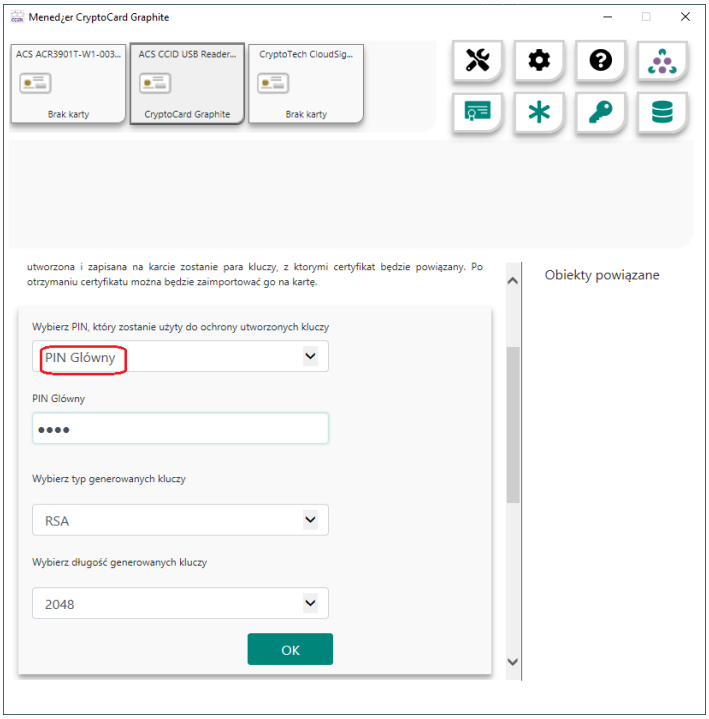
Oprogramowanie **CryptoCard Suite dla Graphite** jest dostępne na stronach internetowych pod poniższym adresem:

http://www.cryptotech.com.pl/Produkty/CryptoCard_Suite_Pobieranie,content.html

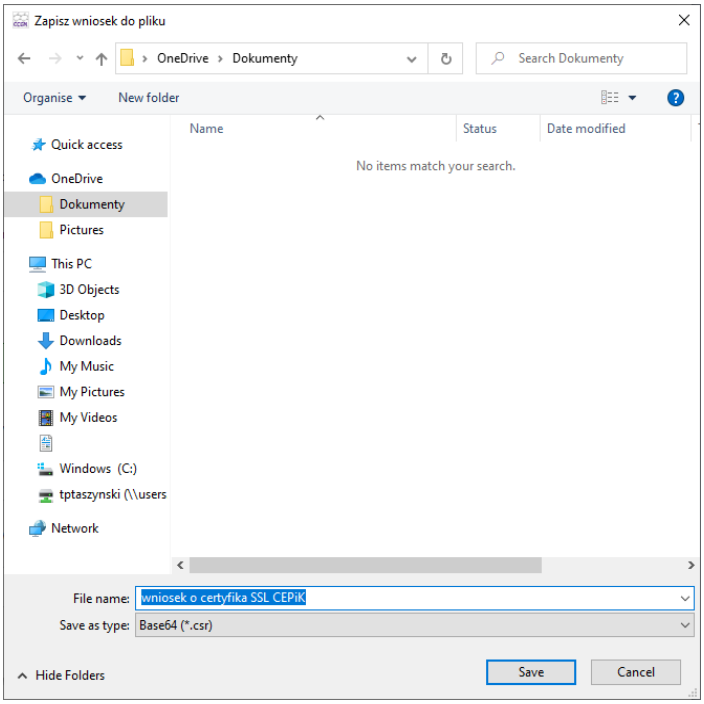
1. Po uruchomieniu i włożeniu karty do czytnika należy uruchomić funkcję „*Generuj wniosek o certyfikat oraz utwórz klucze na karcie*”:



2. Do ochrony utworzonych kluczy należy wybrać i podać „*PIN Główny*”, typ kluczy „*RSA*”, długość kluczy „*2048*” i nacisnąć przycisk OK.

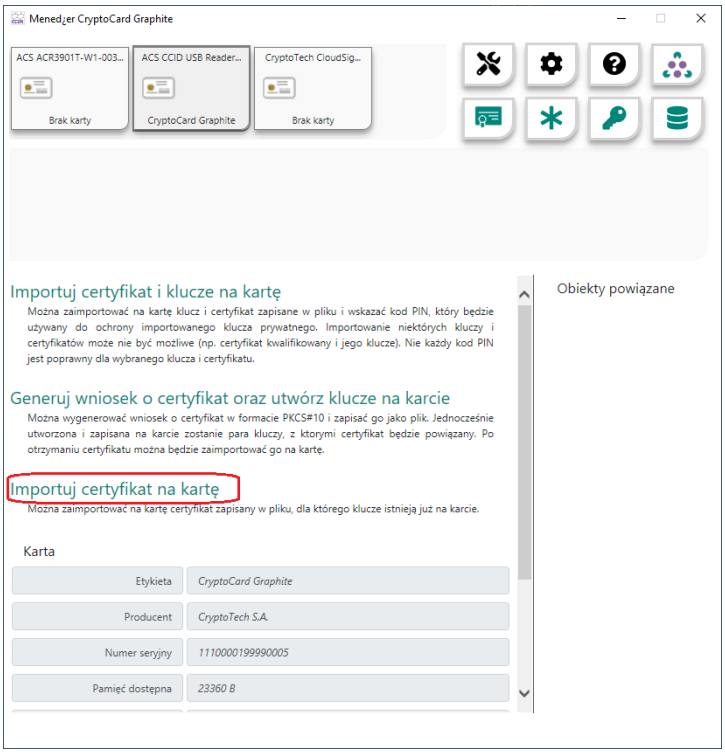


3. Na karcie zostanie wygenerowana para kluczy RSA 2048 chroniona podanym kodem PIN Główny oraz przygotowany zostanie plik wniosku CSR (PKCS#10), który zostanie zapisany na dysku, we wskazanym miejscu i pod wpisaną nazwą pliku (rozszerzenie .csr).

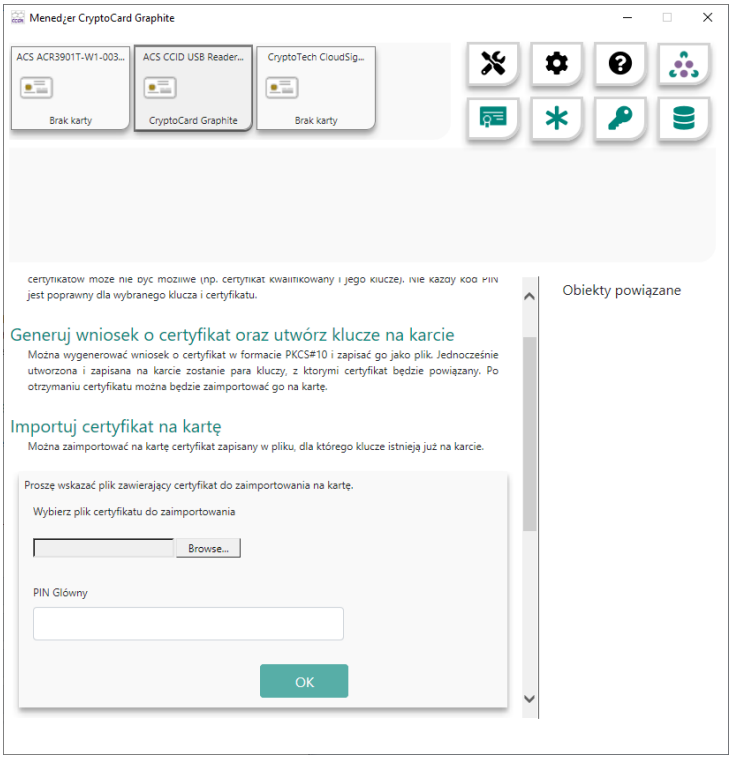


Plik ten należy przesłać do CEPiK w ramach procedury uzyskania certyfikatu CEPiK zgodnie z opisaną w CEPiK procedurą, czyli jako uzupełnienie składanego wniosku o uzyskanie certyfikatu dostępowego CEPiK.

4. Po realizacji przesłanego wniosku (procedura może trwać do 30 dni) zostanie odesłany zwrotnie plik z certyfikatem TLS, który należy zaimportować na kartę za pomocą oprogramowania CryptoCard Suite Graphite wybierając funkcję „*Importuj certyfikat na kartę*”:



5. Następnie należy wskazać plik z certyfikatem otrzymany od CEPIK i podać ten sam PIN Główny, który podawano podczas wcześniejszego generowania kluczy RSA na karcie:



6. Certyfikat SSL do systemu CEPiK zostanie zaimportowany na kartę i stosownie powiązany z istniejącym już na karcie prywatnym kluczem kryptograficznym RSA.

Od tej chwili karta nadaje się do użycia w ramach aplikacji łączących się z systemem CEPiK przez SSL/TLS (np. przeglądarka WWW lub aplikacja dedykowana dla Stacji Kontroli Pojazdów).
Aby skutecznie posługiwać się kartą w przeglądarce internetowej przy uzyskiwaniu dostępu do Systemu CEPIK, sama przeglądarka może wymagać dodatkowej konfiguracji by mogła używać certyfikatu dostępowego znajdującego się na karcie.

Najłatwiejsze w konfiguracji w tym zakresie są przeglądarki Internet Explorer, Edge oraz Chrome (jak i inne korzystające z systemowych rejestrów zaufanych certyfikatów) – w ich przypadku, typowo, nie ma potrzeby jakiejkolwiek dodatkowej konfiguracji samej przeglądarki gdyż korzysta ona z konfiguracji certyfikatów w samym systemie operacyjnym Windows.

Aktualne wersje przeglądarki Mozilla FireFox (wersje v90.x i nowsze) posiadają wsparcie do używania certyfikatów zarejestrowanych w systemie operacyjnym i związanych z nimi urządzeń kryptograficznych (np. kart elektronicznych) podobnie jak inne przeglądarki (Internet Explorer, Edge, Chrome itp.).

Te nowe wydania Firefox również nie wymagają dodatkowych kroków konfiguracyjnych ze strony użytkownika.

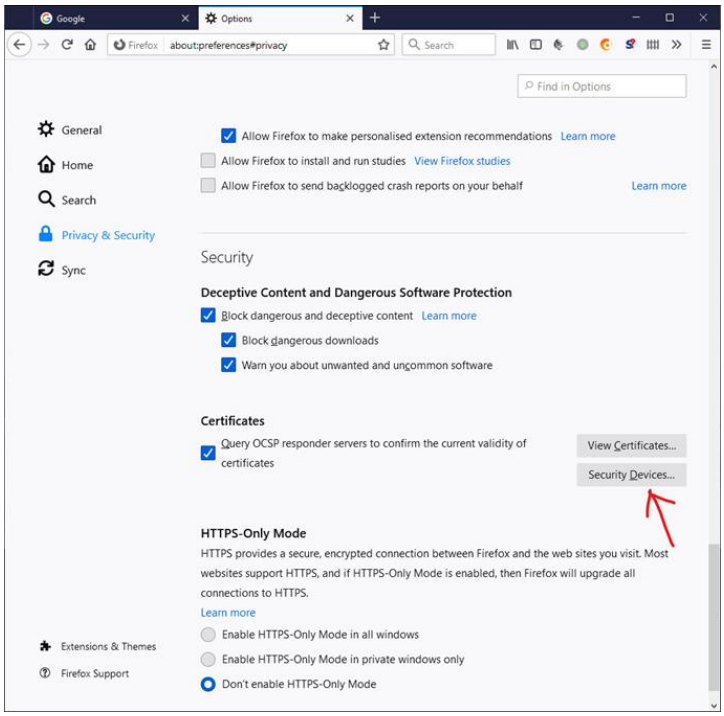
Wspierane wersje systemów Windows (od Windows 7 w górę) automatycznie importują i rejestrują w systemie operacyjnym certyfikat dostępowy CEPiK znajdujący się na karcie **CryptoCard Graphite** w momencie włożenia karty z takim certyfikatem do czytnika kart.

Inne przeglądarki mogą wymagać odpowiedniej konfiguracji samej przeglądarki by zaczęła współpracować z kartą w czytniku i pozwoliła na używanie znajdującego się na karcie certyfikatu dostępowego CEPiK.

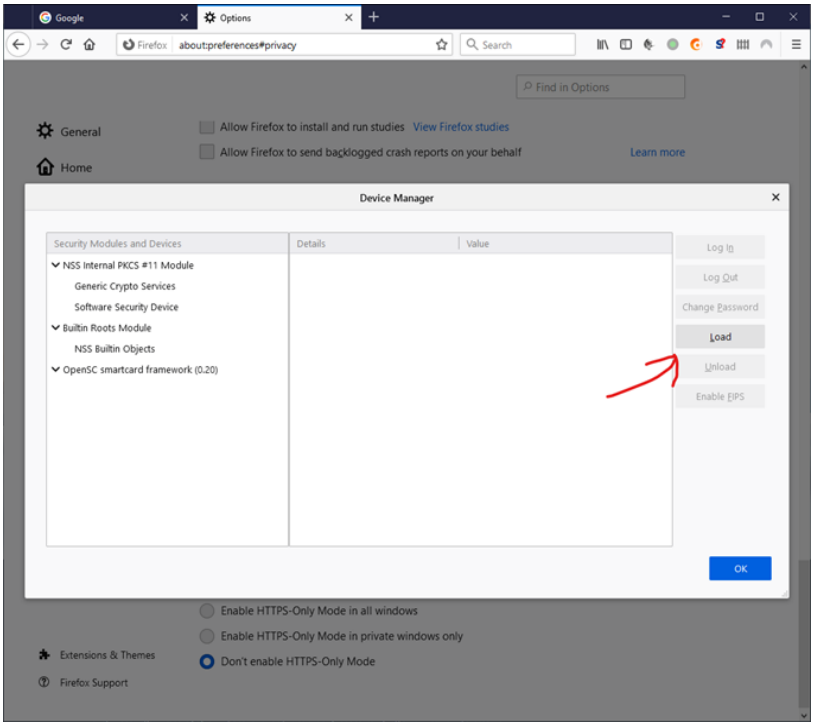
Przykładowo przeglądarka Mozilla Firefox, w wersjach starszych niż wersja v90.x, wymaga przejścia jednorazowo dodatkowych kroków konfiguracji, aby umożliwić jej korzystanie z kart kryptograficznych obsługiwanych za pośrednictwem interfejsu PKCS#11 API. Taka możliwość istnieje również dla kart **CryptoCard Graphite.**

Poniższej opisana procedura (jednorazowej) konfiguracji przeglądarki Mozilla Firefox jest niezbędna tylko dla starszych wersji przeglądarki (starszych niż v90.x)!

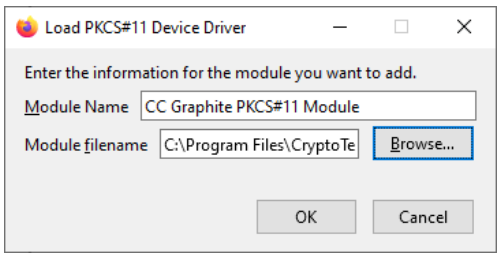
1. W przeglądarce FireFox należy skonfigurować moduł PCKS#11 by przeglądarka potrafiła korzystać z kart przez interfejs PKCS#11:



2. Wybrać przycisk „Load” w celu dodania nowego interfejsu PKCS#11 do karty kryptograficznej



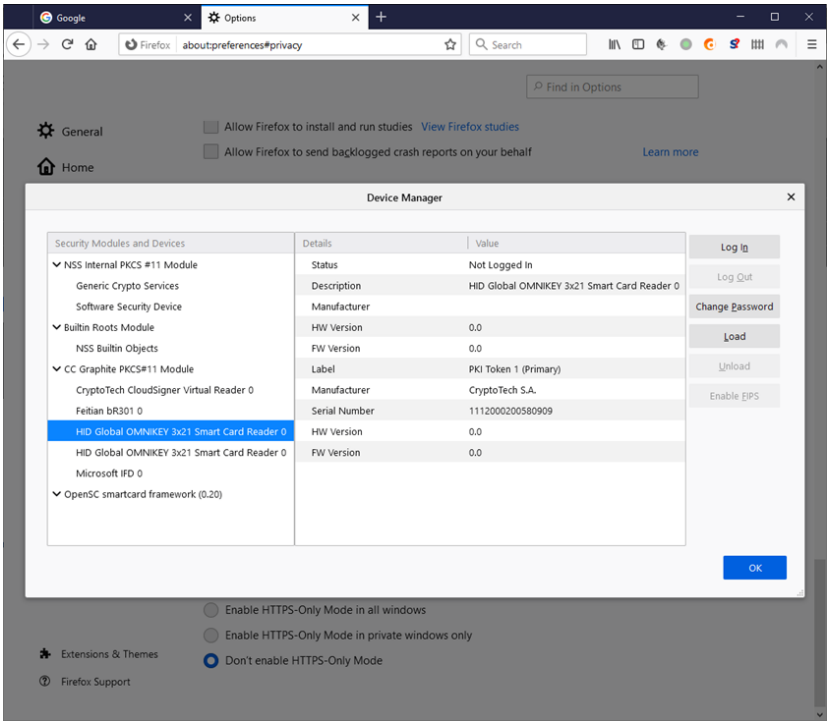
3. Zdefiniować dowolną własną nazwę dla tego modułu i wskazać lokalizację biblioteki PKCS#11 DLL odpowiedzialnej za współpracę z kartą CryptoCard Graphite



Dla kart **CryptoCard Graphite** jest to domyślnie ścieżka:

- **C:\Program Files\CryptoTech\CryptoCard\CCGraphiteP1164.dll**
  (dla aplikacji **64bit** na Windows **64bit**),
- **C:\Program Files (x86)\CryptoTech\CryptoCard\CCGraphiteP11.dll**
  (dla aplikacji **32bit** na Windows **64bit**),
- **C:\Program Files\CryptoTech\CryptoCard\CCGraphiteP11.dll**
  (dla aplikacji **32bit** na Windows **32bit**),

4. Moduł PCKS#11 (biblioteka DLL) obsługująca karty **CryptoCard Graphite** zostanie zarejestrowana w FireFox



Na powyższym zrzucie okienka widać moduł PKCS#11 dla karty CryptoCard Graphite, który listuje wszystkie widoczne dla niego w danym systemie czytniki kart i ewentualnie pokazuje czy rozpoznaje kartę w danym czytniku.

Przeglądarki zwykle poproszą o podanie kodu PIN w chwili, gdy będą chciały użyć certyfikat i/lub klucz prywatny znajdujący się na karcie. Można też użyć przycisku „Log in" widocznego na powyższym oknie przeglądarki Firfox w celu „zalogowania się do karty", co wymaga podania stosownego kodu PIN i umożliwia również używanie przez przeglądarkę certyfikatów i kluczy znajdujących się na karcie **CryptoCard Graphite**.

Sposób konfiguracji odrębnych/dedykowanych aplikacji dostępowych do systemu CEPiK może być odmienny i jest określonych przez ich producentów.

Jeśli aplikacja firmy trzeciej używa interfejsu PCKS#11 API do współpracy z kartami kryptograficznymi to najczęściej wymaga wskazania gdzieś w jej konfiguracji ścieżki dostępu do biblioteki PKCS#11 DLL na dysku komputera.