



Instrukcja przygotowania wniosku o certyfikat CEPIK dla kart CryptoCard Graphite

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 muszą 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 - 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 zwrótnie 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 CEPIK ograniczają się do przesyłania pocztą elektroniczną dwóch plików (wniosku o certyfikat i zwrótnie wystawionego certyfikatu).

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.

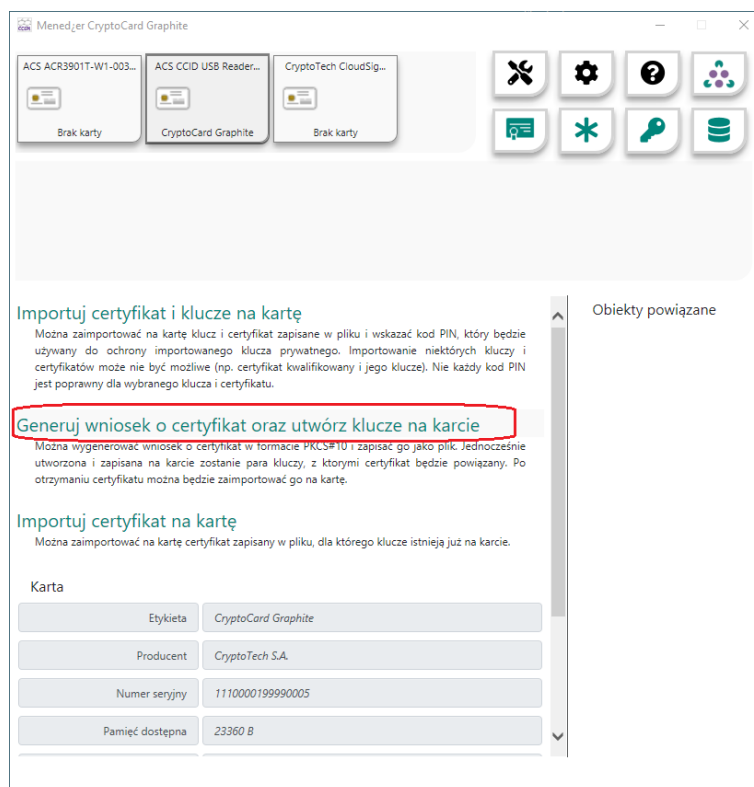
Nowe karty CC Graphite obecnie nie są obsługiwane przez system CEPIK w tej metodzie, a sama metoda obsługi online karty przez przeglądarkę napotyka na kolejne problemy lub ograniczenia w aktualnych wersjach przeglądarek internetowych lub systemach operacyjnych. W wielu przypadkach albo nie jest ona łatwa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

Przed rozpoczęciem generowania 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).

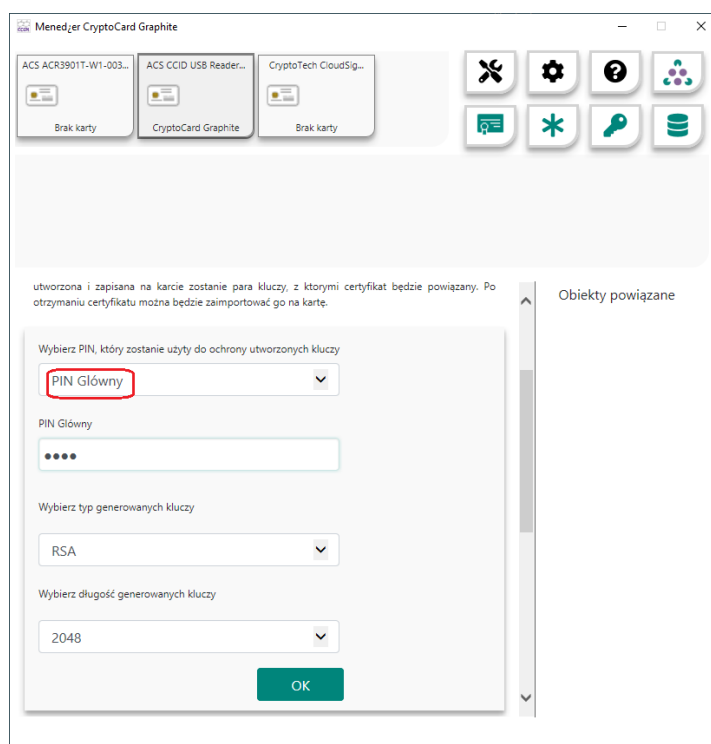
Oprogramowanie **CryptoCard Suite dla Graphite** jest dostępne na stronach internetowych pod poniższym adresem:

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

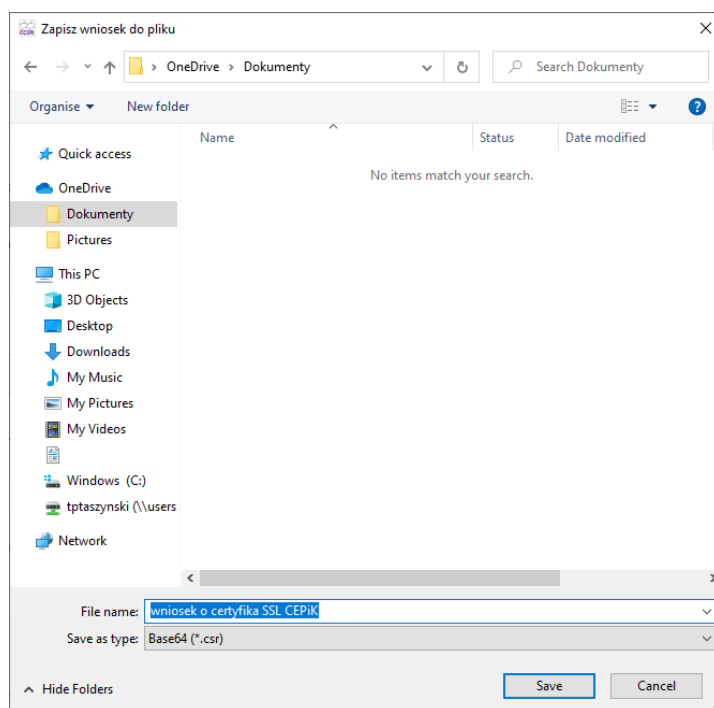
1. Po uruchomieniu i włożeniu karty do czytnika należy uruchomić funkcję „Generuj wniosek o certyfikat oraz utwórz klucze na karcie”:



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

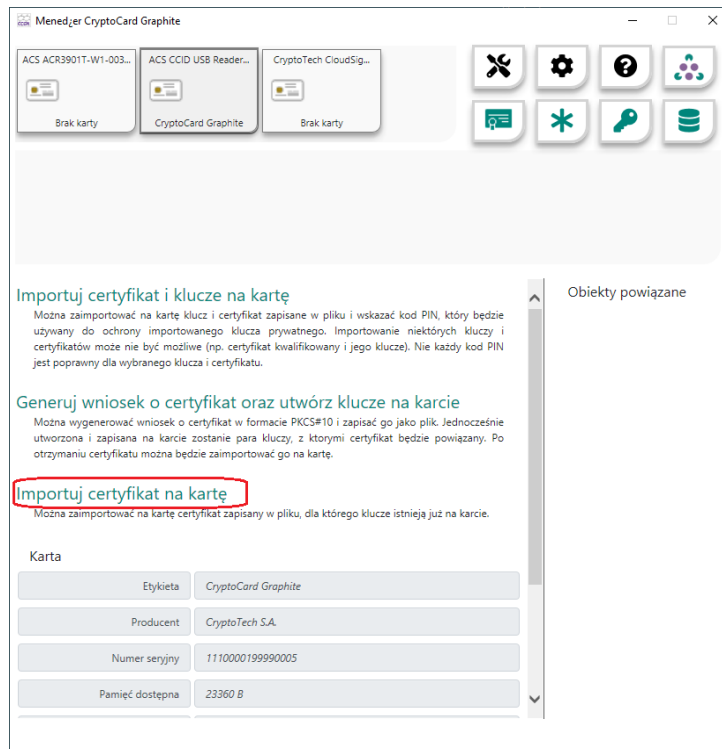


3. Na karcie zostanie wygenerowana para kluczy RSA 2048 chroniona podanym kodem PIN Główny oraz przygotowany zostanie plik wniosku CSR (PKCS#10), który zostanie zapisany na dysku, we wskazanym miejscu i pod wpisaną nazwą pliku (rozszerzenie .csr).

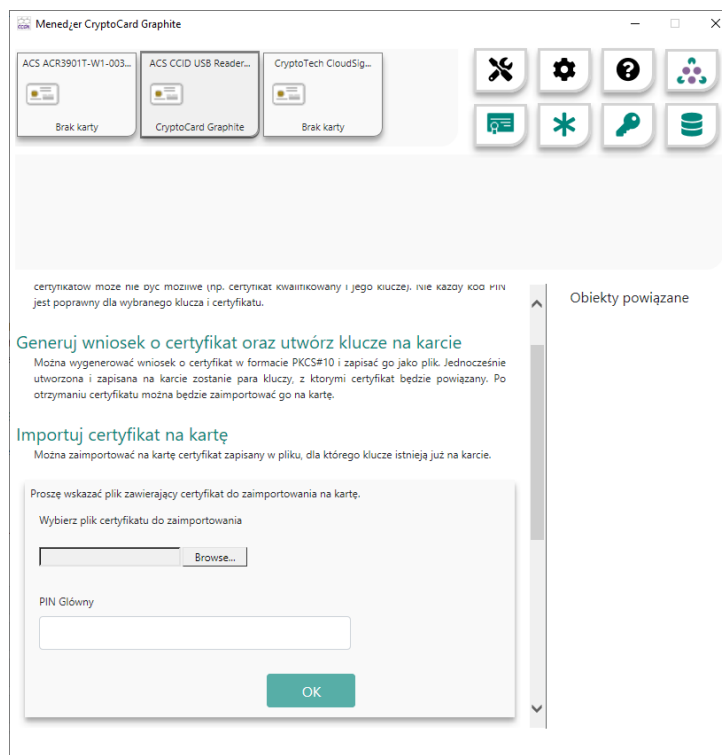


Plik ten należy przesłać do CEPiK w ramach procedury uzyskania certyfikatu CEPiK zgodnie z opisaną w CEPiK procedurą, czyli jako uzupełnienie składanego wniosku o uzyskanie certyfikatu dostępowego CEPiK.

4. Po realizacji przesłanego wniosku (procedura może trwać do 30 dni) zostanie odesłany zwrótnie 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 kluczem RSA.

Od tej chwili karta nadaje się do użycia w ramach aplikacji łączących się z systemem CEPIK przez SSL/TLS (np. przeglądarka WWW).

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.

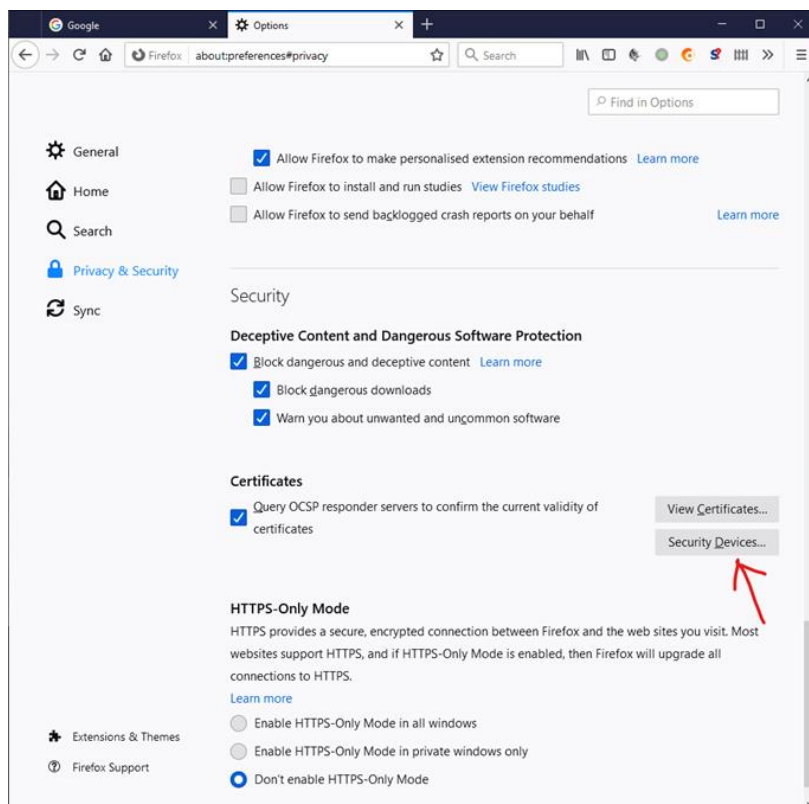
Najłatwiejsze w konfiguracji w tym zakresie są przeglądarki Internet Explorer, Edge oraz Chrome (jak i inne korzystające z systemowych rejestrów zaufanych certyfikatów) – w ich przypadku, typowo, nie ma potrzeby jakiegokolwiek dodatkowej konfiguracji samej przeglądarki gdyż korzysta ona z konfiguracji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

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.

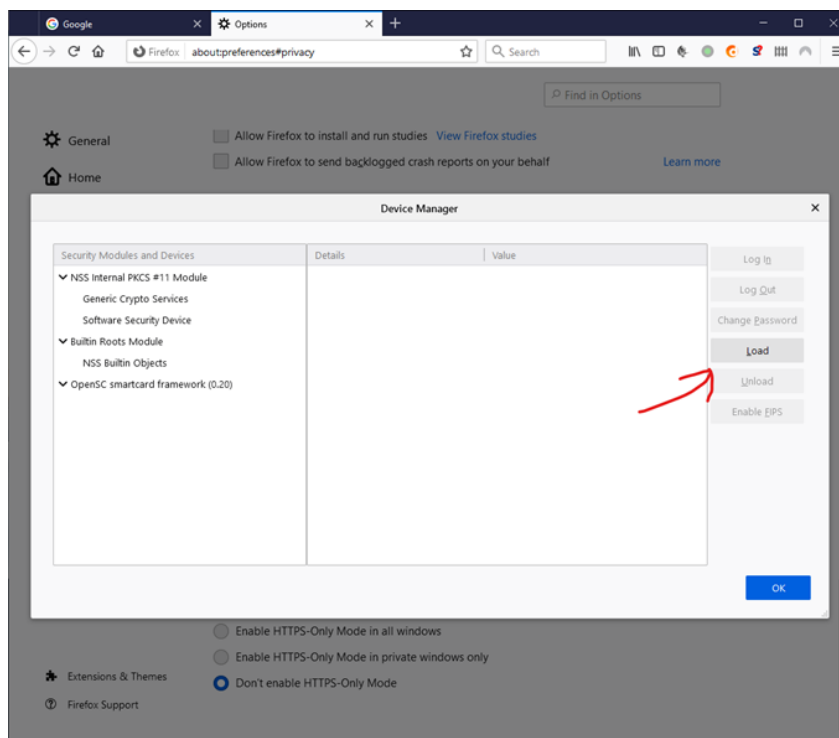
Inne przeglądarki mogą wymagać odpowiedniej konfiguracji samej przeglądarki by zaczęła współpracować z kartą w czytniku i pozwoliła na używanie znajdującego się na karcie certyfikatu dostępowego CEPIK.

Przykładowo przeglądarka Mozilla Firefox wymaga przejścia jednorazowo takich kroków konfiguracji, aby umożliwić jej korzystanie z kart **CryptoCard Graphite**:

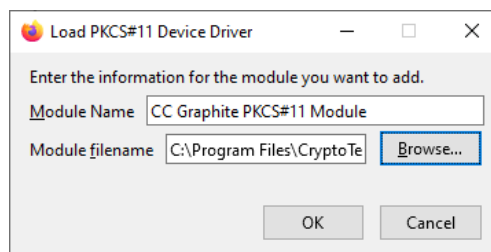
1. W przeglądarce FireFox należy skonfigurować moduł PKCS#11 by przeglądarka potrafiła korzystać z kart przez interfejs PKCS#11:



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



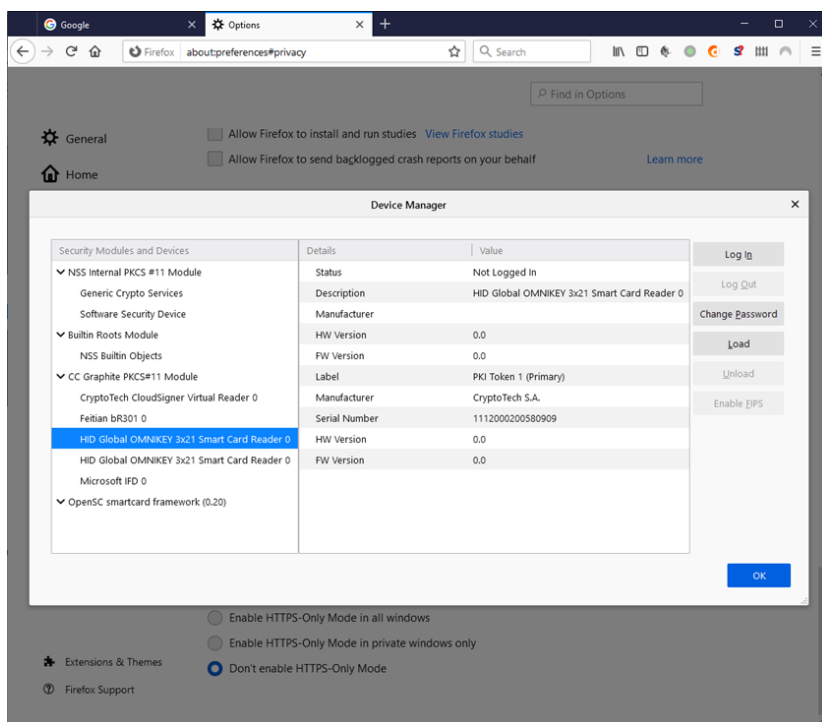
- Zdefiniować dowolną własną nazwę dla tego modułu i wskazać lokalizację biblioteki PKCS#11 DLL odpowiedzialnej za współpracę z kartą CryptoCard Graphite



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 PKCS#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 certyfikatu znajdującego się na karcie. Można też użyć przycisku „Log in” widocznego na powyższym oknie przeglądarki Firefox w celu „zalogowania się do karty”, co wymaga podania stosownego kodu PIN i umożliwi 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 PKCS#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.