CEPiK Uploader
Instrukcja obsługi

1 Wstęp

Program CEPiK Uploader składa się z pliku wykonywalnego CepikUploader.exe i modułu komunikacyjnego CepikUploaderCfg.dll, a także z poniżej opisanych bibliotek i programów pomocniczych.

Biblioteka CepikUploaderCfg.dll jest modułem komunikacyjnym pośredniczącym między programem Patronat a serwerem CEPiK 2.0. Aby program Patronat mógł go wczytać, zmienna środowiskowa PATH musi zawierać prowadzącą do niego ścieżkę dostępu C:\CEPIK2\openssl\bin
Instalator programu CEPiK Uploader tworzy tą ścieżkę dostępu podczas instalacji.

Program CepikUploader.exe służy do testowania połączenia z serwerem CEPIK 2.0 i aktualizacji słowników używanych przez program Patronat.
Obecnie słowniki można aktualizować także za pomocą programu Patronat.

Do korzystania z programu CEPiK Uploader niezbędne jest zestawienie połączenia VPN.
Po uruchomieniu program będzie co 29 minut wysyłał za pomocą systemowego polecenia PING.exe jeden pakiet ICMP do serwera CEPiK 2.0 w celu podtrzymania połączenia VPN.
Zatem program PING.exe powinien znajdować się w ścieżce dostępu.

Komunikacja między programem CEPiK Uploader a serwerem CEPiK 2.0 odbywa się za pośrednictwem formularzy SOAP będących formularzami XML opakowanymi w kopertę SOAP umożliwiającą dokonanie podpisu cyfrowego. Do realizacji komunikacji sieciowej używane są biblioteki programistyczne cURL i OpenSSL wraz z silnikiem kryptograficznym pkcs11.dll, umożliwiającym korzystanie z karty kryptograficznej PKCS#11.

Podpisy cyfrowe formularzy SOAP z wykorzystaniem w. w. karty lub pliku keystore .p12 są dokonywane za pomocą programu SignSoap.exe, wykorzystującego maszynę wirtualną JRE (Java Runtime Engine) w wersji 32-bitowej nie starszej niż wersja 8 Update 151 (id. wersji 1.8.0_151).

Jeżeli odpowiednia wersja Javy nie jest zainstalowana, program otworzy stronę internetową
z której można pobrać wersję 8 Update 151 32-bitowego środowiska uruchomieniowego Java SE JRE
Jest ona także dostępna pod adresem http://sd.coi.gov.pl/Java
http://sd.coi.gov.pl/Java/Instalator-Java-jre-8u151.exe
Strona ta jest dostępna dla użytkownika cepik po wprowadzeniu hasła cepik .

Tą wersję środowiska uruchomieniowego Java SE JRE można także pobrać używając programu Downloader, wybierając powyższy plik z listy rozwijanej z pola edycyjnego URL i klikając Pobierz.
Ikona programu Downloader w kształcie chmury z zieloną strzałką skierowaną w dół po zainstalowaniu programu CEPiK Uploader znajdzie się na pulpicie.

Program CEPiK Uploader działa pod kontrolą systemów operacyjnych Microsoft Windows w wersjach: XP, Vista, 7, 8, 8.1, 10.
Zalecana jest aktualizacja systemu Windows XP do nowszej wersji.

UWAGI:

Przed wprowadzeniem PINu upewnij się, że włożyłeś kartę PKCS#11 i zestawiłeś połączenie VPN.

Po włożeniu karty zaczekaj co najmniej 3 sekundy przed jej użyciem, aby system miał czas ją rozpoznać. Zbyt krótki odstęp czasu pomiędzy włożeniem karty i próbą jej użycia może być przyczyną błędnego działania lub zawieszania się programu SignSoap.exe lub modułu komunikacyjnego.
Naprawa tego błędu może wymagać zresetowania komputera.

Na karcie kryptograficznej powinien być zapisany dokładnie jeden certyfikat i jeden klucz prywatny (nie licząc certyfikatu CA). Jeżeli program zarządzający kartą nie kasuje starego, nieważnego certyfikatu przed zapisaniem nowego, należy to zrobić samodzielnie.

Zalecane jest, aby certyfikat stacji i jej klucze publiczny i prywatny miały ten sam ID i etykietę będącą symbolem stacji, a certyfikat Centrum Autoryzacyjnego (np. „Certyfikat CCK") nie miał ustawionego ID. Dzięki temu zostanie on pominięty przy wyborze certyfikatu stacji przez silnik kryptograficzny.
ID certyfikatu można zmienić za pomocą programu Encard - Zarządca kart (menu główne Obiekt, opcja Ustaw/Zmień Identyfikator, Typ identyfikatora „Z rozszerzenia SubjectPublicKeyIdentifier certyfikatu" lub „Dowolny ciąg bajtów (HEX)" przy czym do pola Wartość należy wkleić ID klucza prywatnego (ciąg wartości heksadecymalnych oddzielonych spacjami).
Identyfikator certyfikatu Centrum Autoryzacyjnego (np. „Certyfikat CCK") można usunąć w podobny sposób, wybierając w opcji Ustaw/Zmień Identyfikator -Typ identyfikatora „Brak identyfikatora (nie zalecane !!!)".
Wskazane jest także usunąć z karty nieważne lub nieużywane certyfikaty stacji (tzn. te których ważność wkrótce mija i dlatego zostały zastąpione nowymi).
Wykonanie powyższych czynności ułatwi silnikowi kryptograficznemu pkcs11.dll znalezienie certyfikatu i odpowiadającego mu klucza prywatnego bez potrzeby dodatkowej konfiguracji opisanej w rozdziale 7.
Wyłącz oszczędzanie energii przez czytnik karty, tak jak to opisano w rozdziale 4.

Brak aktualizacji słowników przez tydzień powoduje konieczność ich odnowy, co może trwać od 15 minut do kilku godzin, w zależności od prędkości komputera i jego pamięci masowej (dysku twardego lub SSD). Dlatego też tą operację nalepiej jest przeprowadzić poza godzinami pracy SKP.

Jeżeli przy próbie zalogowania się do CEPiK Uploadera lub wysłania badania otwiera się okno przeglądarki, ściągnij i uruchom plik Instalator-Java-jre-8u151.exe

Przyczyną problemów z generacją podpisu elektronicznego za pomocą programu SignSoap może być:

- zablokowany PIN karty lub nieważny certyfikat - proszę sprawdzić stan karty za pomocą jej programu administracyjnego i ją odblokować używając kodu PUK lub uaktualnić jej certyfikat;

- nieprawidłowa wersja Javy - proszę odinstalować wszystkie wersje poza najnowszą wersją 8 32-bitową;

- program antywirusowy lub wirus zakłócający działanie programu lub komunikację z czytnikiem USB;

- obecność innych urządzeń kryptograficznych niż czytnik karty używanej do łączenia się z CEPiK 2.0 (tzn. innych czytników kart, e-tokenów etc.). Proszę je usunąć i odinstalować ich sterowniki.;

- wybrana została nieodpowiednia dla danej karty biblioteka DLL PKCS#11 (CRYPTOKI).
  Prawidłowe nazwy plików biblioteki DLL modułu PKCS#11 (CRYPTOKI) to:
  enigmap11.dll dla kart Encard Enigma;
  crypto3PKCS.dll dla kart Asseco Certum (profil zwykły);
  cmP11.dll dla kart EuroCert;
  CCPkiP11.dll dla kart CryptoTech Cryptocard.

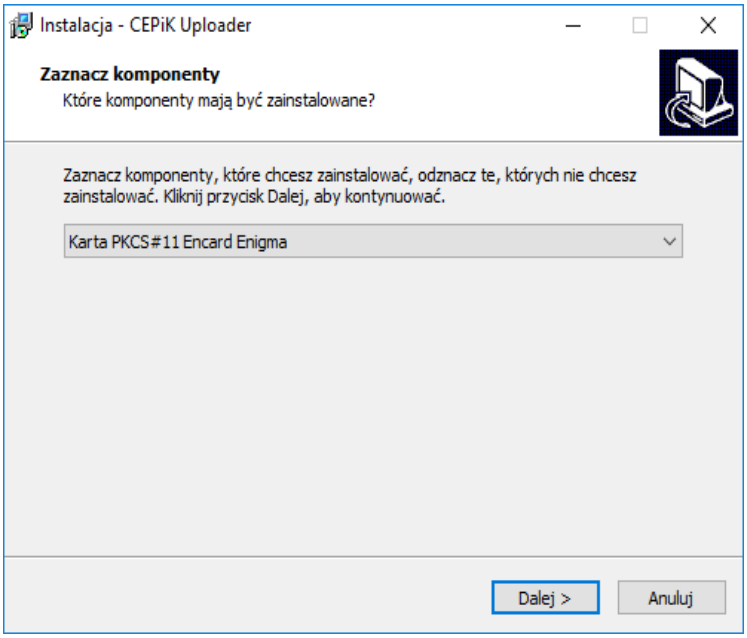
Problem nieprzyjmowania poprawnego PINu oznacza że program wymaga dodatkowej konfiguracji opisanej w rozdziale 7, w szczególności odczytania identyfikatorów certyfikatu i klucza prywatnego z karty (przez kliknięcie na przycisk […] na prawo od ID certyfikatu lub klucza prywatnego) i skopiowania ich do odpowiednich pól edycyjnych okna „Ustawienia połączenia", widocznych po kliknięciu przycisku ekranowego „Ustawienia zaawansowane".

W przypadku wystąpienia błędu „Error: Authorization failure. Rejected by policy" proszę za pomocą przeglądarki Firefox dotychczas używanej do wysyłania danych do CEPiK 1 (ze skonfigurowaną kartą kryptograficzną) wejść na stronę:
https://hello.skp.cepik
Jeżeli przeglądarka wyświetli błąd 403 „Brak uprawnień do usługi"

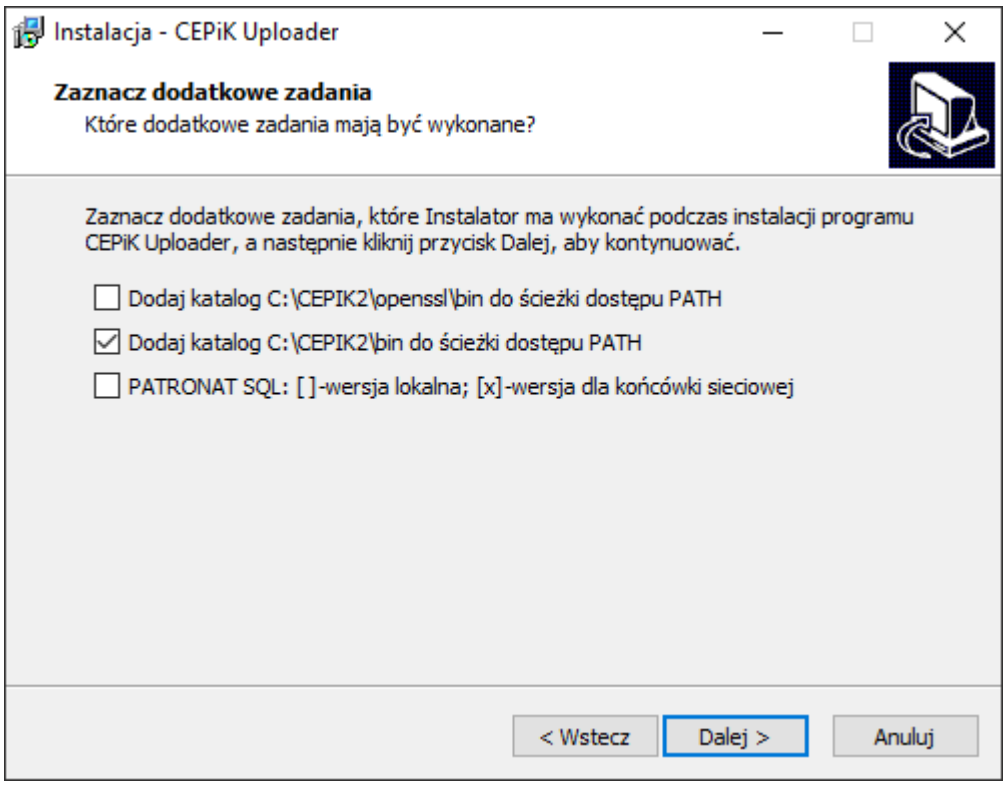
problem jest po stronie serwera COI i jest niezależny od działania programów CEPiK Uploader i Patronat.

2 Instalacja programu CEPiK Uploader

Program instalacyjny o nazwie pliku „setup_CEPIK2.exe” znajduje się w katalogu:
C:\DIAGOGOL\INSTALUJ
Po jego uruchomieniu ukaże się okno Kontroli Konta Użytkownika z pytaniem, czy zezwolić tej aplikacji na wprowadzenie zmian na tym urządzeniu. Odpowiedz „tak”.
Pojawi się następujące okno programu instalacyjnego:



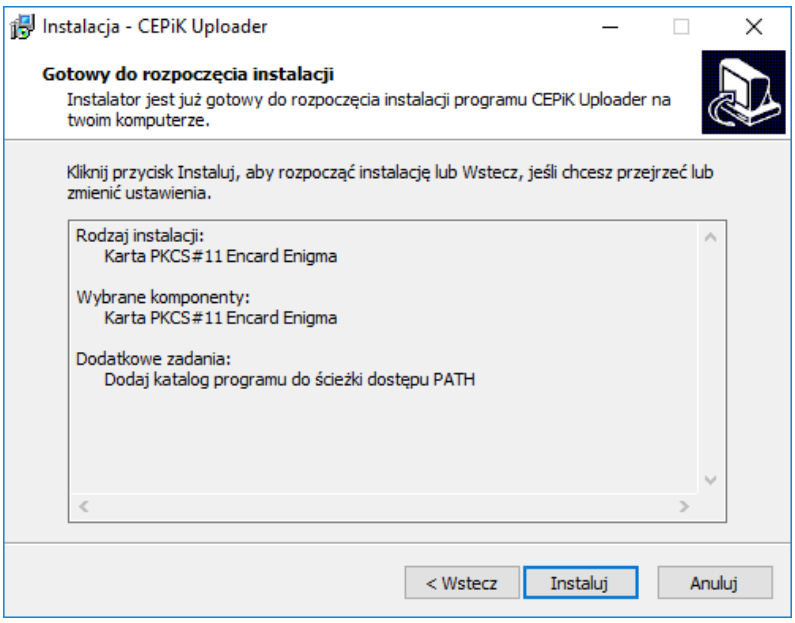
Okno to umożliwia wybranie używanego czytnika i karty.
Program obsługuje następujące czytniki kart kryptograficznych PKCS#11:
Encard Enigma, CryptoTech CryptoCard, Asseco Certum (profil zwykły), EuroCert.
Po wybraniu posiadanego czytnika kliknij przycisk ekranowy „Dalej”.



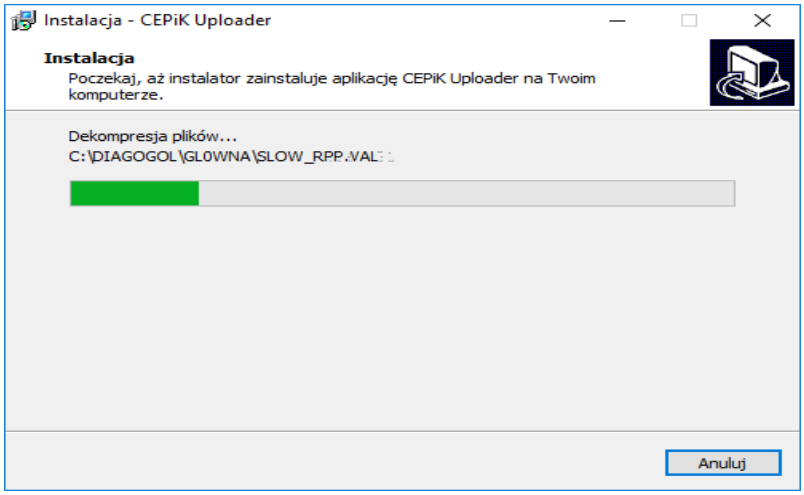
Na następnej stronie znajdują się pola wyboru:
„Dodaj katalog C:\CEPIK2\openssl\bin do ścieżki dostępu PATH”,
„Dodaj katalog C:\CEPIK2\bin do ścieżki dostępu PATH”
Będą one zaznaczone przy pierwszej instalacji, nie zaznaczone przy reinstalacji.

Poniżej znajduje się pole wyboru wersji programu Patronat SQL.
Wersja lokalna udostępnia swój katalog roboczy (zwykle C:\DIAGOGOL) końcówkom sieciowym, na których jest on zmapowany (zwykle jako F:\ ). Na końcówkach sieciowych w ich katalogu roboczym znajduje się plik dirsieci.dat, zawierający tekst odpowiadający temu mapowaniu (zwykle F:\ ).

Nie zmieniając tych ustawień kliknij „Dalej”.



Na tej stronie możesz przeczytać podsumowanie dokonanych wyborów i kliknąć „Instaluj”.



Rozpocznie się instalacja programu na dysk do katalogu C:\CEPIK2 .

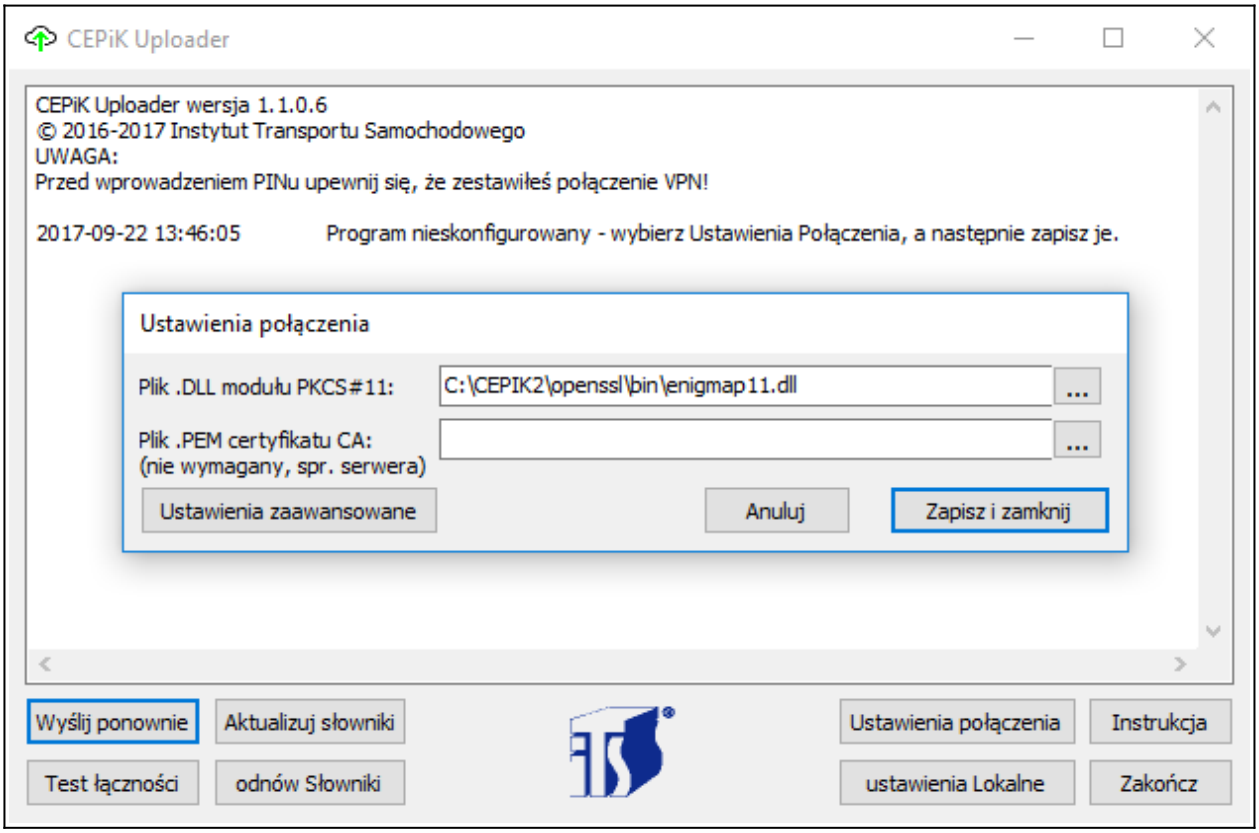
Aktualizację tabel bazodanowych marek, modeli, typów etc. należy wykonywać na instalacji lokalnej i na instalacjach sieciowej programu Patronat.
Obecnie słowniki można aktualizować także za pomocą programu Patronat.

Po zakończeniu kopiowania pokaże się okienko z informacją o zakończeniu instalacji.

Po zakończeniu instalacji program należy uruchomić klikając na jego ikonę na pulpicie (w kształcie chmury) lub wybierając CEPiK Uploader SQL z menu Start.

3 Pierwsze uruchomienie programu CEPiK Uploader

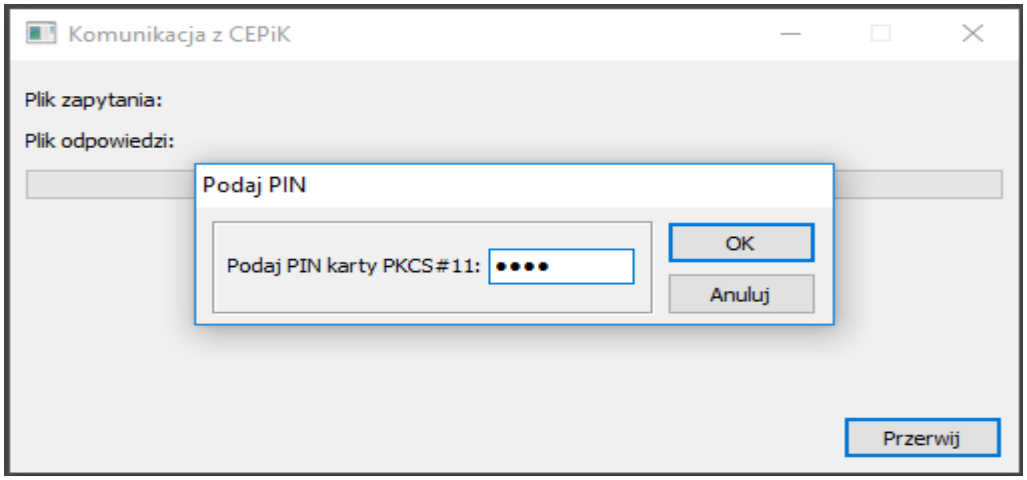
Po pierwszym uruchomieniu program zgłosi że wymaga wstępnej konfiguracji.



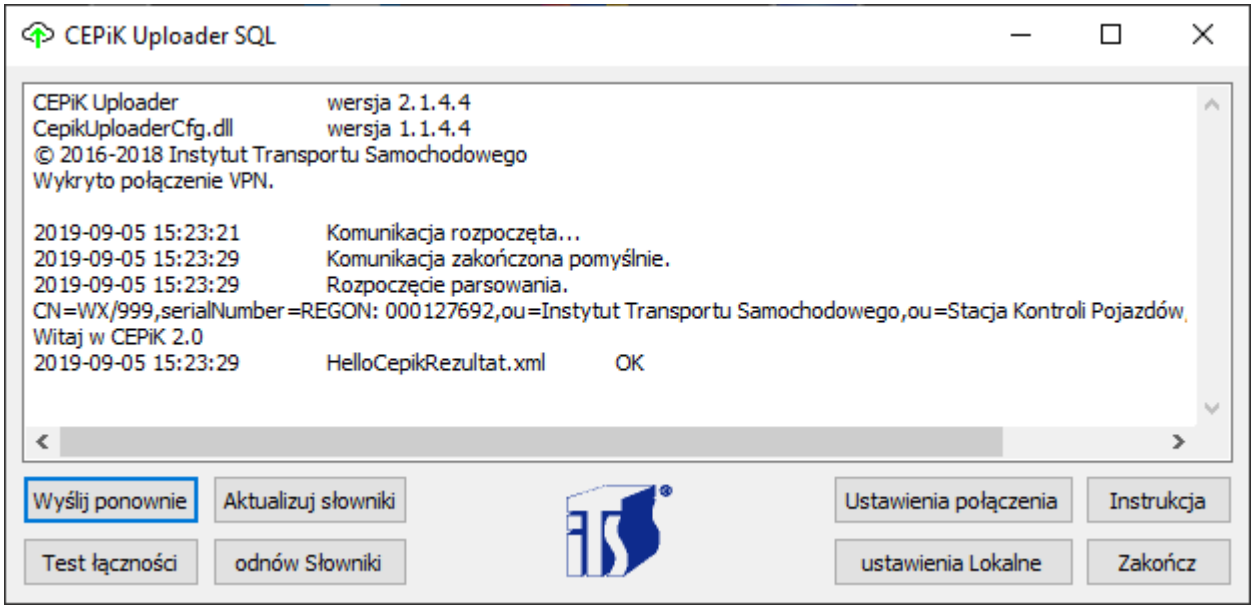
Prawidłowe nazwy plików biblioteki DLL modułu PKCS#11 (CRYPTOKI) to:

enigmap11.dll dla kart Encard Enigma;
crypto3PKCS.dll dla kart Asseco Certum (profil zwykły);
cmP11.dll dla kart EuroCert;
CCPkiP11.dll dla kart CryptoTech Cryptocard.

W większości przypadków (gdy typ karty został poprawnie wybrany w instalatorze programu) wystarczy kliknąć przycisk ekranowy „Zapisz i zamknij”.
Utworzony zostanie plik konfiguracyjny o nazwie „UploaderConfig.xml” znajdujący się na koncie użytkownika w ukrytym podkatalogu AppData\Roaming\CEPIKuploader

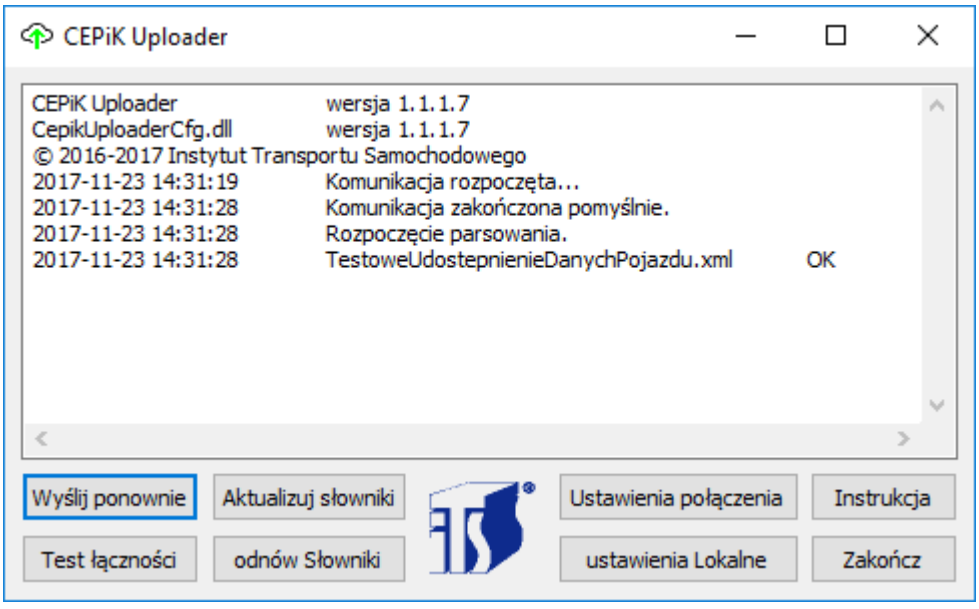


Następnie program otworzy okno komunikacyjne, w którym wyświetli okno dialogowe służące do wprowadzenia numeru PIN karty kryptograficznej. Przed wprowadzeniem PINu należy upewnić się, że karta jest włożona do czytnika, czytnik jest prawidłowo zainstalowany i VPN jest połączony.



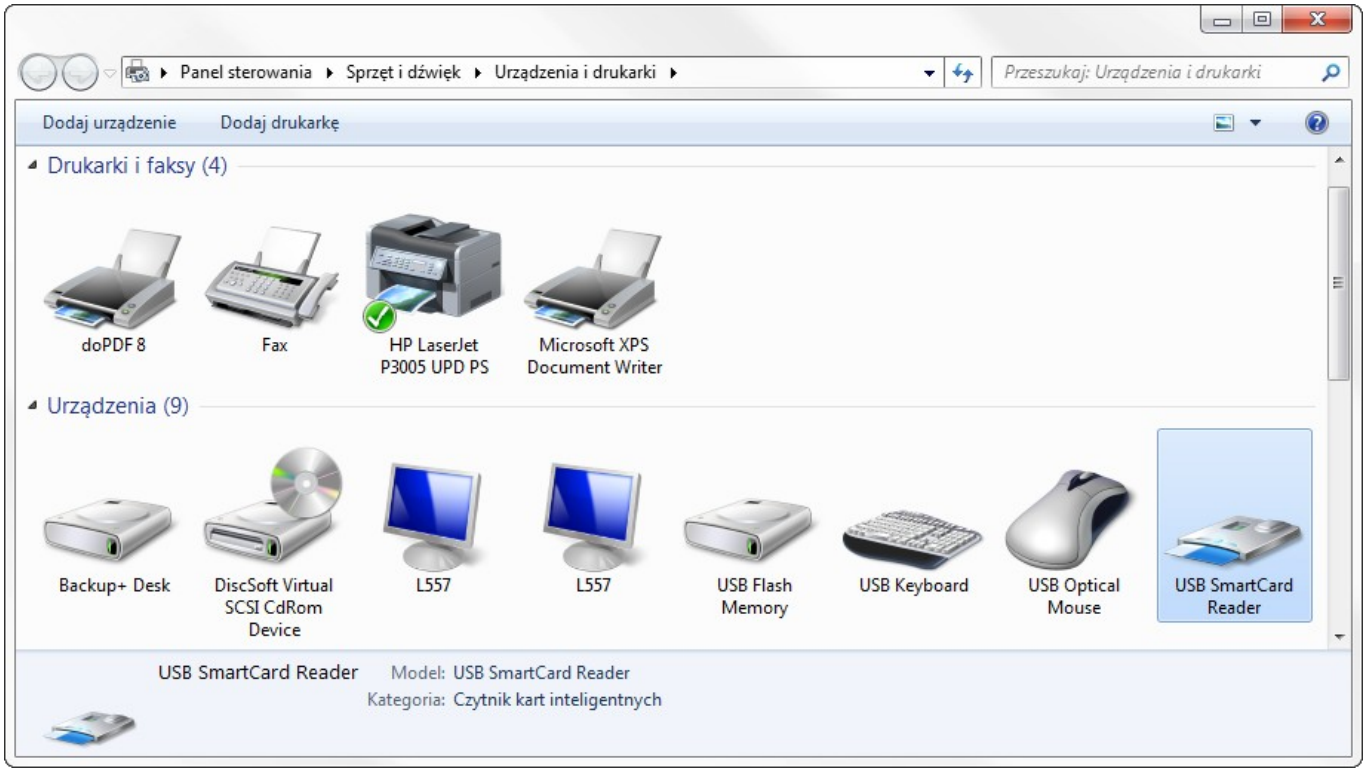
Wygląd głównego okna programu po dokonaniu wstępnej konfiguracji oraz przetestowaniu generowania podpisu cyfrowego i łączności z serwerem CEPiK 2.0.

UWAGA:
Uruchamiając program z parametrem będącym numerem identyfikatora pojazdu, zmieniasz rodzaj testu łączności z testu Hello CEPiK na testowe pytanie o pojazd o podanym numerze identyfikatora.
Jeżeli podany parametr nie jest numerem, użyty zostanie domyślny identyfikator pojazdu.

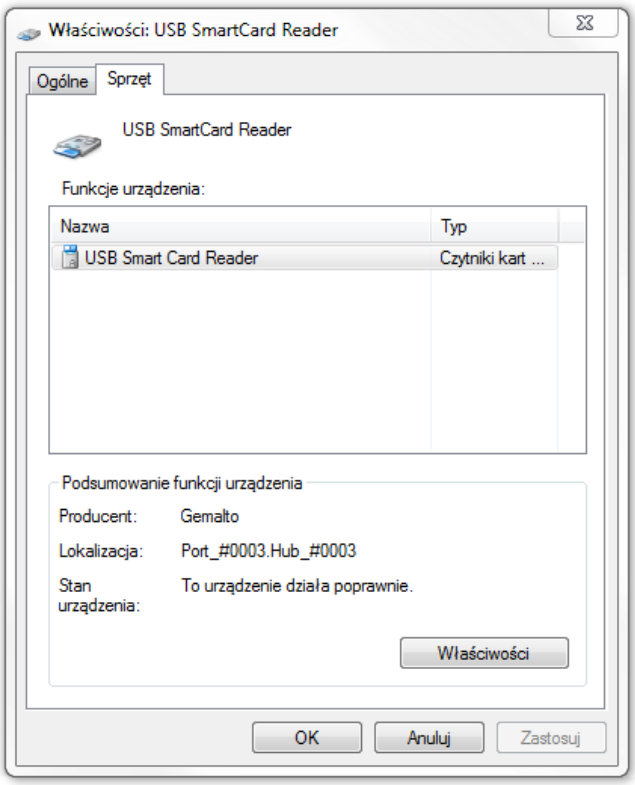


4 Wyłączanie oszczędzania energii przez czytnik USB kart kryptograficznych PKCS#11

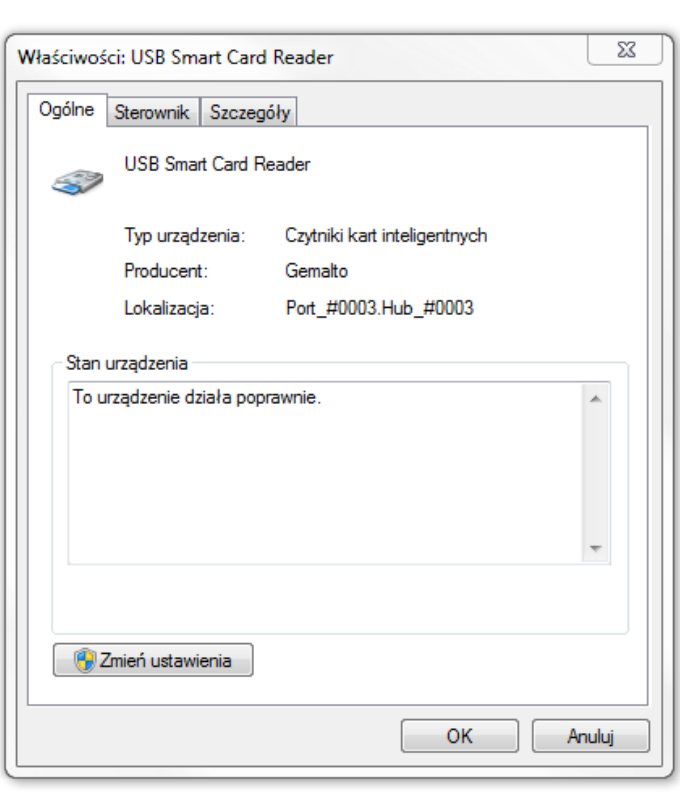
W celu zapewnienia niezawodnego działania czytnika USB należy wyłączyć oszczędzanie energii.



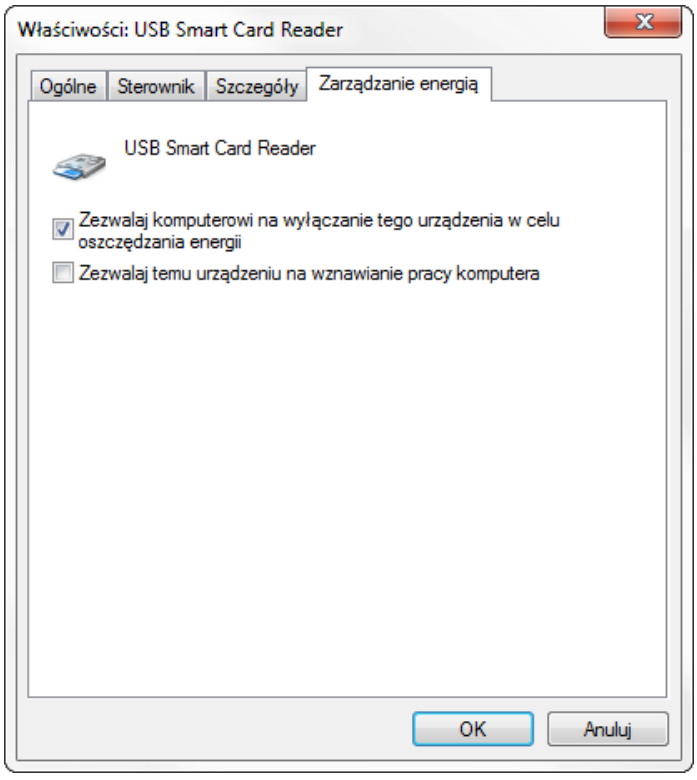
Otwórz panel „Urządzenia i drukarki”, a następnie dwukrotnie kliknij na ikonę czytnika USB.



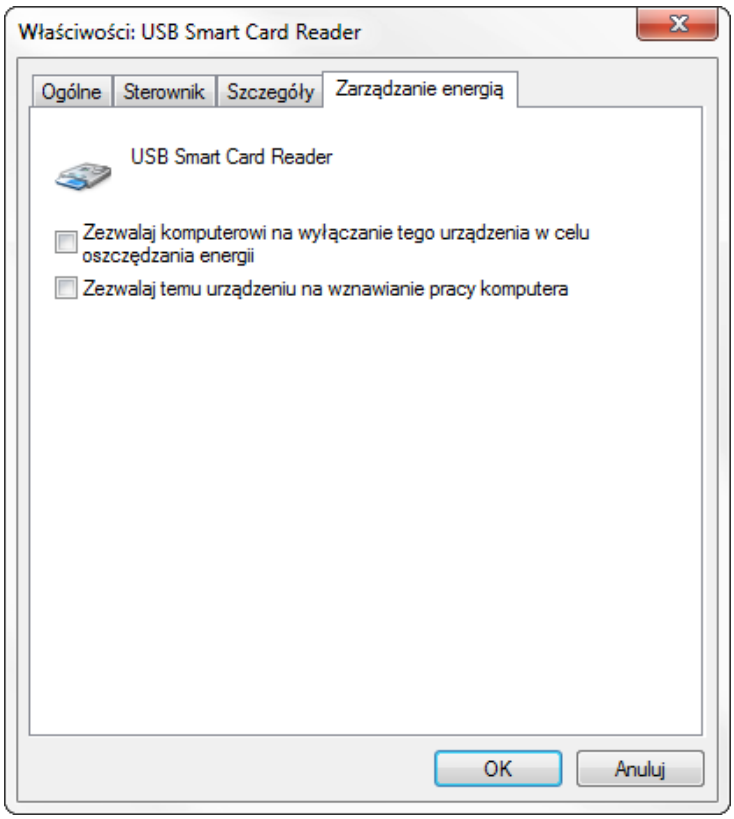
Wybierz z listy czytnik USB i kliknij przycisk ekranowy „Właściwości”.



Kliknij przycisk ekranowy „Zmień ustawienia” i potwierdź zamiar zmiany ustawień w oknie Kontroli Konta Użytkownika (UAC).

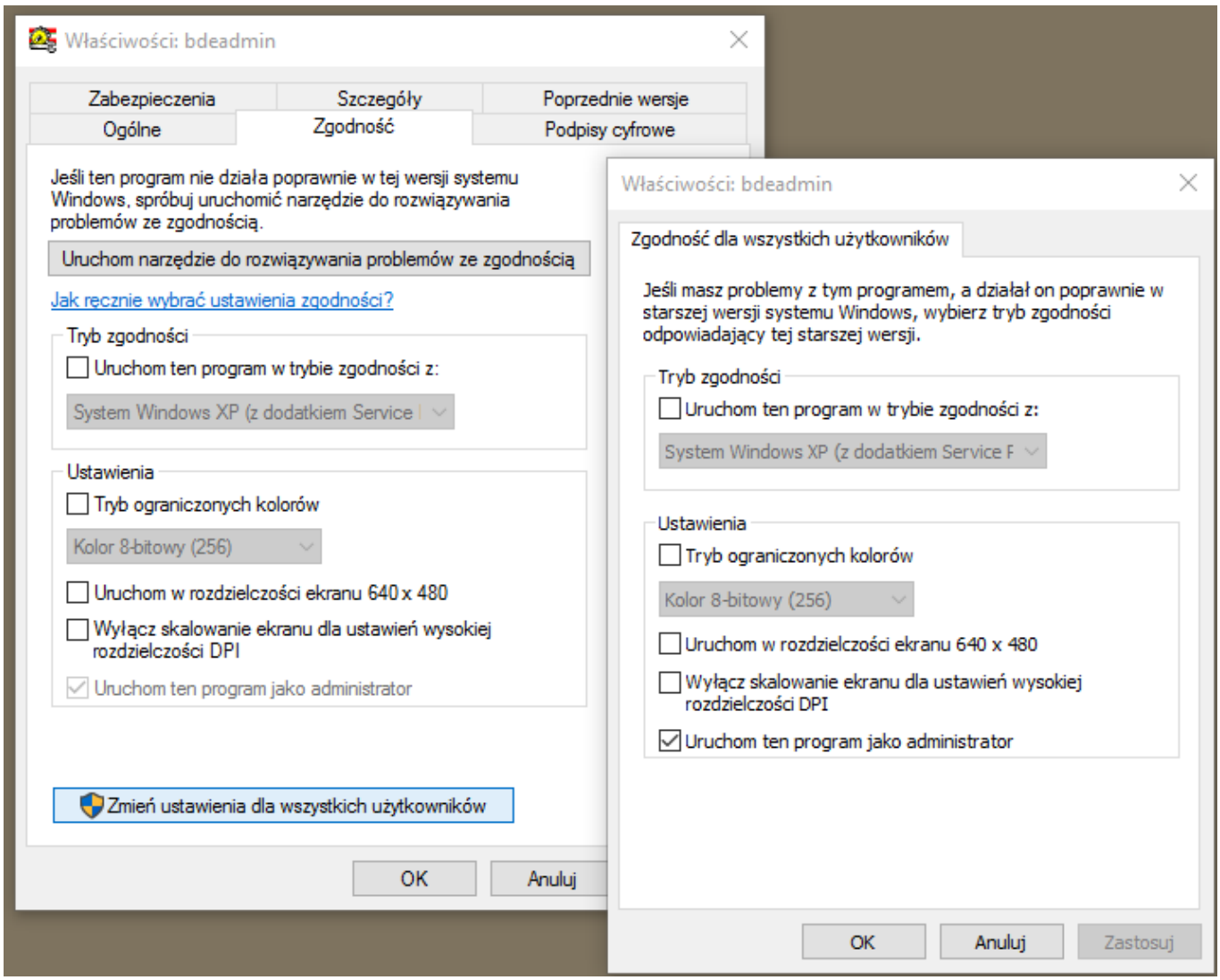


Pojawi się dodatkowa zakładka „Zarządzanie energią”. Jeżeli pole wyboru „Zezwalaj komputerowi na wyłączanie tego urządzenia w celu oszczędzania energii” jest zaznaczone, odznacz je (tzn. usuń zaznaczenie klikając na nie ponownie).



Po wyłączeniu oszczędzania energii, kliknij OK.

Uwaga:
W przypadku korzystania z Windows XP można wyłączyć oszczędzanie energii przez czytnik kart za pomocą Menedżera urządzeń. W tym celu należy rozwinąć gałąź „Czytniki kart inteligentnych”, kliknąć prawym przyciskiem myszki na ten czytnik i wybrać Właściwości, po czym skonfigurować go w powyższy sposób.


Właściwości: bdeadmin
Zabezpieczenia
Szczegóły
Poprzednie wersje
Ogólne
Zgodność
Podpisy cyfrowe
Jeśli ten program nie działa poprawnie w tej wersji systemu Windows, spróbuj uruchomić narzędzie do rozwiązywania problemów ze zgodnością.
Uruchom narzędzie do rozwiązywania problemów ze zgodnością
Jak ręcznie wybrać ustawienia zgodności?
Tryb zgodności
Uruchom ten program w trybie zgodności z:
System Windows XP (z dodatkiem Service
Ustawienia
Tryb ograniczonych kolorów
Kolor 8-bitowy (256)
Uruchom w rozdzielczości ekranu 640 x 480
Wyłącz skalowanie ekranu dla ustawień wysokiej rozdzielczości DPI
Uruchom ten program jako administrator
Zmień ustawienia dla wszystkich użytkowników
OK
Anuluj
Właściwości: bdeadmin
Zgodność dla wszystkich użytkowników
Jeśli masz problemy z tym programem, a działał on poprawnie w starszej wersji systemu Windows, wybierz tryb zgodności odpowiadający tej starszej wersji.
Tryb zgodności
Uruchom ten program w trybie zgodności z:
System Windows XP (z dodatkiem Service F
Ustawienia
Tryb ograniczonych kolorów
Kolor 8-bitowy (256)
Uruchom w rozdzielczości ekranu 640 x 480
Wyłącz skalowanie ekranu dla ustawień wysokiej rozdzielczości DPI
Uruchom ten program jako administrator
OK
Anuluj
Zastosuj

5 Konfiguracja OpenSSL

Podczas instalacji programu do katalogu C:\CEPIK2 instalator powinien ustawić zmienną środowiskową
OPENSSL_KONF=C:\CEPIK2\openssl\ssl\openssl.cnf
i dopisać C:\CEPIK2\openssl\bin na początek ścieżki dostępu PATH .

CEPiK Uploader używa autorskiej wersji OpenSSL, skompilowanej za pomocą gcc z pakietu mingw32, współpracującej ze zgodnym z tą wersją silnikiem kryptograficznym (pluginem) pkcs11.dll.
Dla uniknięcia konfliktów z innymi programami ta wersja OpenSSL czerpie konfigurację ze zmiennej środowiskowej OPENSSL_KONF a nie OPENSSL_CONF.
Dzięki temu te inne programy (np. Symantec Endpoint Protection) zawierające w swoim pliku exe statycznie linkowaną wersję OpenSSL skompilowaną za pomocą MS Visual Studio nie wczytają pluginu pkcs11.dll skompilowanego za pomocą gcc z pakietu mingw32, wykorzystującego inną definicję sterty.

Na początku pliku konfiguracyjnego openssl.cnf znajduje się odnośnik do sekcji openssl_def:

```
openssl_conf  = openssl_def
```

Na końcu tego pliku znajdują się sekcje opisujące konfigurację pluginu pkcs11.dll:

```
[openssl_def]
engines = engine_section

[engine_section]
pkcs11 = pkcs11_section

[pkcs11_section]
engine_id = pkcs11
dynamic_path = C:/CEPIK2/openssl/bin/pkcs11.dll
MODULE_PATH = C:/CEPIK2/openssl/bin/enigmap11.dll
init = 0
```

Proszę pamiętać o rodzaju separatorów nazw podkatalogów ścieżki dostępu
(slash / a nie backslash \ ) używanych w pliku konfiguracyjnym.

Uwaga: nie należy w sekcji [pkcs11_section] zapisywać numeru PIN karty, gdyż jest to sprzeczne z wytycznymi MSWiA. Ponadto program i tak zapyta się o PIN, niezbędny do dokonania podpisu cyfrowego.

Program jest domyślnie skonfigurowany dla czytników USB kart PKCS#11 firmy Encard.

W pliku openssl.cnf należy zmienić MODULE_PATH na
MODULE_PATH = C:/CEPIK2/openssl/bin/crypto3PKCS.dll
(dla profilu zwykłego karty Certum);
MODULE_PATH = C:/CEPIK2/openssl/bin/cmP11.dll
(dla karty EuroCert);
MODULE_PATH = C:/CEPIK2/openssl/bin/CCPkiP11.dll
(dla karty CryptoCard firmy CryptoTech/PWPW).

Uwaga:
Obecna wersja CEPiK Uploadera dokonuje powyższej konfiguracji OpenSSL automatycznie podczas zmiany biblioteki DLL CRYPTOKI w oknie „Ustawienia połączenia”.

Po skonfigurowaniu OpenSSL można go przetestować poleceniami:
openssl engine -t
(rdrand) Intel RDRAND engine
    [available]
(dynamic) Dynamic engine loading support
    [unavailable]
(pkcs11) pkcs11 engine
    [available]

curl --engine list
Build-time engines:
  rdrand
  dynamic
  pkcs11

Dla działania programu CEPiK Uploader ważne jest aby powyższe polecenia wykazały obecność silnika kryptograficznego pkcs11.

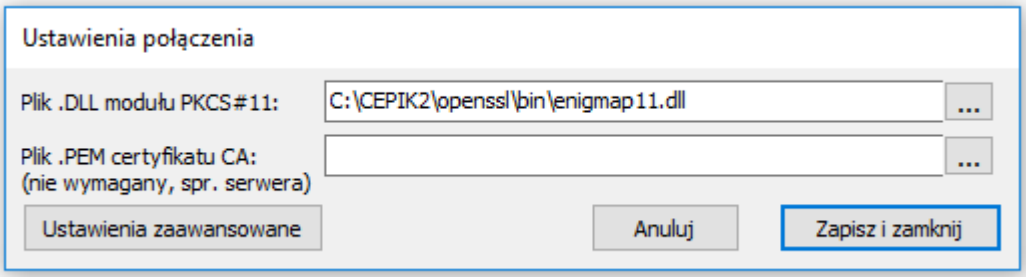
Poniższe polecenie (lub skrypt curl_hello.bat) powinno zapytać użytkownika o PIN i wypisać na ekran definicję WSDL usługi Hello CEPiK (ping).

curl --engine pkcs11 --tlsv1.1 --key-type ENG --cert-type ENG -k https://skp.api.cepik/cepik/ping?wsdl
PKCS#11 token PIN:
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:soap11="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:http="http://schemas.xmlsoap.org/wsdl/http/" xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:wsp200409="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsp200607="http://www.w3.org/2006/07/ws-policy"
xmlns:ns0="http://ping.api.cepik.msw.gov.pl" targetNamespace="http://ping.api.cepik.msw.gov.pl">
<wsdl:types xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:schema>
<xsd:import schemaLocation="ping.xsd2.xsd" namespace="http://ping.api.cepik.msw.gov.pl"/>
<xsd:import schemaLocation="ping.xsd3.xsd"
namespace="http://ping.api.cepik.msw.gov.pl"/></xsd:schema></wsdl:types>
<wsdl:message name="pingRequest">
<wsdl:part name="pingRequest" element="xsns:PING"
[...]

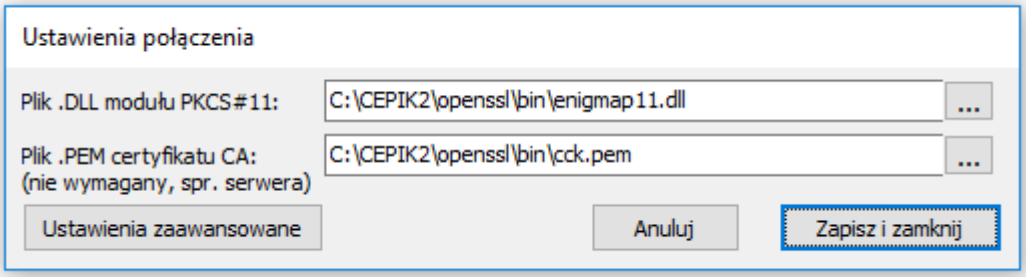
6 Ustawienia połączenia

Po pierwszym uruchomieniu lub kliknięciu przycisku ekranowego „Ustawienia połączenia” pojawi się okno konfiguracji modułu komunikacyjnego programu.
Należy podać ścieżkę do pliku biblioteki DLL modułu kryptograficznego PKCS#11 zgodnego ze standardem CRYPTOKI, klikając górny przycisk […], a następnie [Zapisz i zamknij]
Prawidłowe nazwy plików biblioteki DLL modułu PKCS#11 (CRYPTOKI) to:

enigmap11.dll dla kart Encard Enigma;
crypto3PKCS.dll dla kart Asseco Certum (profil zwykły);
cmP11.dll dla kart EuroCert;
CCPkiP11.dll dla kart CryptoTech Cryptocard.



Opcjonalnie można też podać ścieżkę do pliku PEM zawierającego ważny certyfikat główny CA, co umożliwi weryfikację autentyczności serwera.



Certyfikat główny CA można wyeksportować do formatu PEM używając programu ENCARD-zarządca kart. W tym celu kliknij prawym przyciskiem myszy na certyfikat główny CA (np. „Certyfikat CCK”) i wybierz z menu opcję Eksport certyfikatu.
W oknie dialogowym „Zapisywanie jako” wybierz katalog zapisu (najlepiej „C:\CEPIK2\openssl\bin”), podaj nazwę pliku i wybierz format PEM, a następnie kliknij Zapisz. Nie gwarantuje to jednak, że ten certyfikat CA będzie umożliwiał połączenie z wybranym serwerem, do tego jest potrzebny certyfikat CA tego serwera, udostępniony przez jego właściciela / administratora.

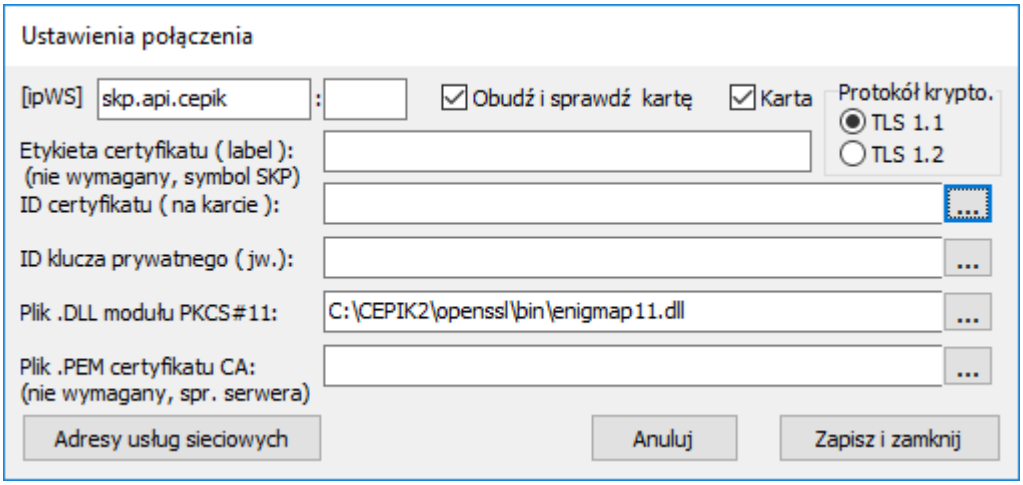
Uwaga: w poniższych poleceniach zakładam że katalogiem bieżącym jest C:\CEPIK2\openssl\bin

Ważność certyfikatu można sprawdzić poleceniem OpenSSL:
openssl x509 -in cck.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 438 (0x1b6)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=PL, O=MSWiA, CN=CCK CEPiK Podsystem dla inst. zew. [...]
        Validity
            Not Before: Jun 9 11:32:23 2010 GMT
            Not After : Jun 9 23:59:59 2020 GMT
[…]

Certyfikat główny w formacie DER (o rozszerzeniu crt lub der) można skonwertować na format PEM poleceniem OpenSSL:
openssl x509 -inform DER -in nazwa_certyfikatu.crt -out nazwa_certyfikatu.pem -text

7 Ustawienia zaawansowane

Po kliknięciu na przycisk ekranowy [Ustawienia Zaawansowane] okno ustawień zmieni wygląd na następujący:



Pole wpisowe [ipWS] przed dwukropkiem określa adres serwera w postaci tekstowej (nazwa domeny) lub numeru IP. Pole wpisowe za dwukropkiem określa numer portu (standardowo 443).
Numer portu należy podać w przypadku gdy pierwsze pole wpisowe zawiera numer IP,
gdy pierwsze pole wpisowe zawiera adres w postaci tekstowej
drugie pole wpisowe zawierające numer portu należy pozostawić puste.

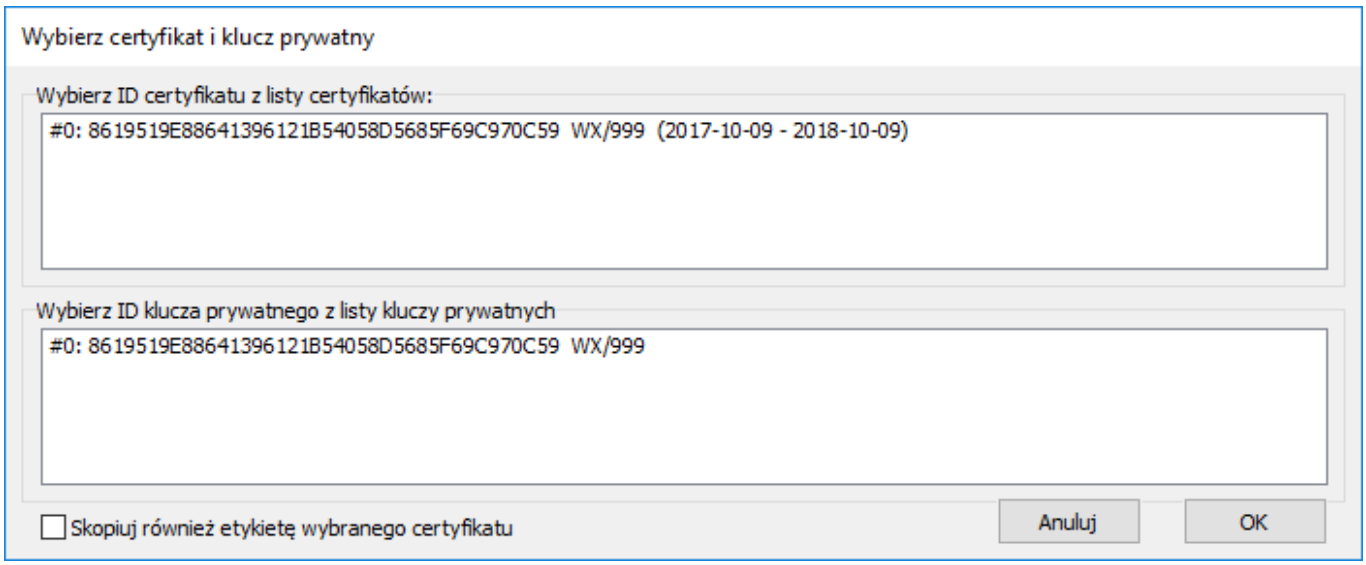
Zaznaczone pole wyboru „Obudź i sprawdź kartę” uaktywnia czytnik kart kryptograficznych, jeżeli jest on w stanie oszczędzania energii, ponadto włącza ostrzeżenia przed zbliżającym się wygaśnięciem ważności certyfikatu (gdy program działa pod kontrolą systemu nowszego niż Windows XP).
W przypadku problemów z czytnikiem kart lub innymi urządzeniami USB (np. drukarki fiskalne) proszę wyłączyć tą opcję i zamiast tego wyłączyć oszczędzanie energii przez czytnik kart (patrz rozdział 4).

Pole wyboru „Karta” określa, czy komunikacja ma odbywać się za pomocą karty kryptograficznej PKCS#11, czy też certyfikatów zapisanych w plikach P12 i PEM.

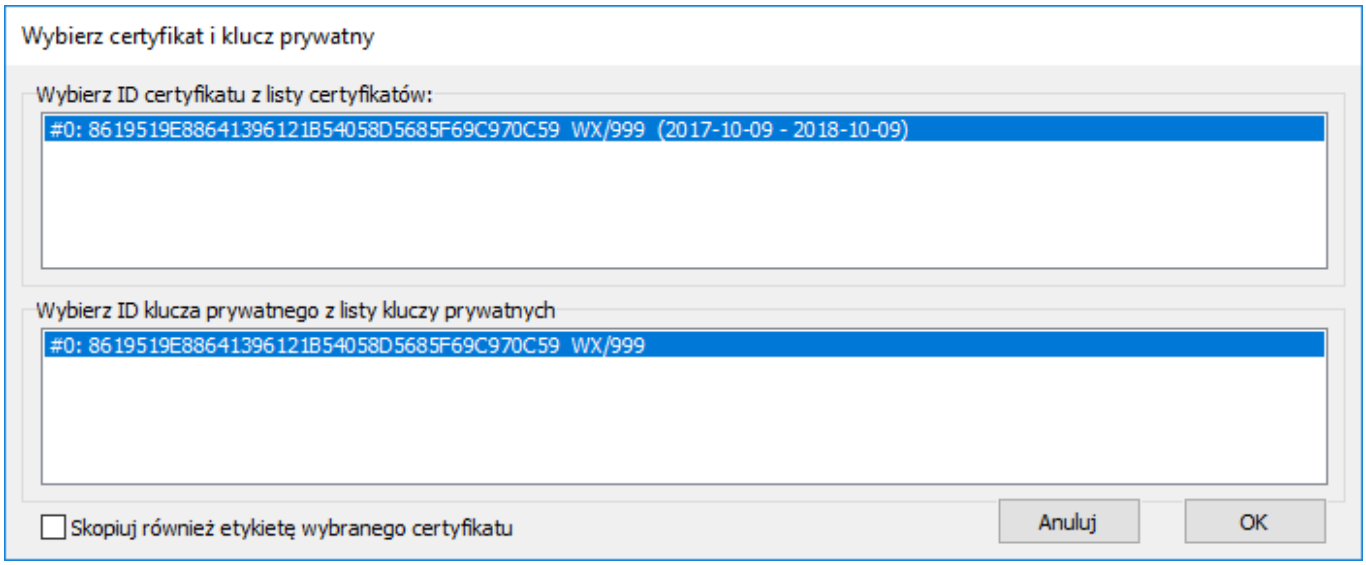
Pole wyboru „Protokół krypto.” określa używaną wersję protokołu TLS.
W przypadku stosowania kart Encard należy wybrać TLS 1.1 z powodu ich ograniczeń sprzętowych.
Użytkownicy korzystający z kart Certum lub certyfikatów zapisanych w plikach mogą wybrać nowszy protokół TLS 1.2.

Pole wpisowe „Etykieta certyfikatu (label)” umożliwia wybór jednego z certyfikatów różniących się etykietą (ang. label) w celu wykorzystania go do wygenerowania podpisu cyfrowego przez program SignSoap.exe. Etykietą certyfikatu jest zwykle symbol SKP, np. WX/999. Jeżeli użytkownik korzysta z tylko jednego czytnika kart i na karcie jest zapisany tylko jeden token, pole to należy pozostawić puste.

Pole wpisowe „ID certyfikatu (na karcie)” umożliwia wybór identyfikatora certyfikatu SKP, co jest niezbędne tylko gdy na karcie jest zapisanych kilka tokenów lub gdy certfikat CA jest pierwszym certyfikatem na liście i posiada identyfikator . W pozostałych przypadkach pole to należy pozostawić puste, gdyż jego wypełnienie powiąże program z konkretnym tokenem i uniemożliwi swobodną wymianę kart kryptograficznych na stanowisku pracy.
Klikając na zaznaczony niebieską ramką przycisk ekranowy […] na prawo od ID certyfikatu można wyświetlić okno wyboru identyfikatora certyfikatu i klucza prywatnego oraz etykiety tego certyfikatu. Przedtem jednak należy podać poprawny PIN karty, niezbędny do odczytania listy kluczy prywatnych.
Uwaga: podając niepoprawny PIN można zablokować kartę!



Po ukazaniu się tego okna kliknij na ID certyfikatu oraz ID klucza prywatnego.



Jeżeli tego nie zrobisz, pola edycyjne ID certyfikatu i ID klucza prywatnego w oknie ustawień połączenia zostaną wyczyszczone po naciśnięciu OK.
Pole wyboru „Skopiuj również etykietę wybranego certyfikatu” umożliwia zapisanie tej etykiety do pola edycyjnego „Etykieta certyfikatu (label)” w oknie ustawień połączenia po naciśnięciu OK.
Jeżeli żaden certyfikat nie zostanie wybrany a powyższe pole wyboru będzie zaznaczone, to po naciśnięciu OK pole etykiety certyfikatu w oknie ustawień połączenia zostanie wyczyszczone.

Pole wpisowe „ID klucza prywatnego (j. w.)” w oknie ustawień połączenia umożliwia wybór identyfikatora klucza prywatnego, co jest niezbędne tylko gdy na karcie jest zapisanych kilka tokenów lub gdy wypełnione zostało pole ID certyfikatu. W pozostałych przypadkach pole to należy pozostawić puste.
Klikając na przycisk ekranowy […] na prawo od ID klucza prywatnego można wyświetlić powyższe okno wyboru identyfikatora certyfikatu i klucza prywatnego oraz etykiety tego certyfikatu.
Przedtem jednak należy podać poprawny PIN karty, niezbędny do odczytania listy kluczy prywatnych.
Uwagi: podając niepoprawny PIN można zablokować kartę!
Jeżeli program jest uruchomiony pod kontrolą systemu Windows XP, wyświetlany jest tylko ID certyfikatu, ponadto funkcja ostrzegania przed zbliżającym się wygaśnięciem certyfikatu jest wyłączona.

Identyfikatory certyfikatów kart Encard Enigma można także wyświetlić za pomocą skryptu show_enigma.bat znajdującego się w katalogu C:\CEPIK2\openssl\bin lub polecenia:
pkcs11-tool.exe --module enigmap11.dll --type cert --list-objects

Dla kart Asseco Certum (profil zwykły) należy użyć skryptu show_certum.bat lub polecenia:
pkcs11-tool.exe --module crypto3PKCS.dll --type cert --list-objects

Dla kart EuroCert należy użyć skryptu show_eurocert.bat lub polecenia:
pkcs11-tool.exe --module cmP11.dll --type cert --list-objects

Dla kart CryptoTech CryptoCard należy użyć skryptu show_cryptocard.bat lub polecenia:
pkcs11-tool.exe --module CCPkiP11.dll --type cert --list-objects

Using slot 0 with a present token (0x0)
Certificate Object, type = X.509 cert
  label: WX/999
  ID: d7f4b99792cc4dd708e408d3eb91b566e0a06c02
Certificate Object, type = X.509 cert
  label: Certyfikat CCK

Skopiuj do schowka identyfikator wybranego certyfikatu (na prawo od ID:) i wklej do pola wpisowego. W tym celu kliknij na ikonę menu systemowego okna cmd (w lewym górnym rogu okna) i wybierz Edytuj → Oznacz. Następnie posługując się klawiszami kursora ustaw kursor na pierwszy znak identyfikatora i trzymając klawisz [Shift] przesuń kursor na prawo od ostatniego znaku, a następnie puść [Shift] i naciśnij [Enter]. Zaznaczony tekst znajdzie się w schowku Windows.

Identyfikatory kluczy prywatnych dla kart Encard Enigma można wyświetlić za pomocą skryptu show_enigma.bat lub polecenia:
pkcs11-tool.exe --module enigmap11.dll --login --login-type user --type privkey --list-objects

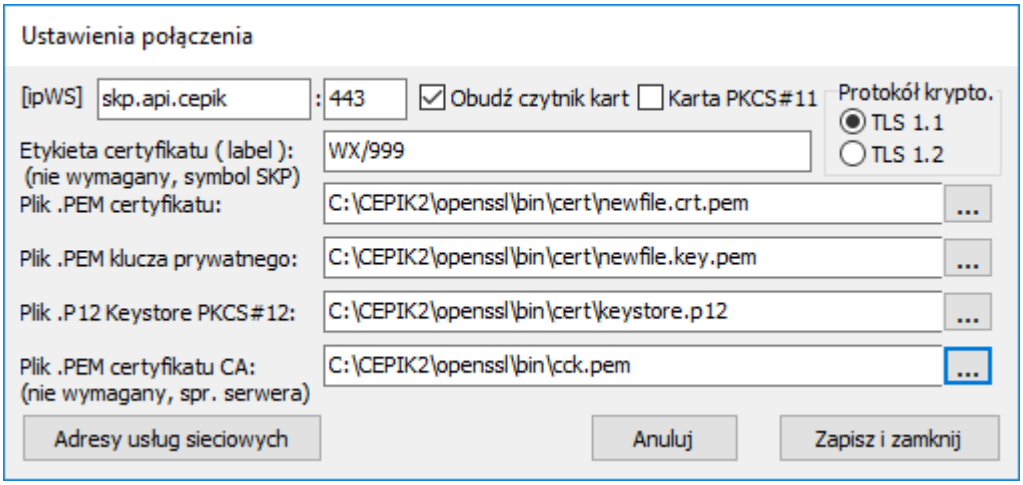
Dla kart Asseco Certum (profil zwykły) należy użyć skryptu show_certum.bat lub polecenia:
pkcs11-tool.exe --module crypto3PKCS.dll --login --login-type user --type privkey --list-objects

Dla kart EuroCert należy użyć skryptu show_eurocert.bat lub polecenia:
pkcs11-tool.exe --module cmP11.dll --login --login-type user --type privkey --list-objects

Dla kart CryptoTech CryptoCard należy użyć skryptu show_cryptocard.bat lub polecenia:
pkcs11-tool.exe --module CCPkiP11.dll --login --login-type user --type privkey –list-objects

Using slot 0 with a present token (0x0)
Logging in to "ENCARD Token kwalifikowany".
Please enter User PIN:
Private Key Object; RSA
  label:
  ID: d7f4b99792cc4dd708e408d3eb91b566e0a06c02
  Usage: decrypt, sign
Skopiuj do schowka identyfikator wybranego klucza prywatnego (na prawo od ID:) i wklej do pola wpisowego.

8 Ustawienia zaawansowane z wykorzystaniem certyfikatów w plikach P12 i PEM



Wyłącznie do celów testowych możliwe jest wykorzystanie certyfikatów umieszczonych w magazynie kluczy (keystore) PKCS#12 czyli w pliku o rozszerzeniu P12 oraz w plikach o rozszerzeniu PEM.

Plik o rozszerzeniu P12 jest używany przez program signsoap.exe, natomiast OpenSSL wykorzystuje certyfikaty i klucze prywatne zapisane w formacie PEM.
Zatem dysponując magazynem kluczy w formacie PKCS#12 należy wyodrębnić z niego klucz prywatny i certyfikaty, zapisując je w formacie PEM.

Służą do tego następujące polecenia OpenSSL:

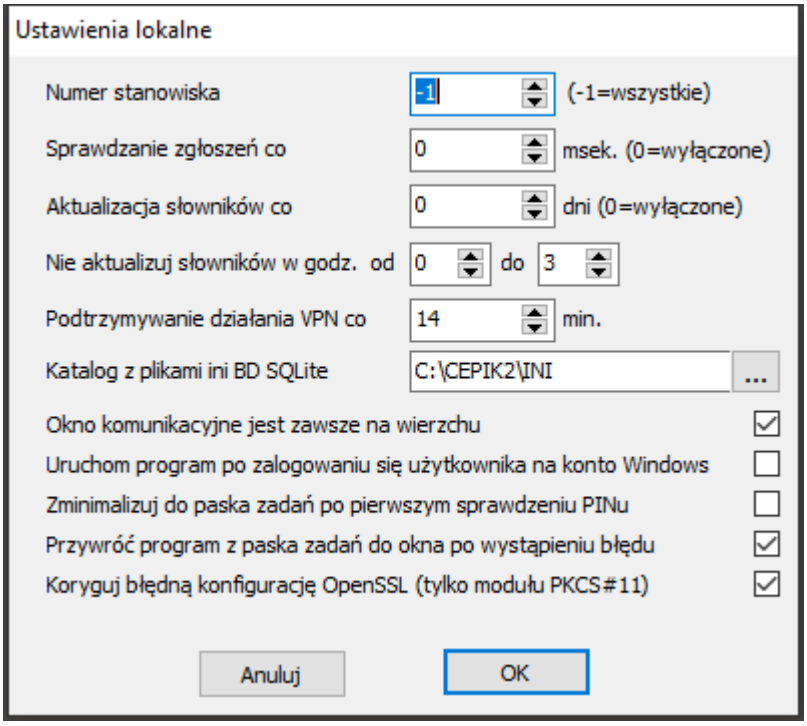
```
openssl pkcs12 -in keystore.p12 -out newfile.crt.pem -clcerts -nokeys
```

```
openssl pkcs12 -in keystore.p12 -out newfile.key.pem -nocerts -nodes
```

```
openssl pkcs12 -in keystore.p12 -out newfile.cacrt.pem -cacerts -nokeys
```

Uwaga:
Certyfikat CA uzyskany w powyższy sposób nie gwarantuje, że będzie on umożliwiał połączenie z wybranym serwerem, do tego jest potrzebny certyfikat CA tego serwera, udostępniony przez jego właściciela / administratora.
Ponieważ certyfikat CA nie jest wymagany, jego pole edycyjne można pozostawić puste.

9 Ustawienia lokalne



„Numer stanowiska” wiąże program CEPiK Uploader uruchomiony na tym stanowisku z konkretną instalacją programu Patronat, działającą w sieci LAN. W przypadku wersji jednostanowiskowej (lokalnej) programu Patronat, numer stanowiska powinien być ustawiony na -1.

„Sprawdzanie zgłoszeń co … msek.” określa, co ile milisekund sprawdzana jest tabela PRPOM, do której program Patronat zapisuje zapytania oraz zgłoszenia i z której odczytuje odpowiedzi. Wartość domyślna 0 wyłącza automatyczne sprawdzanie żądań przez CEPiK Uploader (domyślnie zajmuje się tym program Patronat), obsługa ich jest nadal możliwa za pomocą przycisku ekranowego „Wyślij ponownie” w głównym oknie programu CEPiK Uploader.

„Aktualizacja słowników co … dni.” określa jak często aktualizowane będą słowniki. Wartość 0 wyłącza aktualizację słowników. W środowisku sieciowym wystarczy, że aktualizacja słowników będzie włączona na jednym ze stanowisk sieciowych albo na serwerze, o ile jest na nim zainstalowany program Patronat i CEPiK Uploader.

„Nie aktualizuj słowników w godz. od … do …” blokuje aktualizację słowników w wybranym przedziale czasu, wartości oznaczają pełne godziny, przy czym wartość w polu „od” jest rozumiana włącznie „do” zaś wyłącznie. Aktualizacja nastąpi, gdy program będzie aktywny poza tym przedziałem czasu. Jeśli wartość w polu „od” będzie większa niż wartość w polu „do”, wybrany przedział czasu będzie zawierał północ.

„Podtrzymywanie działania VPN co … min.” określa jak często będzie wywoływana komenda PING w celu podtrzymania połączenia VPN podczas braku aktywności.

„Katalog z plikami ini BD SQLite” określa położenie plików Robocza.ini i Slowniki.ini zawierających m.in. ścieżki do plików bazodanowych SQLite.

Opcja „Okno komunikacyjne jest zawsze na wierzchu” określa sposób jego wyświetlania i czy będzie się ono pojawiać na ekranie, gdy główny moduł jest zminimalizowany do paska zadań.

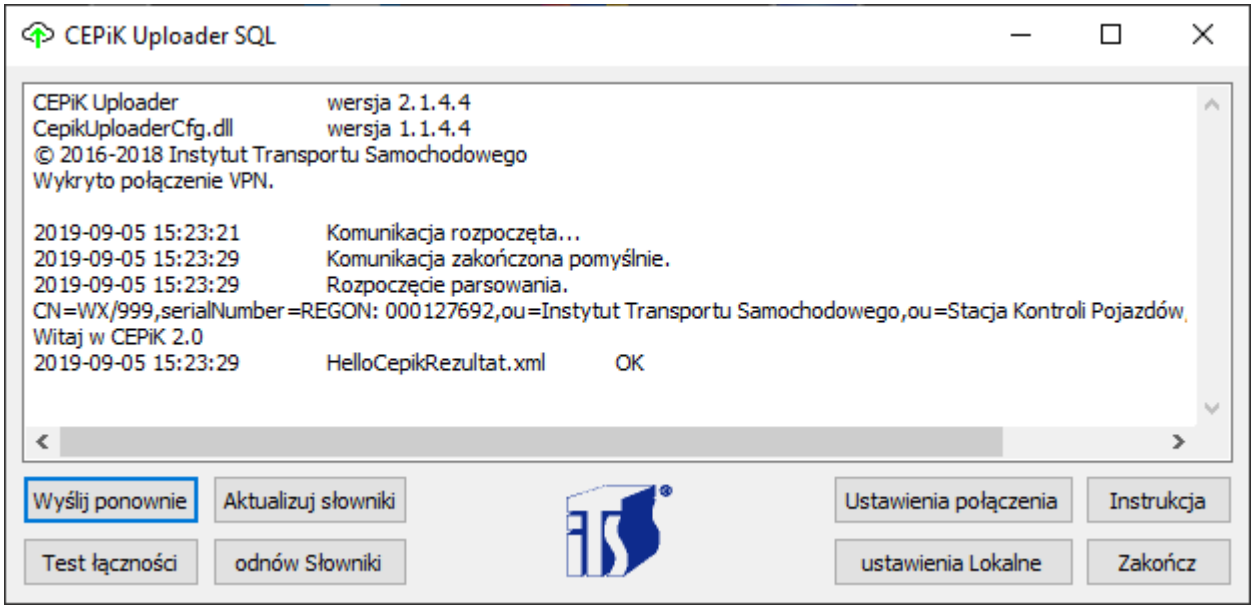
Opcja „Uruchom program po zalogowaniu się użytkownika na konto Windows” uruchamia CEPiK Uploader i wyświetla okienko z pytaniem o PIN karty bezpośrednio po zalogowaniu się użytkownika do systemu Windows. Po poprawnym podaniu PINu następuje przetestowanie łącza i rozpoczęcie pracy programu.

Opcja „Zminimalizuj do paska zadań po sprawdzeniu PINu” sprawia że po podaniu PINu przez użytkownika i przetestowaniu łącza, program jest minimalizowany do paska zadań, dzięki czemu nie zajmuje miejsca na ekranie. Funkcja ta działa tylko jeden raz po każdym uruchomieniu programu.

Opcja „Przywróć program z paska zadań do okna po wystąpieniu błędu” wyświetla główne okno programu z komunikatem o błędzie widocznym w oknie logowania (o ile suwak paska przewijania jest na dole).

Opcja „Koryguj błędną konfigurację OpenSSL (tylko moduł PKCS#11)” pozwala wykryć i usunąć problemy związane z błędną konfiguracją programu uniemożliwiającą działanie karty PKCS#11, takie jak inny moduł PKCS#11 określony w pliku konfiguracyjnym OpenSSL niż podany w oknie ustawień połączenia.

10 Główne okno programu



Przycisk **„Wyślij ponownie”** wymusza ponowne wysłanie niedostarczonych formularzy SKP lub zapytań słownikowych w przypadku wystąpienia błędów transmisji lub działania serwera lub klienta.
Jest on także używany w przypadku, gdy w ustawieniach lokalnych wyłączono sprawdzanie zgłoszeń, wpisując wartość 0. W tym przypadku nie będzie ponawiane wysyłanie formularzy, podczas transmisji których wystąpił błąd.
Przycisk **„Aktualizuj słowniki”** wymusza aktualizację słowników nawet w okresie czasu, gdy nie jest dozwolona automatyczna aktualizacja słowników.
Przycisk **„odnów Słowniki”** powoduje wyczyszczenie i pełną aktualizację słowników.
UWAGA: operacja ta może trwać kilka godzin, zatem powinno się ją wykonywać poza godzinami pracy SKP i tylko gdy jest to konieczne.
Przycisk **„Test łączności”** powoduje wyczyszczenie PINu / hasła i ponowne uruchomienie testu łączności i podpisów cyfrowych. Użycie tej opcji jest zalecane po zmianie karty w czytniku lub wyjęciu karty przed opuszczeniem stanowiska.
Przycisk **„Ustawienia połączenia”** wywołuje okno dialogowe opisane w rozdziałach 6, 7, 8.
Przycisk **„ustawienia Lokalne”** wywołuje okno dialogowe opisane w rozdziale 9.
Przycisk **„Instrukcja”** wyświetla niniejszą instrukcję obsługi oraz informacje o wersji programu.
Przycisk **„Zakończ”** wyłącza program.

Ponadto kliknięcie na logo ITS powoduje przywrócenie domyślnego położenia okna konfiguracyjnego.

Na pasku tytułowym znajduje się poza nazwą programu także informacja o aktywności programu w postaci obracającego się elementu semigraficznego. Jest on widoczny tylko gdy program jest aktywny, czyli sprawdza cyklicznie tablicę PRPOM lub pobiera słowniki.

Informacje wyświetlane na ekranie logów są zapisywane do plików znajdujących się w katalogu „Dokumenty” w podkatalogu „CEPIKuploader”.
Log z bieżącego lub ostatniego uruchomienia programu znajduje się w pliku LogOstatni.txt, log z poprzedniego uruchomienia w pliku Log0.txt, logi poprzednie względem Log0.txt w plikach od Log1.txt do Log9.txt (najstarszy).
Logi te można przeglądać za pomocą Notatnika zawartego w systemie operacyjnym Windows.
Jeżeli plik logów nie mieści się w Notatniku, polecam darmowy program NoteTab Light.