Ministerstwo
Spraw Wewnętrznych

Wytyczne dotyczące podłączenia Krajowych Podmiotów Uprawnionych do podsystemu CBE systemu CEPiK 2.0

Centralna Ewidencja Pojazdów i Kierowców (CEPiK)

Metryka dokumentu:

System:	CEPiK 2.0
Nr wersji dokumentu:	1.2
Data ostatniej zmiany:	2014-04-17
Ostatnia zmiana:	Dodano informację o DNS

SPIS TREŚCI

1 INFORMACJE OGÓLNE

Dokument przedstawia wytyczne dotyczące podłączenia podmiotów uprawnionych do modułu CBE uruchomionego w nowej wersji systemu CEPiK, tj. CEPiK 2.0, w ramach Krajowego Punktu Kontaktowego.

Zadaniem Krajowego Punktu Kontaktowego jest umożliwienie i usprawnienie transgranicznej wymiany danych rejestracyjnych pojazdów, która powinna ułatwić identyfikację osób podejrzanych o popełnienie przestępstw lub wykroczeń związanych z bezpieczeństwem ruchu drogowego.

Funkcjonalność systemu Krajowego Punktu Kontaktowego umożliwia wyszukanie informacji o właścicielach i/lub posiadaczach pojazdów, w których popełniono następujące przestępstwa lub wykroczenia związane z bezpieczeństwem ruchu drogowego:

- Przekroczenie dopuszczalnej prędkości
- Kierowanie pojazdem pod wpływem alkoholu
- Niedopełnienie obowiązku korzystania z pasów bezpieczeństwa
- Niezastosowanie się do czerwonego sygnału świetlnego
- Korzystanie z niedozwolonej części drogi
- Kierowanie pojazdem pod wpływem środków odurzających
- Niedopełnienie obowiązku używania w czasie jazdy hełmów ochronnych
- Niezgodne z prawem korzystanie z telefonu komórkowego lub innych środków łączności podczas kierowania pojazdem

Informacje przekazywane do Krajowych Podmiotów Uprawnionych z poszczególnych Państw Członkowskich Unii Europejskiej będą zawierały informacje o pojeździe jak i o jego właścicielu lub/i posiadaczu zgodnie ze stanem na dzień i godzinę popełnienia przestępstwa lub wykroczenia.

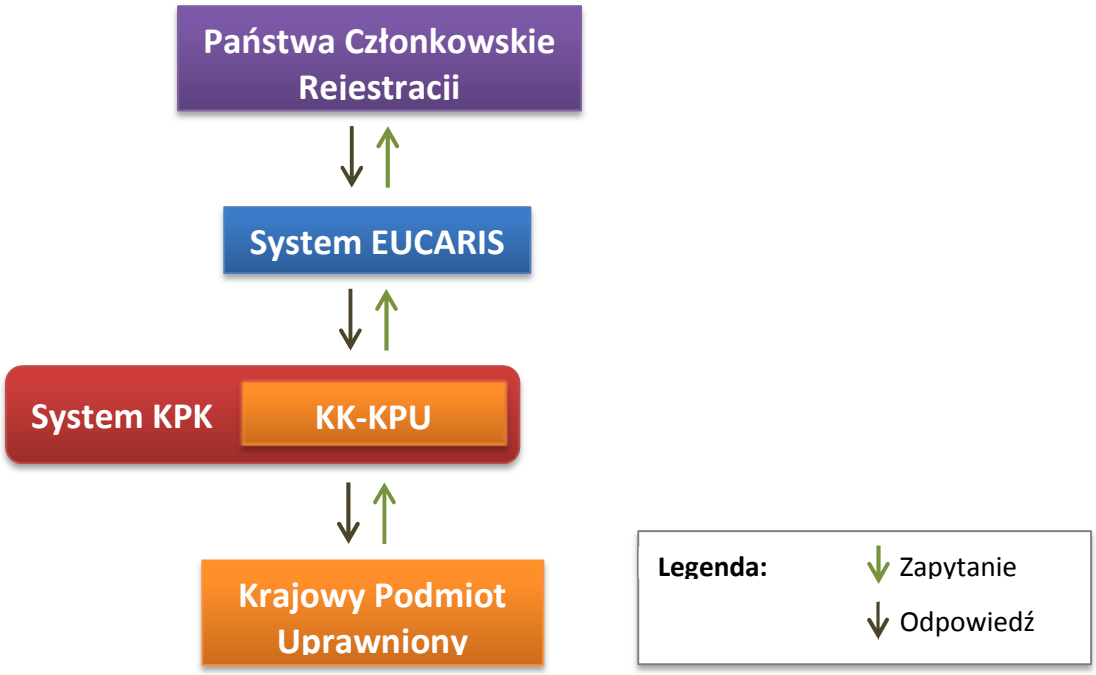
Wymiana danych będzie realizowana za pośrednictwem systemu europejskiego EUCARIS oraz zaimplementowanego modułu CBE w systemie CEPiK 2.0. Na mocy ustawy, wyznaczonym podmiotem (zwanym dalej Krajowym Punktem Kontaktowym – KPK) do realizacji podłączenia Krajowych Podmiotów Uprawnionych do europejskiego systemu wymiany informacji jest Ministerstwo Spraw Wewnętrznych.

Krajowy Punkt Kontaktowy przewiduje dwa sposoby dostępu podmiotów uprawnionych:

1. **Dedykowana aplikacja WWW** – uruchamiana na przeglądarce internetowej strona www dająca możliwość złożenia pojedynczego wniosku do PCzł z zapytaniem o dane właściciela i/lub posiadacza pojazdu. Zapytania realizowane są w trybie synchronicznym.
2. **Usługi web service** – protokół SOAP do komunikacji System-to-System za pomocą wiadomości XML. Pozwala złożyć zapytania pojedyncze i złożone (batch mode) do pojedynczego PCzł.

Podmioty uprawnione będą podłączone do modułu CBE w systemie CEPiK 2.0 poprzez sieć publiczną Internet lub za pośrednictwem już istniejących łączy dedykowanych, w pierwszym przypadku z wykorzystaniem technologii wirtualnych sieci prywatnych (ang. Virtual Private Network – VPN). Takie rozwiązanie pozwoli zminimalizować, a często uniknąć dodatkowych kosztów podłączenia po stronie podmiotów zewnętrznych zapewniając przy tym wysokie bezpieczeństwo komunikacji. Połączenie VPN będzie nawiązywane za pomocą certyfikatu lokalizacji i obowiązkiem administratora podmiotu będzie odpowiednie zabezpieczenie tego certyfikatu tak, aby użytkownicy nie mieli do niego dostępu. Po nawiązaniu bezpiecznego połączenia użytkownik lub system zewnętrzny będzie w stanie skorzystać z usług systemu CEPiK tylko za pomocą tzw. certyfikatu użytkownika do komunikacji SSL.

Ogólny zarys wymiany danych przedstawia poniższy schemat.



UWAGA!: **Niniejszy dokument opisuje wytyczne w zakresie podłączenia do modułu CBE systemu CEPiK w szczególności dla obecnych użytkowników systemu, którzy na mocy przepisów prawa uzyskają dostęp do tego modułu.**

W sytuacji, gdy podmiot uprawniony nie posiada jeszcze dostępu do systemu CEPiK w trybie teletransmisji danych, musi przejść pełną procedurę uzyskania formalnego dostępu do systemu CEPiK. Szczegóły są dostępne pod adresem www.cepik.gov.pl → zakładka Informacje → artykuł „Udostępnianie danych przetwarzanych w SI CEPiK z wykorzystaniem sieci Internet" → link do artykułu TUTAJ.

W przypadku nieposiadania formalnej zgody na dostęp do systemu CEPiK w trybie teletransmisji danych, w celu uzyskania szczegółowych informacji o procedurze uzyskania dostępu prosimy o kontakt z Wydziałem Udostępniania Danych Departamentu Ewidencji Państwowych Ministerstwa Spraw Wewnętrznych, tel. (22) 60-28-208.

2 UWIERZYTELNIENIE LOKALIZACJI

Przy dostępie poprzez sieć publiczną Internet uwierzytelnienie lokalizacji realizowane jest za pomocą certyfikatu lokalizacji (certyfikat na połączenie VPN). Dla dostępu do systemu realizowanego przez sieć wydzieloną uwierzytelnienie realizowane jest z zastosowaniem certyfikatu użytkownika (SSL). Użytkownicy sytemu korzystający z sieci publicznej Internet mogą łączyć się z wykorzystaniem dwóch typów połączeń VPN:

- połączenie typu **LAN-to-LAN**,
- połączenie typu **remote access**.

2.1 POŁĄCZENIE TYPU LAN-TO-LAN

Komputery w lokalizacji mogą korzystać z połączenia VPN bez instalacji dodatkowego oprogramowania, ponieważ urządzenie sieciowe np. Router zapewnia funkcjonowanie VPN w sposób niezauważalny dla stacji roboczych.

Użytkownik modułu CBE, który będzie chciał zestawić połączenie VPN LAN-to-LAN, powinien posiadać urządzenie sieciowe wspierające protokół IPsec oraz wsparcie dla określonego algorytmu szyfrowania.

2.2 POŁĄCZENIE TYPU REMOTE ACCESS

W przypadku lokalizacji zestawiających połączenie typu remote access, niezbędne będzie zainstalowanie na stacji roboczej oprogramowania Cisco VPN Client. Użytkownik może także wykorzystać dostępne oprogramowanie alternatywne, które jest kompatybilne z protokołem IPSec i rozwiązaniami VPN firmy Cisco. Możliwe jest również wykorzystanie oprogramowania Cisco AnyConnect, ale wymaga to posiadania przez użytkownika odpowiedniej licencji.

3 UWIERZYTELNIENIE UŻYTKOWNIKA

Po nawiązaniu połączenia VPN użytkownicy uzyskają dostęp do usług WWW / Web Service modułu CBE. Aby móc skorzystać z usług WWW / Web Service modułu CBE wymagane jest uwierzytelnienie za pomocą certyfikatu użytkownika, przy czym certyfikaty i klucze prywatne użytkowników korzystających z aplikacji WWW będą bezwarunkowo przechowywane na mikroprocesorowych kartach kryptograficznych. Certyfikaty i klucze prywatne użytkowników korzystających z własnych systemów (tzw. systemów zewnętrznych) mogą być przechowywane w postaci plików, przy zachowaniu odpowiedniego poziomu bezpieczeństwa. Odpowiedzialność za zapewnienie niezbędnego poziomu bezpieczeństwa w ramach systemów zewnętrznych, w szczególności w zakresie zapewnienia kontroli dostępu do pomieszczeń, stanowiska komputerowego, karty kryptograficznej oraz rozliczalności wykonywanych czynności, leży po stronie podmiotu.

Wykorzystując mechanizm protokołu ssl: *client authentcation* możliwe jest uwierzytelnienie użytkownika. Użytkownik próbując nawiązać połączenie SSL jest proszony o przedstawienie ważnego certyfikatu. Oprogramowanie użytkownika (system zewnętrzny w przypadku usług typu WebService lub przeglądarka internetowa w przypadku użytkownika indywidualnego) wysyła odpowiedni certyfikat podpisując komunikację swoim kluczem prywatnym. W ten sposób serwer może uwierzytelnić, że użytkownik przedstawił się ważnym certyfikatem i posiada odpowiadający mu klucz prywatny.

Przy uwierzytelnianiu z wykorzystaniem kart kryptograficznych (w przypadku użytkowników indywidualnych) klucz prywatny certyfikatu użytkownika nie jest w ogóle przesyłany do komputera użytkownika. Deszyfrowanie i podpisywanie odbywa się w układzie karty kryptograficznej, dzięki czemu klucz prywatny jest chroniony wewnątrz samej karty. Wymaga to użycia karty przy każdej próbie nawiązania połączenia SSL.

4 WYTYCZNE DLA PODMIOTÓW UPRAWNIONYCH

W celu podłączenia do systemu CBE, podmioty uprawnione muszą spełnić określone wymagania związane z bezpieczeństwem, opisane w dokumencie „**Wymagania i zalecenia bezpieczeństwa dla podmiotów wnioskujących o dostęp lub zmianę warunków dostępu do systemu teleinformatycznego Centralnej Ewidencji Pojazdów i Kierowców z wykorzystaniem sieci publicznej Internet**”.

W przypadku podmiotów uprawnionych, korzystających aktualnie z wydzielonych sieci transmisji danych oraz własnych systemów (tzw. systemów zewnętrznych) lub rozwiązania PIC, zastosowanie mają zawarte umowy oraz porozumienia w zakresie dostępu tych podmiotów do systemu informatycznego Centralnej Ewidencji Pojazdów i Kierowców.

4.1 WYMAGANIA ZWIĄZANE Z POŁĄCZENIAMI VPN TYPU REMOTE ACCESS

Podmiot musi posiadać:

- stację roboczą,
- czytnik kart kryptograficznych,
- kartę kryptograficzną,
- certyfikat na połączenie VPN wydany w ramach **Polityki certyfikacji dla urządzeń systemu CEPiK**,
- certyfikat użytkownika na karcie kryptograficznej wydany w ramach **Polityki certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK łączących się przez sieć publiczną**.

Szczegółowe wymagania techniczne zostały wskazane w rozdziale 6.

4.2 WYMAGANIA ZWIĄZANE Z POŁĄCZENIAMI VPN TYPU LAN-TO-LAN

Podmiot musi posiadać:

- urządzenie sieciowe do zestawienia połączenia LAN-to-LAN,
- w przypadku, gdy korzysta z aplikacji WWW – stację roboczą, czytnik kart oraz kartę kryptograficzną, certyfikat na karcie kryptograficznej wydany w ramach **Polityki certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK łączących się przez sieć publiczną**,
- w przypadku, gdy korzysta z Web Service – certyfikat użytkownika dla systemu zewnętrznego, wydany w ramach **Polityki certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK łączących się przez sieć publiczną**.

W przypadku połączeń typu LAN-to-LAN certyfikat z kluczem prywatnym lokalizacji jest przechowywany tylko i wyłącznie na dedykowanym urządzeniu sieciowym. Tam skonfigurowane są parametry połączenia VPN i połączenie to jest transparentnie udostępniane podłączonym stacjom roboczym lub systemowi zewnętrznemu. Urządzenie sieciowe musi być odpowiednio zabezpieczone przed nieupoważnionym dostępem, zarówno fizycznym jak i zdalnym. Dostęp do urządzenia musi być

zabezpieczony hasłem (jeśli urządzenie to umożliwia, należy stosować imienne konta). Certyfikat z kluczem prywatnym lokalizacji nie jest dostępny dla użytkowników.

W przypadku systemów zewnętrznych klucz prywatny certyfikatu użytkownika może być przechowywany w postaci pliku. W związku z tym plik ten musi być odpowiednio zabezpieczony m.in.:

- na poziomie uprawnień systemu plików i systemu operacyjnego,
- usługi i aplikacje uruchomione w tym samym systemie muszą być odpowiednio odizolowane (osobny użytkownik oraz izolacja środowiska – tzw. sandbox),
- powinien być zainstalowany i na bieżąco aktualizowany program antywirusowy,
- niezbędne jest monitorowanie pracy systemu i analiza logów.

Za wdrożenie odpowiedniego poziomu zabezpieczeń w ramach lokalnej polityki bezpieczeństwa podmiotu odpowiada personalnie Kierownik jednostki organizacyjnej i delegowany przez niego lokalny administrator systemu.

5 PODŁĄCZENIE I CERTYFIKACJA

Przed pierwszym podłączeniem do systemu CEPiK 2.0 podmiot uprawniony musi posiadać certyfikaty pozwalające na poprawne uwierzytelnienie i zestawienie połączenia VPN. Certyfikaty wydaje Centrum Certyfikacji MSW. Ogólne kroki postępowania w celu uzyskania certyfikatów:

1. Administrator podmiotu generuje prywatny klucz lokalizacji na urządzeniu sieciowym,
2. Wykorzystując wygenerowany klucz prywatny, administrator generuje żądanie podpisania certyfikatu lokalizacji (ang. certificate signing request – CSR) z odpowiednimi parametrami, a następnie wysyła to żądanie jako załącznik do wniosku o wydanie certyfikatów do Centrum Certyfikacji MSW. [1]
3. W przypadku, gdy podmiot będzie korzystał z połączenia VPN typu Remote Access, administrator wybiera we wniosku opcję wygenerowania certyfikaty w postaci pkcs#12.
4. Centrum Certyfikacji MSW sprawdza poprawność wniosku oraz żądania CSR i generuje certyfikat. Następnie certyfikat jest wysyłany do administratora podmiotu.
5. Administrator podmiotu konfiguruje oprogramowanie Cisco VPN Client lub router sieciowy.
6. Administrator podmiotu dla każdej karty kryptograficznej:
    a. wykorzystując oprogramowanie do zarządzania kartą kryptograficzną generuje żądanie CSR dla certyfikatu użytkownika z odpowiednimi parametrami, następnie żądanie wysyłane jest razem z wnioskiem do Centrum Certyfikacji MSW[1].
    b. Centrum Certyfikacji sprawdza poprawność wniosku, żądania, generuje certyfikat i wysyła do wnioskodawcy.
7. W przypadku systemu zewnętrznego:
    a. Administrator systemu zewnętrznego generuje klucz prywatny systemu.
    b. Za pomocą tego klucza generowane jest żądanie podpisania certyfikatu użytkownika z odpowiednimi parametrami, a następnie wysyłane jest razem z wnioskiem do Centrum Certyfikacji MSW[1].
    c. Centrum Certyfikacji MSW sprawdza poprawność wniosku i żądania, generuje certyfikat i wysyła do wnioskodawcy.
    d. Administrator konfiguruje system do korzystania z otrzymanego certyfikatu i odpowiadającego mu klucza prywatnego.

Po wykonaniu powyższych kroków możliwe jest korzystanie z usług WWW / Web Service podsystemu CBE.

W przypadku użytkowników aplikacji WWW uruchomienie aplikacji będzie wyglądać następująco:

1. Użytkownik z ograniczonymi uprawnieniami loguje się do systemu operacyjnego.
2. W przypadku połączeń LAN-to-LAN połączenie VPN jest już nawiązane. W przypadku remote access połączenie to jest automatycznie lub na żądanie użytkownika inicjowane (może to wymagać uprawnień administratora, musi być w związku z tym odpowiednio zabezpieczone).
3. Użytkownik uruchamia przeglądarkę internetową i łączy się z systemem poprzez zestawione wcześniej połączenie VPN. Następnie proszony jest o wskazanie odpowiedniego certyfikatu z

[1] Żądania CSR wysyłane do Centrum Certyfikacji MSW muszą być dostarczone z wnioskiem, na podstawie odpowiedniego wzoru.

karty kryptograficznej i potwierdzeniu operacji PIN kodem, w celu nawiązania połączenia ssl i dokonania uwierzytelnienia.

4. Po poprawnym uwierzytelnieniu możliwe jest korzystanie z usługi WWW zgodnie z instrukcją obsługi i jej przeznaczeniem.

Szczegółowy opis postępowania i obsługi aplikacji został opisany w podręczniku użytkownika końcowego aplikacji WWW CBE.

6 ZAGADNIENIA TECHNICZNE

6.1 STACJA ROBOCZA

Komputer klasy PC o parametrach pozwalających na uruchomienie wymaganego oprogramowania:

- system operacyjny: Microsoft Windows Vista lub nowszy, alternatywnie system Linux,
- oprogramowanie Cisco VPN Client, lub oprogramowanie równoważne zapewniające wykorzystanie IPSec i poprawną komunikację z rozwiązaniami VPN Cisco,
- oprogramowanie ochrony antywirusowej z zapewnioną opcją aktualizacji definicji wirusów,
- przeglądarka internetowa (wspierane przeglądarki to Mozilla Firefox 4.5 lub nowsza, Google Chrome lub Internet Explorer w wersji 8 lub nowszej),
- oprogramowanie do zarządzania karta kryptograficzną, w szczególności umożliwiające wygenerowanie pary kluczy na karcie i stworzenie CSR-a w formacie PKCS#10.

6.2 CZYTNIK KART KRYPTOGRAFICZNYCH

- zgodny z PC/SC,
- sterowniki umożliwiające poprawną pracę czytnika w środowisku Windows Vista z Service Pack 1 (lub wyższym), Windows 7, Windows 8, Linux.

6.3 KARTA KRYPTOGRAFICZNA

- 32kB pamięci EPROM na certyfikaty, klucze kryptograficzne oraz kody PIN,
- operacje na kluczach asymetrycznych RSA o długości do 2048 bitów,
- algorytmy symetryczne DES, Triple-DES,
- funkcja skrótu SHA-1,
- zgodność z czytnikami PC/SC,
- zgodność ze standardami: ISO 7816-3, 7816-4, 7816-5, 7816-6, 7816-8,
- zgodność ze standardem PKCS#11,
- certyfikacja do poziomu ITSEC E3 High, zgodnie z wymogami Ustawy o Podpisie Elektronicznym.

6.4 URZĄDZENIE SIECIOWE

- kompatybilność z rozwiązaniami Cisco VPN,
- algorytm szyfrowania: AES256,
- funkcja HMAC: SHA.

6.5 POŁĄCZENIE VPN LAN-TO-LAN – KONFIGURACJA URZĄDZENIA SIECIOWEGO

- Host: 193.150.69.234
- IPsec – użycie certyfikatu
- Faza 1:

  - algorytm szyfrowania: AES256,
  - funkcja HMAC: SHA,
  - grupa DH: 2,
  - uwierzytelnianie urządzenia: certyfikat.

- Faza 2:
  - algorytm szyfrowania AES 256,
  - funkcja HMAC: SHA.

6.6 DNS

- Adres serwera DNS, który należy skonfigurować na stacji dostępowej lub we własnym systemie:
  - 10.203.30.3 dla dostępu przez sieć Internet
  - 10.203.26.228 dla dostępu przez łącza dedykowane

7 DOKUMENTY I PLIKI POWIĄZANE

1. Wymagania i zalecenia bezpieczeństwa dla podmiotów wnioskujących o dostęp lub zmianę warunków dostępu do systemu teleinformatycznego Centralnej Ewidencji Pojazdów i Kierowców z wykorzystaniem sieci publicznej Internet.
2. Polityka certyfikacji dla instytucji zewnętrznych korzystających z Systemu Informatycznego CEPiK, łączących się przez sieć publiczną.
3. Polityka Certyfikacji dla urządzeń Systemu Informatycznego CEPiK.
4. Formularz wniosku o certyfikat klucza publicznego dla urządzenia współpracującego z Systemem Informatycznym CEPiK.
5. Formularz wniosku o certyfikat klucza publicznego dla instytucji zewnętrznych, łączących się przez sieć publiczną z Systemem Informatycznym CEPiK.
6. Instalator ENCARD (dostępny po zalogowaniu na swoje konto na portalu www.cepik.gov.pl)
7. Instalator CISCO VPN Client (dostępny po zalogowaniu na konto w portalu www.cepik.gov.pl)
8. Podręcznik użytkownika aplikacji WWW CBE (dostępny po zalogowaniu na konto w portalu www.cepik.gov.pl)
9. Opis interfejsów Web Service (dostępny na życzenie → patrz rozdział 10).

8 INFORMACJE DLA UŻYTKOWNIKÓW DOTYCZĄCE SKŁADANIA WNIOSKU O WYDANIE / ZAWIESZENIE / UCHYLENIE ZAWIESZENIA / UNIEWAŻNIENIE CERTYFIKATÓW LOKALIZACJI I UŻYTKOWNIKA

Aby skorzystać z usług modułu CBE, użytkownik musi posiadać przynajmniej dwa certyfikaty pozwalające na poprawne uwierzytelnienie i autoryzację:

- certyfikat lokalizacji (do zestawienia połączenia VPN),
- jeden lub więcej certyfikatów użytkownika (do nawiązania połączenia https – SSL).

Certyfikaty są wydawane przez Centrum Certyfikacji MSW na pisemny wniosek użytkownika (Subskrybenta). Do wniosku należy dołączyć wygenerowane przez subskrybenta żądanie podpisania certyfikatu (tzw. CSR) lub mikroprocesorową kartę kryptograficzną (dla certyfikatów użytkownika) i/lub nośnik do nagrania certyfikatu lokalizacji (dla certyfikatu na połączenie VPN).

Niniejszy dokument opisuje sposób wypełniania wniosków o wydanie certyfikatów, procedurę generacji żądań CSR oraz sposób instalacji tych certyfikatów.

8.1 CERTYFIKAT LOKALIZACJI

Certyfikat lokalizacji służy do uwierzytelniania lokalizacji Subskrybenta. Powinien on być zainstalowany na urządzeniu sieciowym nawiązującym połączenie VPN z systemem CEPiK lub bezpośrednio na stacji dostępowej. Dostęp do klucza prywatnego tego certyfikatu powinien posiadać tylko administrator placówki i powinien on być zabezpieczony przed dostępem innych użytkowników i osób trzecich.

8.1.1 WNIOSEK O WYDANIE CERTYFIKATU LOKALIZACJI

Subskrybent w celu nawiązania połączenia VPN z systemem CEPiK powinien w pierwszej kolejności uzyskać certyfikat lokalizacji wydany przez Centrum Certyfikacji MSW. Aby to zrobić musi wypełnić wniosek o wydanie certyfikatu w Polityce certyfikacji dla urządzeń systemu CEPiK.

Wniosek należy wypełnić zgodnie z poniższymi wytycznymi:

- *Pieczęć Subskrybenta* (pieczęć podmiotu wnioskującego o wydanie certyfikatu);
- *Podstawa wnioskowania o certyfikat* – powołanie się na przepisy prawa, np. dla CBE będzie to „*art. 80k ust. 4 pkt. … ustawy Prawo o ruchu drogowym (Dz. U. …)*”.

- *Data wypełnienia wniosku* – należy podać datę, kiedy wniosek jest wypełniany przez Subskrybenta w formacie DD-MM-RRRR (dzień-miesiąc-rok);
- *I. Rodzaj wniosku* – należy zaznaczyć 1 z 6 podanych pozycji:
    1. *Wydanie certyfikatu dla nowego użytkownika* – w przypadku, jeżeli Subskrybent ubiega się o wydanie certyfikatu po raz pierwszy lub w sytuacji, kiedy nastąpiła zmiana danych podmiotu takich jak: *nazwa podmiotu* czy *numer REGON podmiotu*.

       UWAGA! W sytuacji zmiany ww. danych użytkownik jest zobowiązany do niezwłocznego wystąpienia do MSW z wnioskiem o wydanie nowego certyfikatu, niezależnie od okresu ważności dotychczasowego certyfikatu.

    2. *Wydanie dodatkowego certyfikatu* – w przypadku, gdy użytkownik dysponuje już jednym bądź większą ilością certyfikatów i ubiega się o wydanie dodatkowych certyfikatów. Może to mieć miejsc w przypadku kiedy Subskrybent ma wiele placówek.
    3. *Odnowienie certyfikatu / Recertyfikacja* – w przypadku, gdy użytkownik ubiega się o przedłużenie ważności dotychczasowego certyfikatu, którego ważność dobiega końca lub w sytuacji kiedy certyfikat już wygasł, a wyżej wymienione dane podmiotu nie uległy zmianie.
    4. *Zawieszenie certyfikatu nr …* – w przypadkach określonych w polityce certyfikacji.
    5. *Uchylenie zawieszenia certyfikatu nr …*– w przypadkach określonych w polityce certyfikacji.
    6. *Unieważnienie certyfikatu nr …*– w przypadkach określonych w polityce certyfikacji.
- *Uzasadnienie wniosku* – należy wpisać przyczynę wnioskowania o wydanie certyfikatu, np. dla CBE może to być: *„Dostęp do usług CBE systemu CEPiK”.*
- *II. Pełna nazwa podmiotu* – zalecane jest sprawdzenie i przepisanie nazwy podmiotu bezpośrednio z zaświadczenia o przyznaniu numeru REGON, a nie np. z pieczęci podmiotu, ponieważ dane w zaświadczeniu i na pieczęci nie zawsze są identyczne.
- *III. Adres do korespondencji* – należy podać adres podmiotu, na który zostanie przesłany wygenerowany certyfikat (certyfikaty).
- *IV. REGON* – należy podać numer REGON wnioskującego. Numeru nie należy sztucznie uzupełniać.
- *V. Lokalizacja urządzenia* – należy podać adres lokalizacji, w której zlokalizowane jest urządzenie VPN (tylko w przypadku, gdy jest w innej lokalizacji, niż lokalizacja podmiotu).
- *VI. Dane osoby upoważnionej do reprezentowania Subskrybenta* – należy podać dane osoby upoważnionej w świetle przepisów prawa do reprezentowania wnioskującego podmiotu.
- *VII i VIII. Dane osoby upoważnionej do zarządzania nośnikami kluczy kryptograficznych* – należy podać dane administratora urządzenia VPN upoważnionego do dostępu do klucza

prywatnego certyfikatu lokalizacji. Zalecane jest w przypadku wnioskowania o więcej niż 1 certyfikat, aby były wskazane różne osoby.

- *IX. Dane osoby upoważnionej do odbioru nośników kluczy kryptograficznych lub dostarczenia zgłoszeń certyfikacyjnych i odbioru certyfikatów* – należy podać dane osoby upoważnionej do dostarczenia zgłoszeń certyfikacyjnych i odbioru certyfikatów (ważne w przypadku odbioru osobistego).
- *X. Proszę o wydanie certyfikatu na podstawie* – należy wybrać jedną z dwóch podanych opcji:
    - *wygenerowanej po stronie CC MSW pary kluczy kryptograficznych* – należy zaznaczyć, jeżeli wraz z wnioskiem **nie** jest przesłane żądanie certyfikacyjne CSR i klucze kryptograficzne mają zostać wygenerowane po stronie CC MSW (w formacie PKCS#12).
    - *zgłoszenia certyfikacyjnego w formacie PKCS#10, załączonego na nośniku/ach w liczbie ... (słownie)* – należy zaznaczyć w przypadku kiedy wysyłane jest wygenerowane po stronie Subskrybenta żądanie certyfikacyjne CSR.
- *XI. Proszę o wydanie ... certyfikatu/ów* – należy wpisać liczbę certyfikatów, o jaką wnioskuje Subskrybent. W przypadku, gdy Subskrybent będzie wnioskował o kilka certyfikatów dla kilku niezależnych lokalizacji, dla każdej należy wypełnić osobny wniosek.
- *Zakres zastosowania certyfikatu* – należy zaznaczyć pozycję „*Certyfikat Urządzenia Sieciowego VPN*”.
- *Miejscowość i data* – miejscowość, w której wypełniany jest wniosek oraz data wypełnienia wniosku w formacie DD-MM-RRRR (dzień-miesiąc-rok).
- *Pieczątka i podpis wnioskodawcy lub osoby upoważnionej do reprezentowania wnioskodawcy* – pieczęć oraz podpis osoby upoważnionej w świetle przepisów prawa do reprezentowania wnioskującego podmiotu.

W przypadku, gdy Subskrybent wygenerował żądanie certyfikacyjne, do wniosku należy dołączyć nośnik z żądaniem CSR.

UWAGA! Nośnik powinien zawierać samo żądanie CSR bez klucza prywatnego.

Wypełniony wniosek wraz z załączonym do niego nośnikiem należy przesłać do MSW na adres:

Ministerstwo Spraw Wewnętrznych
Departament Strategii i Analiz
Centrum Certyfikacji
ul. Pawińskiego 17/21
02-106 Warszawa

WAŻNE:

1. Zgodnie z obowiązującą polityką certyfikacji, wniosek certyfikacyjny powinien być przesłany do MSW listem poleconym za potwierdzeniem odbioru. Dopuszczalne jest osobiste dostarczenie wniosku wyłącznie po uprzednim kontakcie i uzgodnieniu tego faktu z pracownikami Centrum Certyfikacji MSW.
2. Czas realizacji wniosku przez MSW jest zgodny z zapisami Kodeksu Postępowania Administracyjnego oraz obowiązującej polityki certyfikacji. Datą rozpoczynającą upływ czasu realizacji wniosku jest data jego wpływu do MSW.

8.1.2 GENERACJA ŻĄDANIA CSR DLA CERTYFIKATU LOKALIZACJI

Dla połączeń VPN typu LAN-to-LAN żądanie powinien wygenerować administrator urządzenia sieciowego, zgodnie z procedurą i uwarunkowaniami technicznymi danego urządzenia.

Dla połączeń VPN typu remote access po stronie CC MSW generowany jest kompletny certyfikat z kluczami w formacie PKCS#12.

8.1.3 INSTALACJA CERTYFIKATU LOKALIZACJI

Po zakończeniu procesu certyfikacyjnego Subskrybent otrzyma z CC MSW certyfikat. Dalsze czynności zależą od rodzaju wysłanego wniosku (z żądaniem certyfikacyjnym lub bez).

8.1.3.1 Dla wniosku wysłanego bez żądania certyfikacyjnego

Jeżeli Subskrybent wnioskował o wydanie certyfikatu na podstawie wygenerowanej po stronie CC MSW pary kluczy kryptograficznych (wniosek był przesłany bez żądania certyfikacyjnego), w odpowiedzi otrzyma certyfikat w formacie PKCS#12, który jest gotowy do instalacji na urządzeniu służącym do nawiązywania połączeń VPN lub w programie Cisco VPN Client (lub alternatywnym).

8.1.3.2 Dla wniosku wysłanego wraz z żądaniem certyfikacyjnym

W przypadku kiedy Subskrybent wygenerował, żądanie certyfikacyjne, w odpowiedzi otrzyma dwa pliki w formacie PEM:

- swój podpisany certyfikat (np. vpn.crt),
- certyfikat urzędu (np. urzad.crt).

Do administratora urządzenia VPN należy dalsza poprawna konfiguracja urządzenia sieciowego.

8.1.3.3 Instalacja właściwego certyfikatu lokalizacji

W przypadku połączeń VPN typu LAN-to-LAN urządzenie sieciowe (np. router VPN) należy odpowiednio skonfigurować, aby do połączenia VPN wykorzystywało otrzymany certyfikat wraz z kluczem prywatnym.

W przypadku połączeń typu remote access certyfikat powinien zostać zainstalowany na stacji roboczej. Dla systemów Windows procedura przebiega następująco:

1. Kliknij prawym przyciskiem plik certyfikatu PKCS#12 i wybierz opcję Zainstaluj PFX.
2. Uruchomiony zostanie Kreator importu certyfikatu.
   Kliknij Dalej.
3. Pojawi się okno z polem tekstowym w którym wpisana jest ścieżka do pliku certyfikatu. Kliknij Dalej.
4. W kolejnym oknie wypełnij pole hasłem otrzymanym z CC MSW.
   Pozostaw odznaczone oba pola: „*Włącz silną ochronę klucza prywatnego.*” oraz „*Oznacz ten klucz jako eksportowalny.*”.
5. Kliknij Dalej.
6. Na następnym ekranie pozostaw zaznaczoną opcję „Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu” i kliknij Dalej.
7. Kliknij Zakończ.

Po wykonaniu powyższych kroków certyfikat jest gotowy do wykorzystanie w oprogramowaniu Cisco VPN Client. Alternatywnie import (instalację) certyfikatu można przeprowadzić w samym oprogramowaniu Cisco VPN Client.

8.2 CERTYFIKAT UŻYTKOWNIKA (SSL)

Certyfikat użytkownika służy do identyfikacji konkretnego użytkownika w obrębie jednej lokalizacji. Tylko dany użytkownik powinien mieć dostęp do klucza prywatnego jego certyfikatu użytkownika. Dlatego też w przypadku użytkowników wymagane jest, aby certyfikat i klucz prywatny użytkownika były przechowywane na karcie kryptograficznej. Certyfikat użytkownika, tak samo jak certyfikat lokalizacji, jest wydawany przez CC MSW.

8.2.1 WNIOSEK O WYDANIE CERTYFIKATU UŻYTKOWNIKA (SSL)

Subskrybent w celu nawiązania połączenia SSL oraz uwierzytelnienia w systemie CEPiK uzyskać certyfikat użytkownika wydany przez Centrum Certyfikacji MSW. Aby to zrobić musi wypełnić wniosek o wydanie certyfikatu w Polityce certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK, łączących się przez sieć publiczną.

Wniosek należy wypełnić zgodnie z poniższymi wytycznymi:

Wniosek należy wypełnić zgodnie z poniższymi wytycznymi:

- *Pieczęć Subskrybenta* (pieczęć podmiotu wnioskującego o wydanie certyfikatu);
- *Podstawa wnioskowania o certyfikat* – powołanie się na przepisy prawa, np. dla CBE będzie to *„art. 80k ust. 4 pkt. … ustawy Prawo o ruchu drogowym (Dz. U. …)*”.
- *Data wypełnienia wniosku* – należy podać datę, kiedy wniosek jest wypełniany przez Subskrybenta w formacie DD-MM-RRRR (dzień-miesiąc-rok);
- *I. Rodzaj wniosku* – należy zaznaczyć 1 z 6 podanych pozycji:
    1. *Wydanie certyfikatu dla nowego użytkownika* – w przypadku, jeżeli Subskrybent ubiega się o wydanie certyfikatu po raz pierwszy lub w sytuacji, kiedy nastąpiła zmiana danych podmiotu takich jak: *nazwa podmiotu* czy *numer REGON podmiotu*.

       UWAGA! W sytuacji zmiany ww. danych użytkownik jest zobowiązany do niezwłocznego wystąpienia do MSW z wnioskiem o wydanie nowego certyfikatu, niezależnie od okresu ważności dotychczasowego certyfikatu.

    2. *Wydanie dodatkowego certyfikatu* – w przypadku, gdy użytkownik dysponuje już jednym bądź większą ilością certyfikatów i ubiega się o wydanie dodatkowych certyfikatów. Może to mieć miejsc w przypadku kiedy Subskrybent ma wiele placówek.
    3. *Odnowienie certyfikatu / Recertyfikacja* – w przypadku, gdy użytkownik ubiega się o przedłużenie ważności dotychczasowego certyfikatu, którego ważność dobiega końca lub w sytuacji kiedy certyfikat już wygasł, a wyżej wymienione dane podmiotu nie uległy zmianie.
    4. *Zawieszenie certyfikatu nr …* – w przypadkach określonych w polityce certyfikacji.
    5. *Uchylenie zawieszenia certyfikatu nr …*– w przypadkach określonych w polityce certyfikacji.
    6. *Unieważnienie certyfikatu nr …*– w przypadkach określonych w polityce certyfikacji.
- *Uzasadnienie wniosku* – należy wpisać przyczynę wnioskowania o wydanie certyfikatu, np. dla CBE może to być: *„Dostęp do usług CBE systemu CEPiK”*.
- *II. Pełna nazwa podmiotu* – zalecane jest sprawdzenie i przepisanie nazwy podmiotu bezpośrednio z zaświadczenia o przyznaniu numeru REGON, a nie np. z pieczęci podmiotu, ponieważ dane w zaświadczeniu i na pieczęci nie zawsze są identyczne.
- *III. Adres do korespondencji* – należy podać adres podmiotu, na który zostanie przesłany wygenerowany certyfikat (certyfikaty).
- *IV. REGON* – należy podać numer REGON wnioskującego. Numeru nie należy sztucznie uzupełniać.

- *V. Lokalizacja urządzenia* – należy podać adres lokalizacji, w której zlokalizowane jest urządzenie VPN (tylko w przypadku, gdy jest w innej lokalizacji, niż lokalizacja podmiotu).
- *VII. Dane osoby upoważnionej do reprezentowania Subskrybenta* – należy podać dane osoby upoważnionej w świetle przepisów prawa do reprezentowania wnioskującego podmiotu.
- *VIII. Dane osoby upoważnionej do kontaktów z CPR, dostarczenia zgłoszeń certyfikacyjnych, odbioru certyfikatów, unieważniania, zawieszania lub uchylania zawieszenia certyfikatów* – należy podać dane osoby upoważnionej do zarządzania nośnikami kluczy kryptograficznych i kontaktów z Centrum Certyfikacji w sprawach związanych z certyfikatami. W przypadku chęci wskazania więcej niż 1 osoby, pola w sekcji należy powielić.
- *IX. Proszę o wydanie certyfikatu na podstawie* – należy wybrać jedną z podanych opcji:
    - *wygenerowanej po stronie CC MSW pary kluczy kryptograficznych* – należy zaznaczyć, jeżeli wraz z wnioskiem **nie** jest przesłane żądanie certyfikacyjne CSR i klucze kryptograficzne mają zostać wygenerowane po stronie CC MSW bezpośrednio na karcie kryptograficznej.

      WAŻNE: CC MSW ma możliwość wygenerowania kluczy bezpośrednio na kartach wyłącznie w przypadku kart ENCARD. W pozostałych przypadkach należy wybrać opcję drugą i dostarczyć CSR.
    - *zgłoszenia certyfikacyjnego w formacie PKCS#10, załączonego na nośniku/ach w liczbie ... (słownie)* – należy zaznaczyć w przypadku kiedy wysyłane jest wygenerowane po stronie Subskrybenta żądanie certyfikacyjne CSR.
- *X. Proszę o wydanie ... certyfikatu/ów* – należy wpisać liczbę certyfikatów, o jaką wnioskuje Subskrybent. W przypadku, gdy Subskrybent będzie wnioskował o kilka certyfikatów dla kilku niezależnych lokalizacji, dla każdej należy wypełnić osobny wniosek.
- *Zakres zastosowania certyfikatu* – należy zaznaczyć wszystkie zastosowania.
- *Miejscowość i data* – miejscowość, w której wypełniany jest wniosek oraz data wypełnienia wniosku w formacie DD-MM-RRRR (dzień-miesiąc-rok).
- *Pieczątka i podpis wnioskodawcy lub osoby upoważnionej do reprezentowania wnioskodawcy* – pieczęć oraz podpis osoby upoważnionej w świetle przepisów prawa do reprezentowania wnioskującego podmiotu.

Do wniosku należy dołączyć nośnik (w zależności od wyboru w pkt. IX wniosku):

- kartę kryptograficzną ENCARD wraz z kserokopią aktualnego PIN-u,

lub

- nośnik (płyta CD / płyta DVD / pamięć flash) z zapisanym na nim żądaniem certyfikacyjnym CSR.

Wypełniony wniosek wraz z załączonym do niego nośnikiem należy przesłać do MSW na adres:

Ministerstwo Spraw Wewnętrznych
Departament Strategii i Analiz
Centrum Certyfikacji
ul. Pawińskiego 17/21
02-106 Warszawa

WAŻNE:

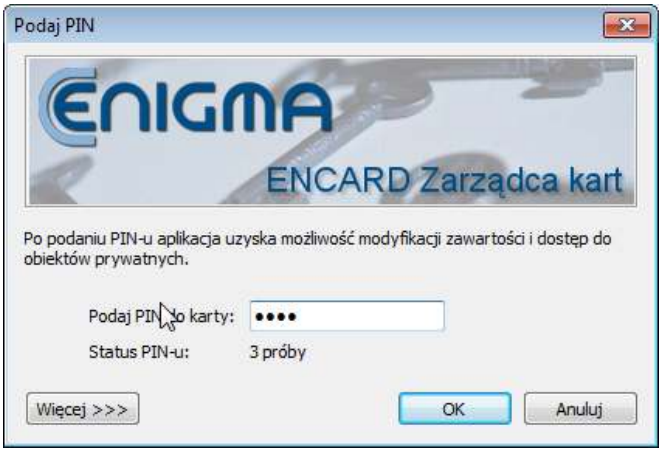
1. Zgodnie z obowiązującą polityką certyfikacji, wniosek certyfikacyjny powinien być przesłany do MSW listem poleconym za potwierdzeniem odbioru. Dopuszczalne jest osobiste dostarczenie wniosku wyłącznie po uprzednim kontakcie i uzgodnieniu tego faktu z pracownikami Centrum Certyfikacji MSW.
2. Czas realizacji wniosku przez MSW jest zgodny z zapisami Kodeksu Postępowania Administracyjnego oraz obowiązującej polityki certyfikacji. Datą rozpoczynającą upływ czasu realizacji wniosku jest data jego wpływu do MSW.

8.2.2 GENERACJA ŻĄDANIA CSR DLA CERTYFIKATU UŻYTKOWNIKA

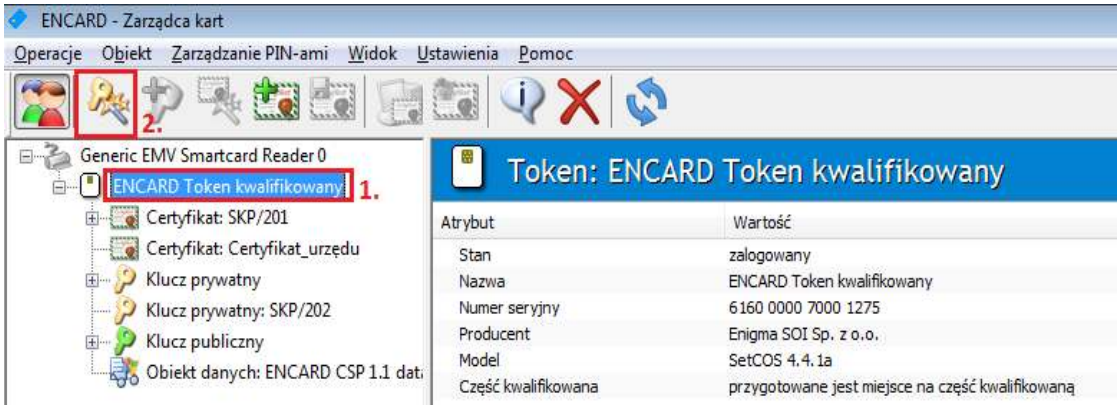
Żądanie certyfikacyjne dla karty kryptograficznej można wygenerować za pomocą oprogramowania dołączonego do karty. W tym rozdziale przykładowo opisany zostanie proces generowania żądania certyfikacyjnego dla kart ENCARD.

1. **Zaloguj się** klikając przycisk logowania.

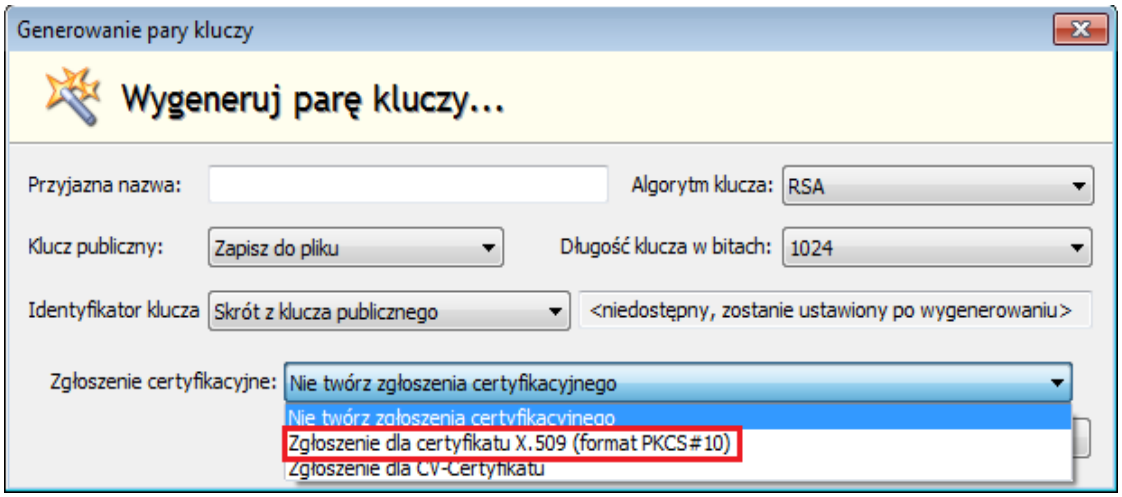
2. **Podaj kod pin** i naciśnij **OK**.



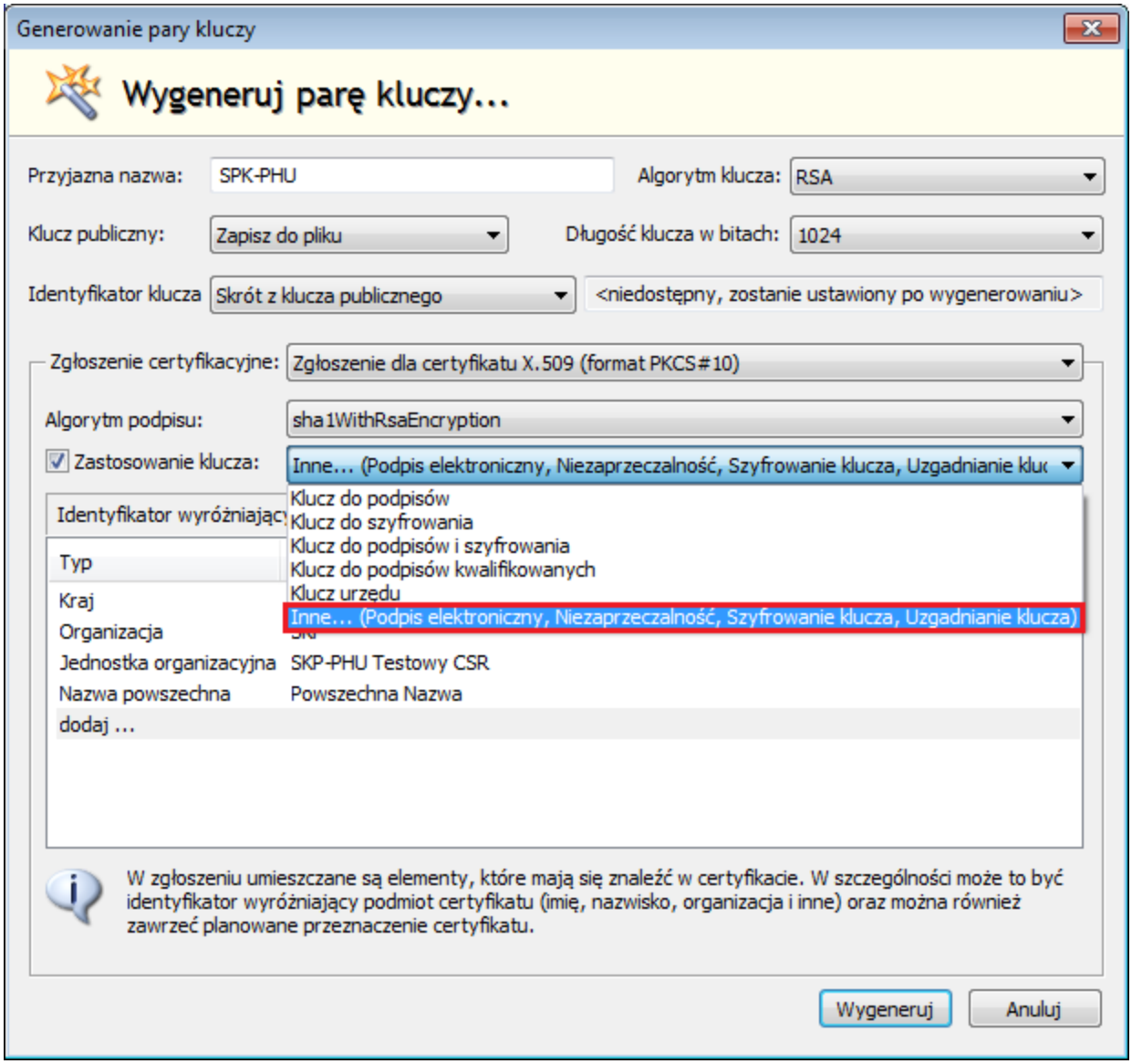
3. Wybierz kartę (1), a następnie wybierz ikonę generacji klucza (2).



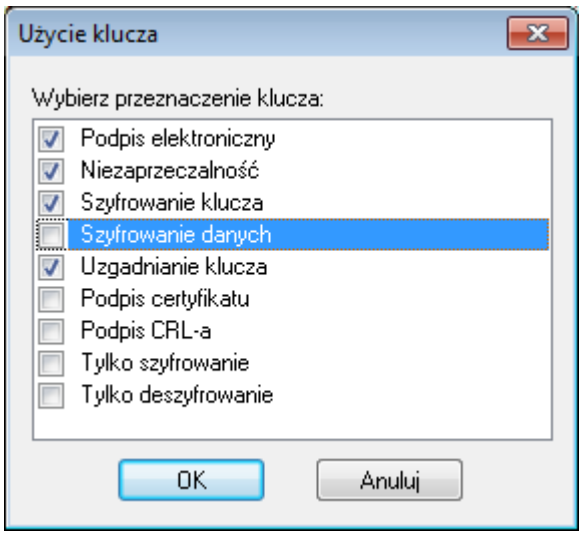
4. W nowo otwartym oknie "**Generowanie pary kluczy**" w polu "**Zgłoszenie certyfikacyjne**" wybierz "**Zgłoszenie dla certyfikatu X.509 (format PKCS#10)**".



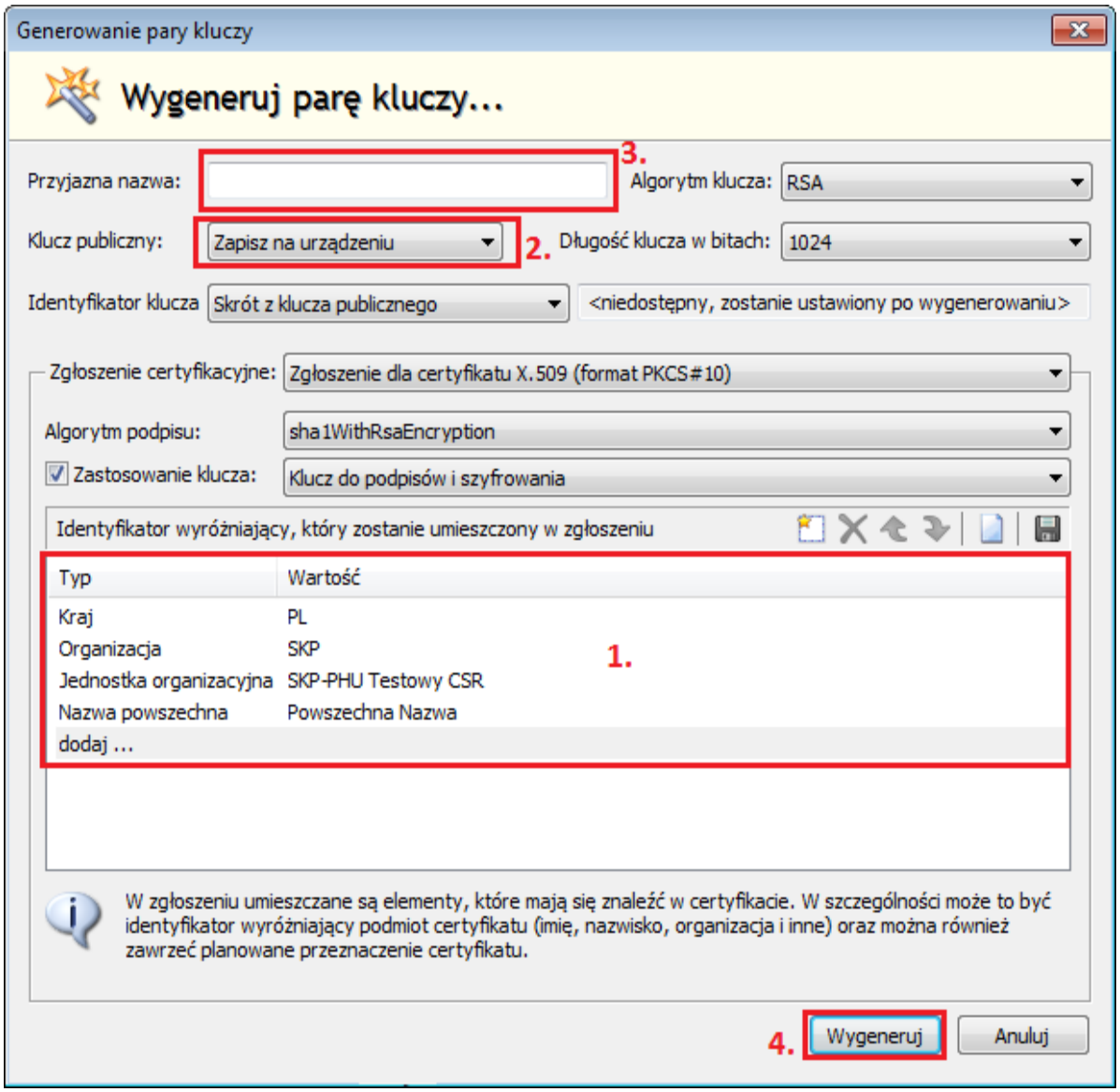
5. Upewnij się, że pole "**Zastosowanie klucza**" jest zaznaczone, następnie wybrać "**Inne...**".



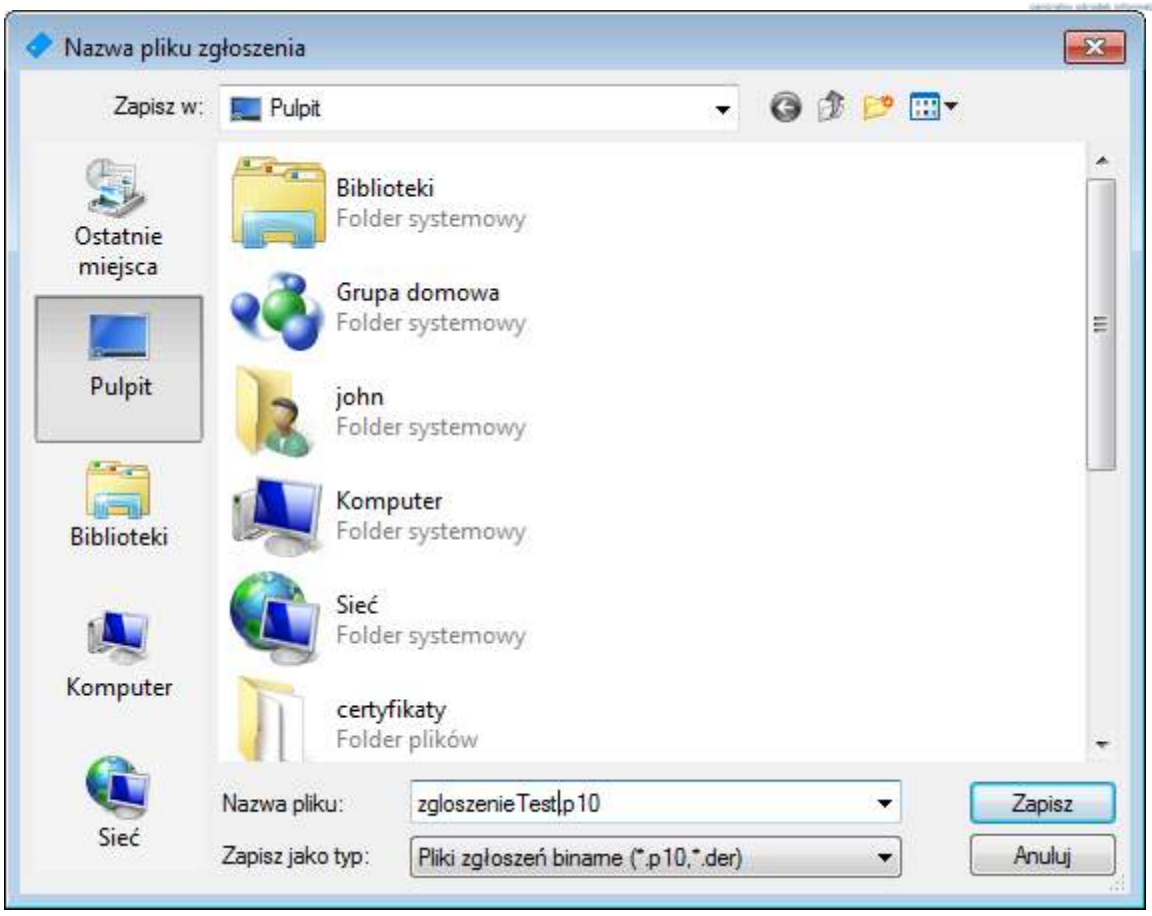
6. W nowo otwartym oknie zaznacz następujące pola: **podpis elektroniczny**, **niezaprzeczalność**, **szyfrowanie klucza**, **uzgadnianie klucza**. Zatwierdź wciskając "**OK**".



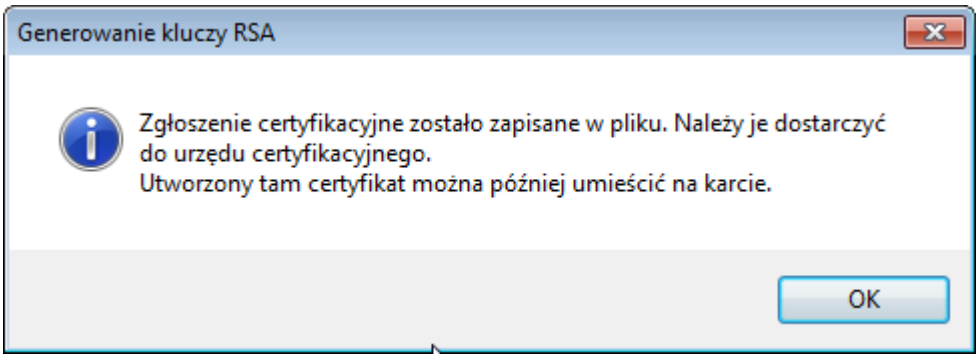
7. W polu "**Identyfikator wyróżniający, który zostanie umieszczony w zgłoszeniu**", klikając w napis "**dodaj ...**" należy dodać pola: **Kraj**, **Organizacja**, **Jednostka Organizacyjna**, **Nazwa Powszechna** oraz je uzupełnić zgodnie z następującymi regułami: w polu **Kraj** wpisz wartość **PL**, w polu **Organizacja** wpisz wartość **MSW**, w polu **Jednostka Organizacyjna** wpisz **nazwę Podmiotu Subskrybenta**, w polu **Nazwa Powszechna** wpisz **łatwo rozpoznawalną nazwę skróconą Podmiotu Subskrybenta** (np. SM Za Górą). (1)



8. Pole "**Klucz publiczny**" ustaw na "**Zapisz na urządzeniu**" (2). Pole "**Przyjazna nazwa**" służy do określenia nazwy przypisanej do certyfikatu (może być dowolna), pod tą nazwą znajdować się będzie certyfikat na karcie (3). Zatwierdzamy klikając "**Wygeneruj**" (4).
9. W nowym oknie (w zależności od systemu operacyjnego wygląd może się różnić) wybieramy miejsce gdzie zapiszemy żądanie podpisania certyfikatu (CSR).



10. Skuteczne wygenerowanie CSR zostanie potwierdzone odpowiednim komunikatem.



11. Tak wygenerowany plik należy wysłać wraz z wnioskiem certyfikacyjnym do Centrum Certyfikacji MSW.

8.2.3 INSTALACJA CERTYFIKATU UŻYTKOWNIKA

Po zakończeniu procesu certyfikacyjnego Subskrybent otrzyma z CC MSW certyfikat. Dalsze czynności zależą od rodzaju wysłanego wniosku (z żądaniem certyfikacyjnym lub bez).

8.2.3.1 Dla wniosku wysłanego wraz z kartą kryptograficzną

Jeżeli Subskrybent wnioskował o wydanie certyfikatu na podstawie wygenerowanej po stronie CC MSW pary kluczy kryptograficznych (wniosek był przesłany bez żądania certyfikacyjnego wraz z kartą kryptograficzną ENCARD), w odpowiedzi otrzyma kartę z zainstalowanym certyfikatem

użytkownika, która jest gotowa do użycia. PIN do karty wysyłany jest, ze względów bezpieczeństwa, osobną przesyłką.

8.2.3.2 Dla wniosku wysłanego wraz z żądaniem certyfikacyjnym CSR

W przypadku kiedy Subskrybent wygenerował żądanie certyfikacyjne CSR i wysłał wniosek bez karty kryptograficznej, wymagane jest zaimportowanie otrzymanego z CC MSW certyfikatu na kartę kryptograficzną, wykorzystując oprogramowanie odpowiednie dla posiadanego typu karty kryptograficznej. Po wczytaniu certyfikatu karta jest gotowa do użycia.

9 ROZPOCZĘCIE PRACY Z APLIKACJĄ WWW

9.1 URUCHOMIENIE POŁĄCZENIA VPN

Pierwszym etapem rozpoczęcia pracy z aplikacją WWW modułu CBE jest poprawne zestawienie połączenia VPN.

9.1.1 POŁĄCZENIA TYPU LAN-TO-LAN

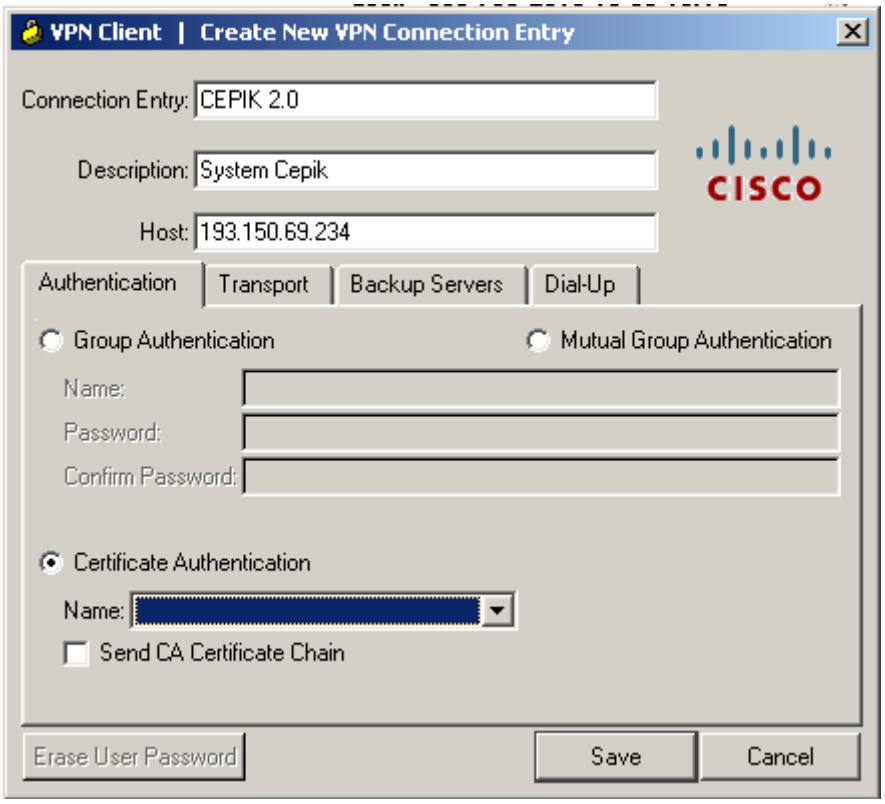
W przypadku połączeń VPN typu LAN-to-LAN urządzenie sieciowe (np. router) należy odpowiednio skonfigurować, aby do połączenia VPN wykorzystywało otrzymany certyfikat wraz z kluczem prywatnym. W celu weryfikacji, czy podmiot posiada zestawione połączenie VPN L2L należy skontaktować się z lokalnym administratorem sieci lub osobą odpowiedzialną w podmiocie za lokalne administrowanie systemem.

9.1.2 POŁĄCZENIA TYPU REMOTE ACCESS

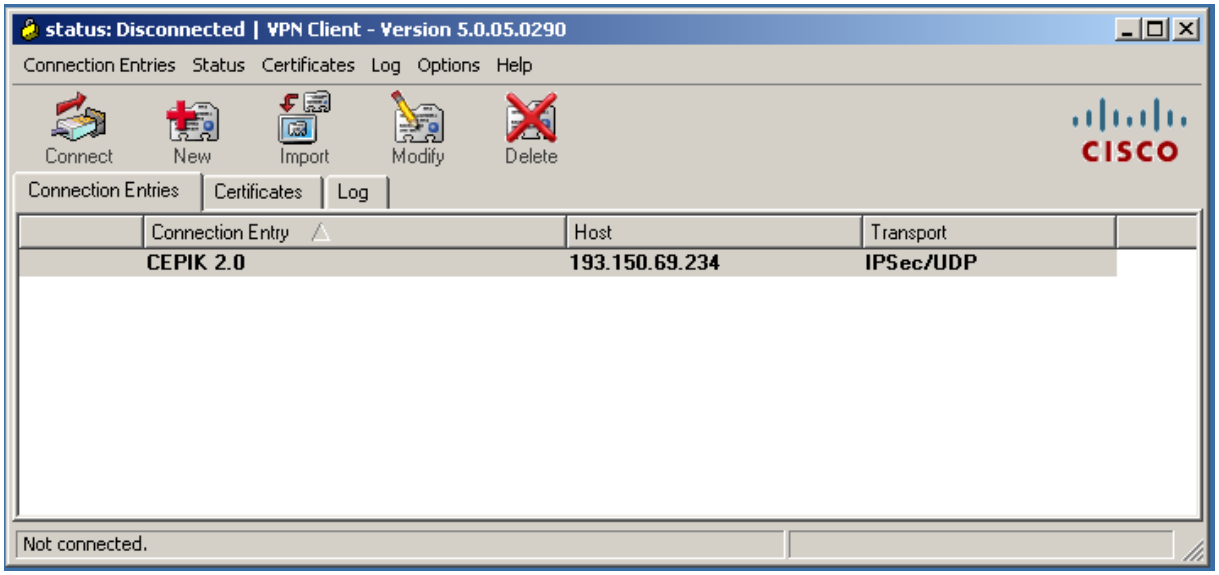
Kanał VPN typu remote access ma na celu umożliwienie zdalnej pracy z aplikacją jednej stacji roboczej z wykorzystaniem transmisji poprzez szyfrowany kanał VPN. Jest to połączenie oparte o architekturę klient – serwer i do zestawienia kanału szyfrowanego niezbędne jest oprogramowanie klienckie, które musi zostać zainstalowane na stacji roboczej. Do poprawnego skonfigurowania zdalnego dostępu należy pobrać i zainstalować oprogramowanie Cisco VPN Client lub skorzystać z innego alternatywnego rozwiązania, wskazanego w niniejszym dokumencie.

Po poprawnej instalacji Cisco VPN Client w systemie operacyjnym, uruchamiamy program i wybieramy z menu opcję **Connection Entries → New** i definiujemy parametry:

- Host: 193.150.69.234
- Wskazujemy posiadany przez nas certyfikat jako parametr uwierzytelniania → zakładka **Authentication**, sekcja **Certificate Authentication**, z listy należy **wybrać właściwy certyfikat**.
  WARUNEK → certyfikat został uprzednio poprawnie zainstalowany w systemie operacyjnym (8.1.3).

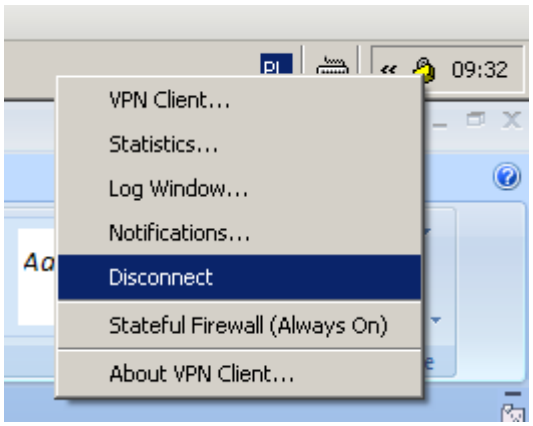


Pozostałe parametry pozostawiamy bez zmian i zapisujemy konfigurację. W celu zestawienia połączenia należy wybrać zdefiniowany uprzednio profil i **dwukrotnie kliknąć lub** wybrać opcję **Connect** z paska narzędziowego.



Po poprawnym połączeniu się w „trayu” zobaczymy ikonę klienta VPN w postaci zamkniętej kłódki.

W celu zakończenia połączenia VPN, na ikonie kłódki klikamy prawym przyciskiem i wybieramy opcje **Disconnect**.



9.2 NAWIĄZANIE SSL I UWIERZYTELNIENIE

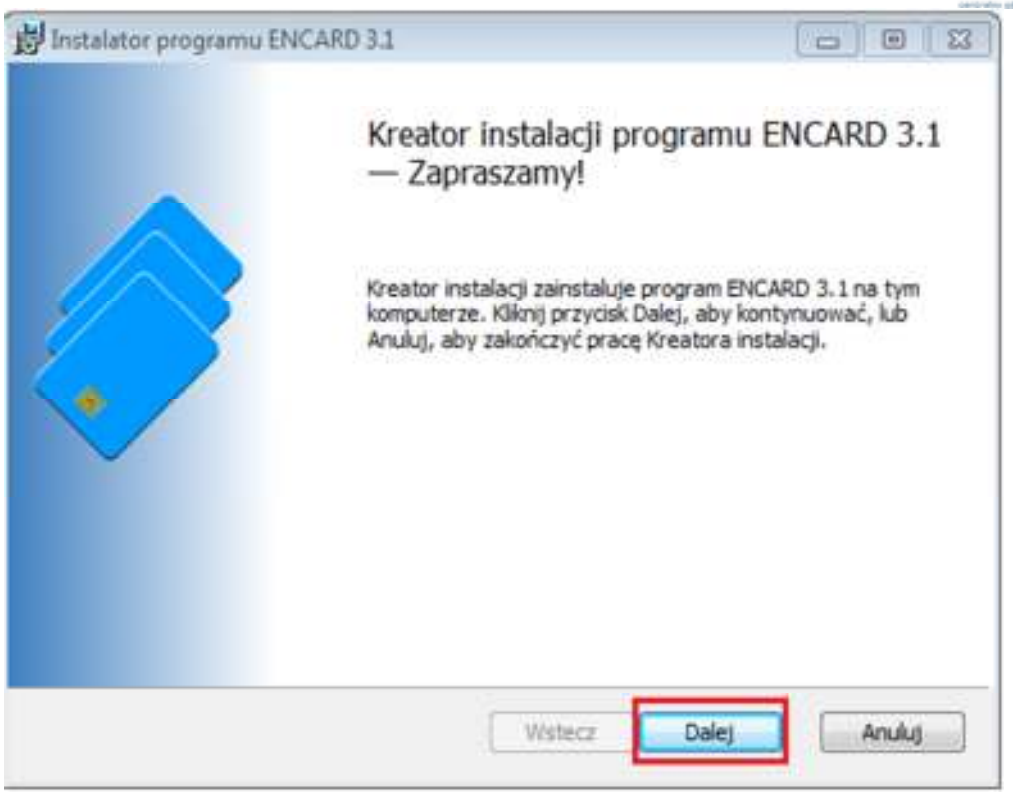
Komunikacja SSL jest niezbędna, aby zapewnić bezpieczeństwo połączenia oraz uwierzytelnienie użytkownika.

9.2.1 UŻYTKOWNICY APLIKACJI WWW

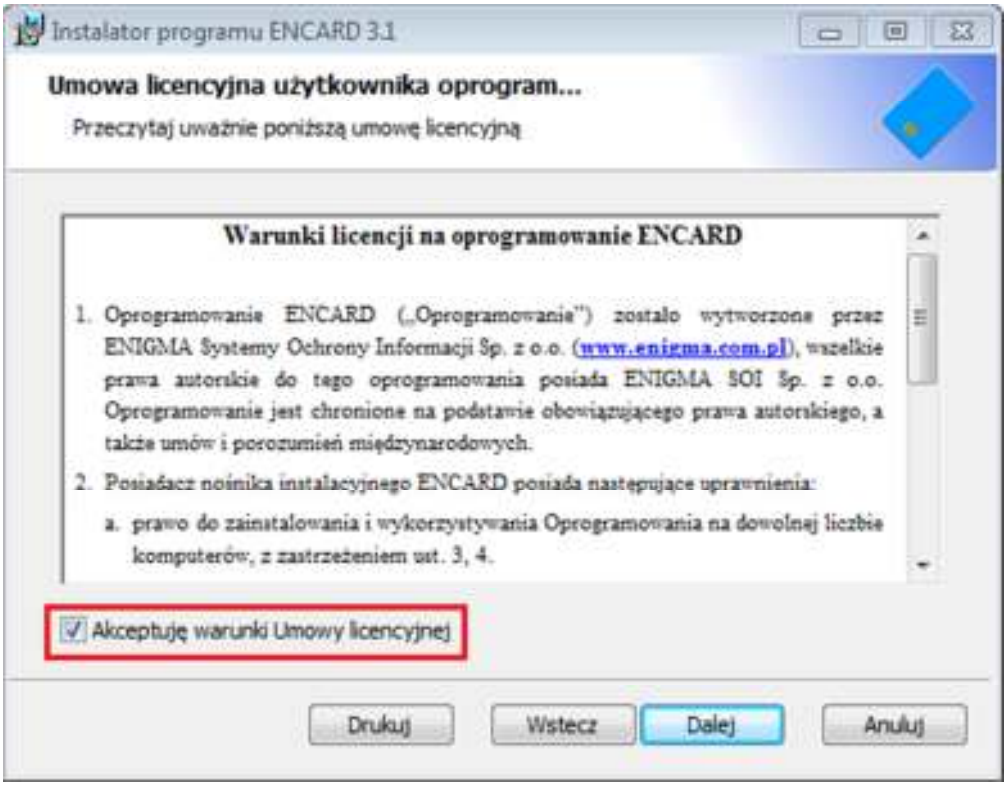
Użytkownicy indywidualni nawiązują połączenie SSL przy użyciu certyfikatów użytkownika umieszczonych na kartach kryptograficznych. Aby to umożliwić, na stacji komputerowej musi być zainstalowane niezbędne oprogramowania oraz podłączony czytnik mikroprocesorowych kart (wewnętrzny lub zewnętrzny).

9.2.2 INSTALACJA – OPROGRAMOWANIE KARTY ENCARD

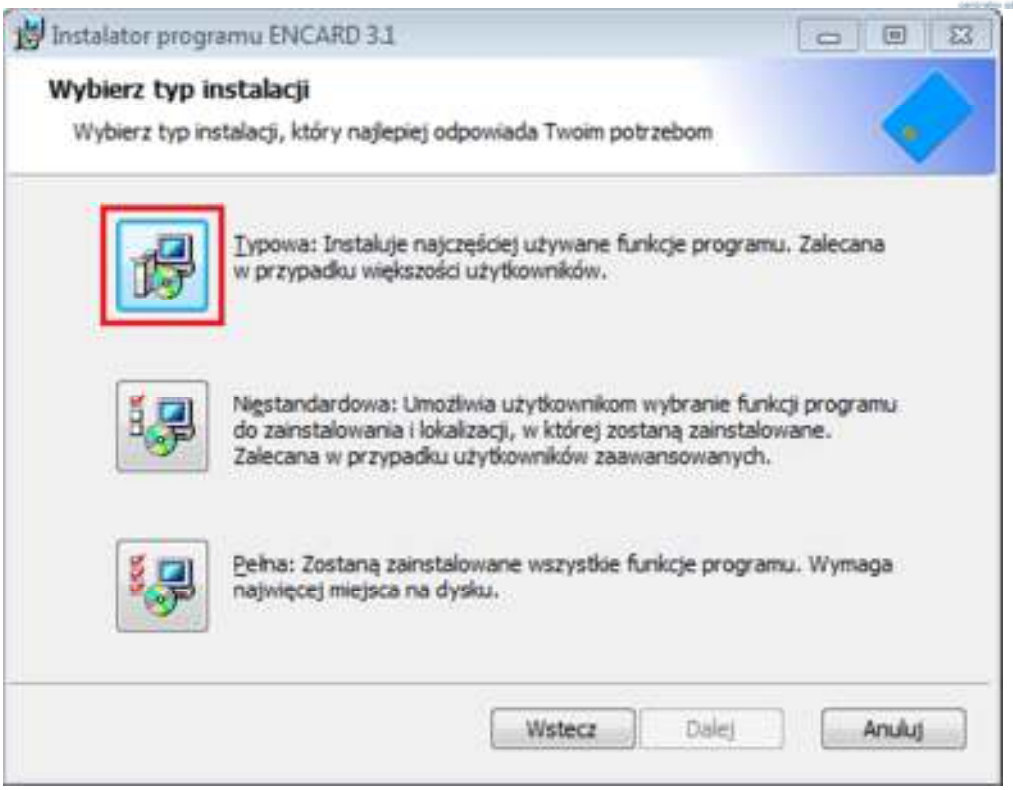
1. **Zainstaluj** oprogramowanie Encard (dołączone do karty lub zawarte w pakiecie instalacyjnym).
   WAŻNE: Zaleca się korzystanie z wersji oprogramowania 3.1 lub wyższej.
2. Po uruchomieniu instalatora kliknij przycisk **Dalej**.



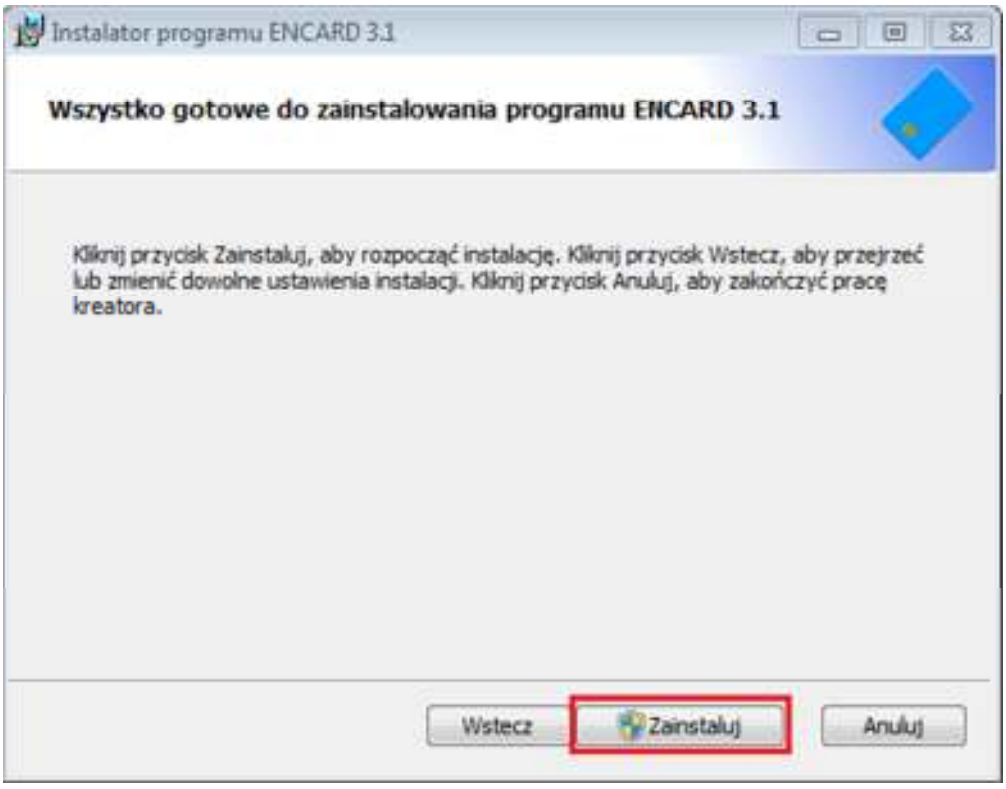
3. **Zapoznaj** się z warunkami umowy licencyjnej i je **zaakceptuj** klikając w miejsce oznaczone na obrazku czerwonym kwadratem, a następnie kliknij przycisk **Dalej**.



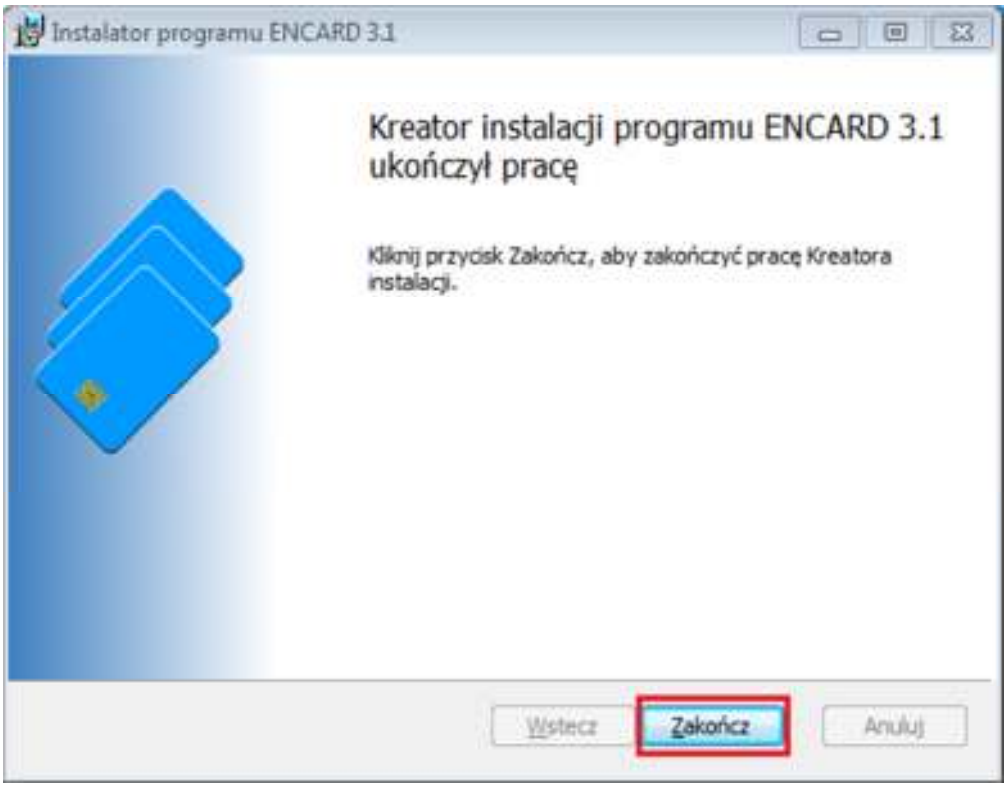
4. Wybierz **Typową instalację**, a następnie kliknij przycisk **Dalej**.



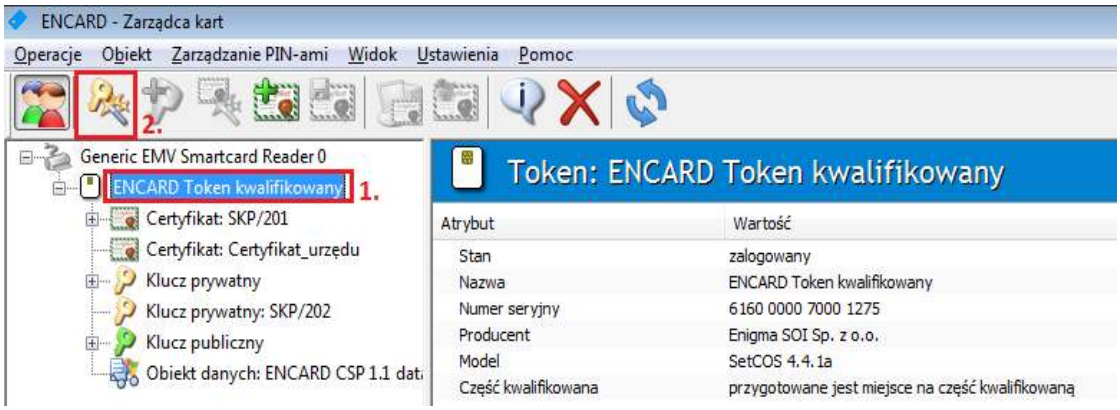
5. Kliknij przycisk **Zainstaluj**. W zależności od systemu operacyjnego i uprawnień konta użytkownika, na którym przeprowadzany jest proces instalacji, może być konieczne potwierdzenie operacji hasłem administratora.



6. Aby zakończyć instalację, kliknij przycisk **Zakończ**.

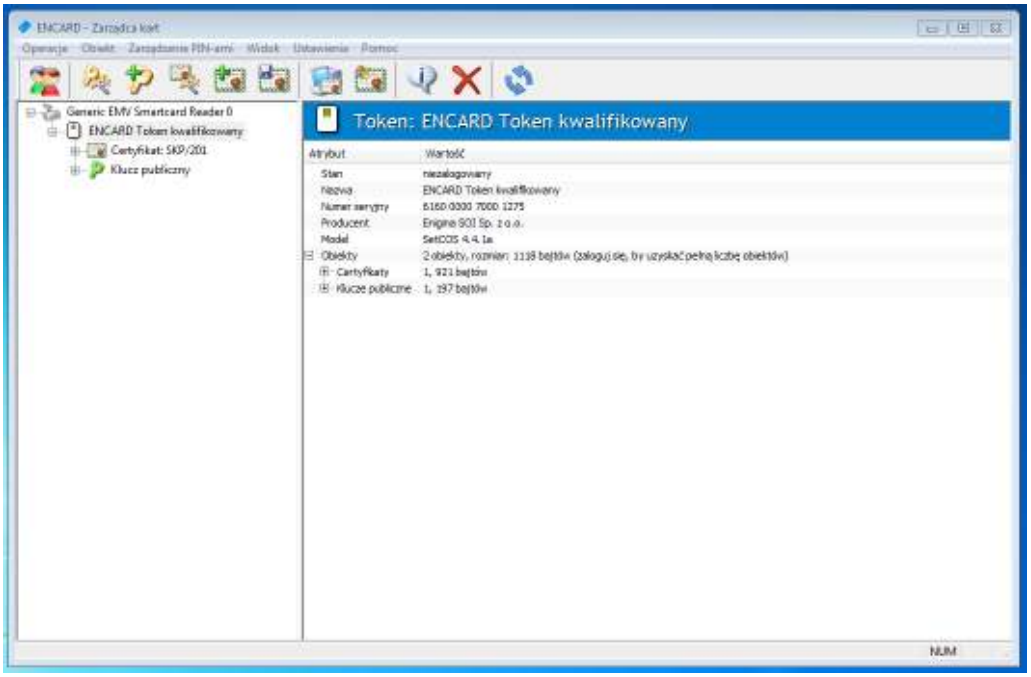


7. Umieścić kartę w czytniku kart.
8. Uruchom aplikację ENCARD – Zarządca Kart.
9. Zweryfikuj, czy karta jest widoczna na liście (1).

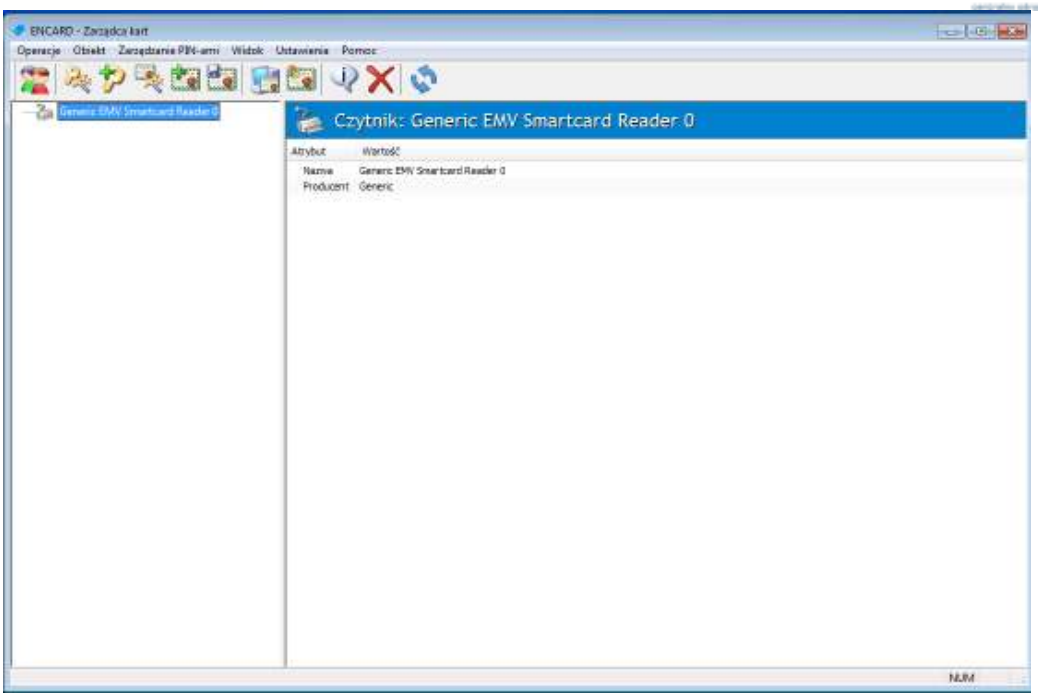


9.2.3 INSTRUKCJA URUCHOMIENIA SSL PRZY UŻYCIU PRZEGLĄDAREK INTERNET EXPLORER W WERSJI 8 LUB WYŻSZYCH ORAZ CHROME DLA KART ENCARD

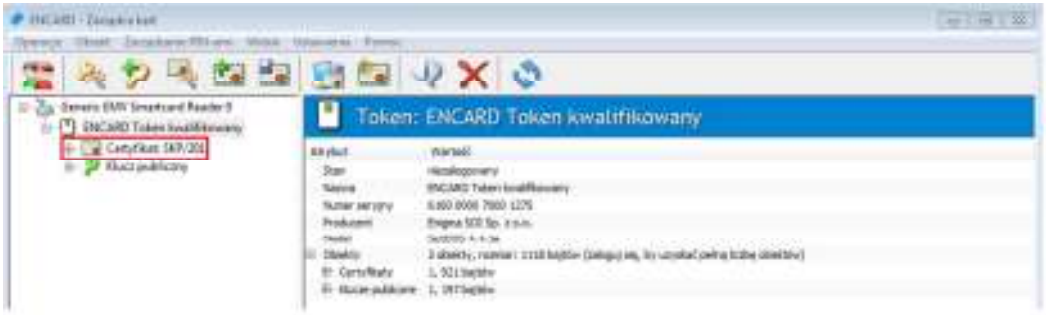
1. Zakłada się, że oprogramowanie ENCARD (9.2.2) oraz przeglądarka Internet Explorer lub Google Chrome są zainstalowane.
2. **Uruchom** program ENCARD – Zarządca Kart.
3. W oknie po lewej stronie powinna być widoczna Karta ENCARD z certyfikatem.



4. W przypadku braku widoczności karty w programie, należy sprawdzić czy karta jest poprawnie włożona do czytnika, a czytnik podłączony do komputera. W przypadku, gdy karta jest poprawnie włożona, czytnik podłączony do komputera, a nie jest widoczna w programie, należy się skontaktować z lokalnym administratorem systemu w celu rozwiązania problemu. Brak Karty zobrazowano na poniższym obrazku.

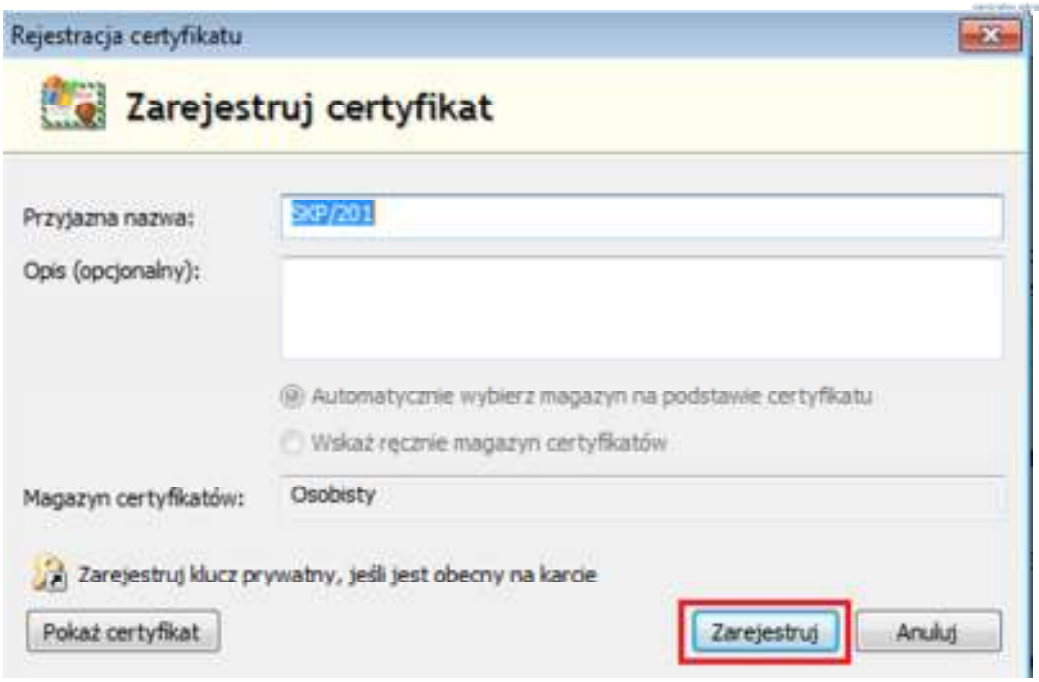


5. **Dodaj** certyfikat do bazy certyfikatów systemu Windows, **wybierając** z lewej strony **certyfikat użytkownika**.



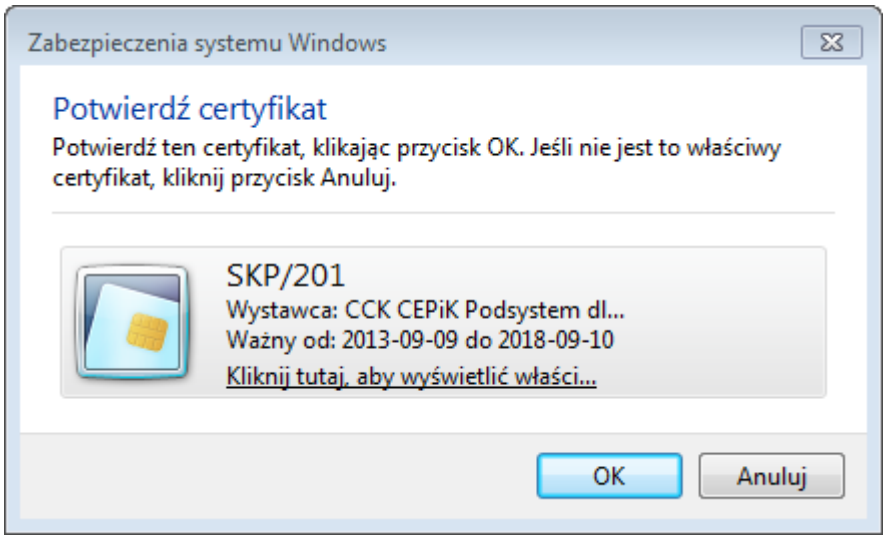
i **klikając** przycisk z logo Microsoft Windows:

6. **Wpisz** *Przyjazną nazwę* (np. CEPiK SM Za Górą).

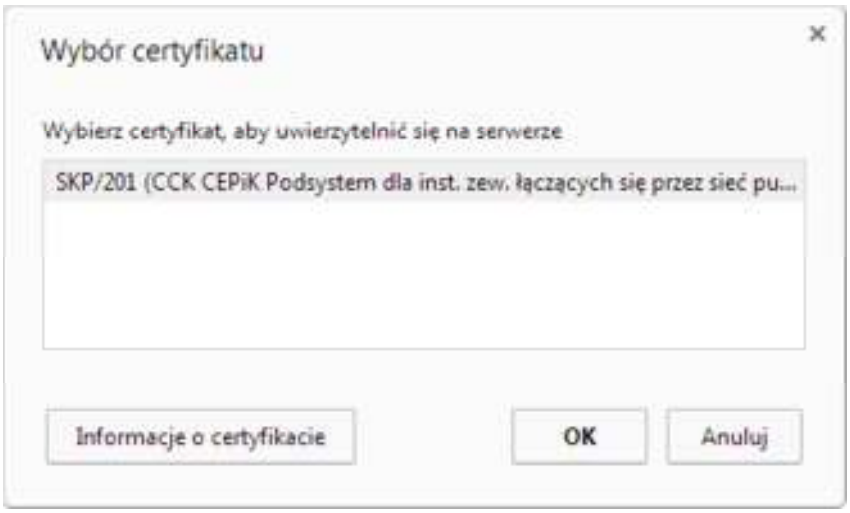


7. **Zatwierdź** operację przyciskiem **Zarejestruj**.
8. **Zamknij** program.
9. Upewnij się, że **karta znajduje się w czytniku**.
10. **Uruchom** przeglądarkę internetową Internet Explorer lub Chrome.
11. Dla przeglądarki Internet Explorer **wyłącz** w ustawieniach „widok zgodności” (przy włączonym widoku zgodności aplikacja może działać niepoprawnie).
12. **Wywołaj** adres aplikacji WWW CBE (**https://cbe.cepik/cbe-web/**).
13. **Wybierz** właściwy certyfikat i potwierdź klikając **OK**.

    Wybór certyfikatu w przypadku Internet Explorera:



    Wybór certyfikatu w przypadku Google Chrome:

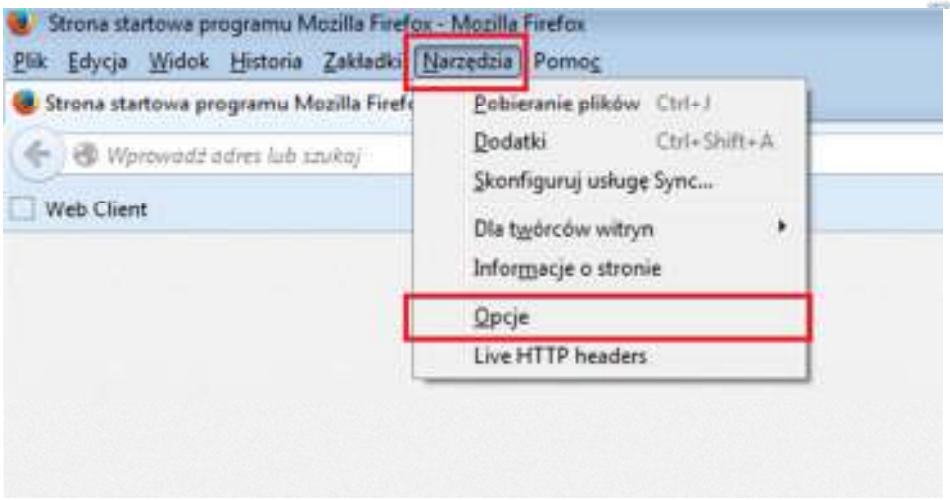


14. **Podaj PIN** do karty. Po wpisaniu PIN-u potwierdź klikając **OK**.

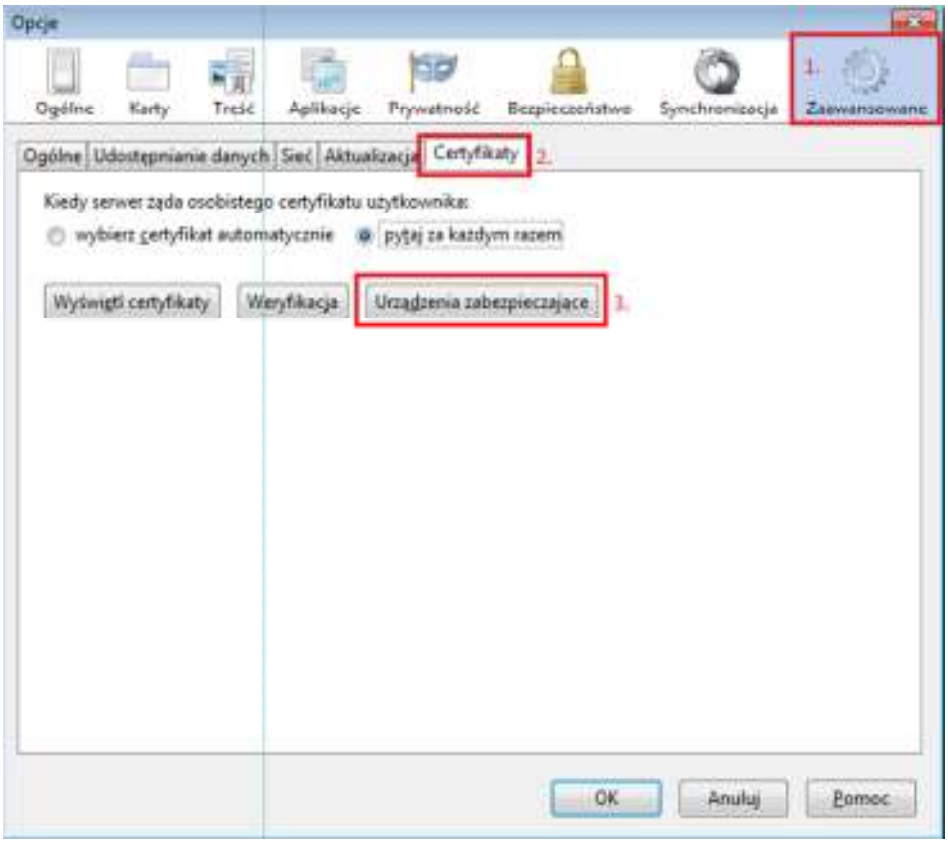
15. W tym momencie będziemy mieli aktywne, bezpiecznie połączenie SSL oraz zostaniemy uwierzytelnieni w aplikacji WWW CBE.

9.2.4 INSTRUKCJA URUCHOMIENIA SSL PRZY UŻYCIU PRZEGLĄDARKI MOZILLA FIREFOX

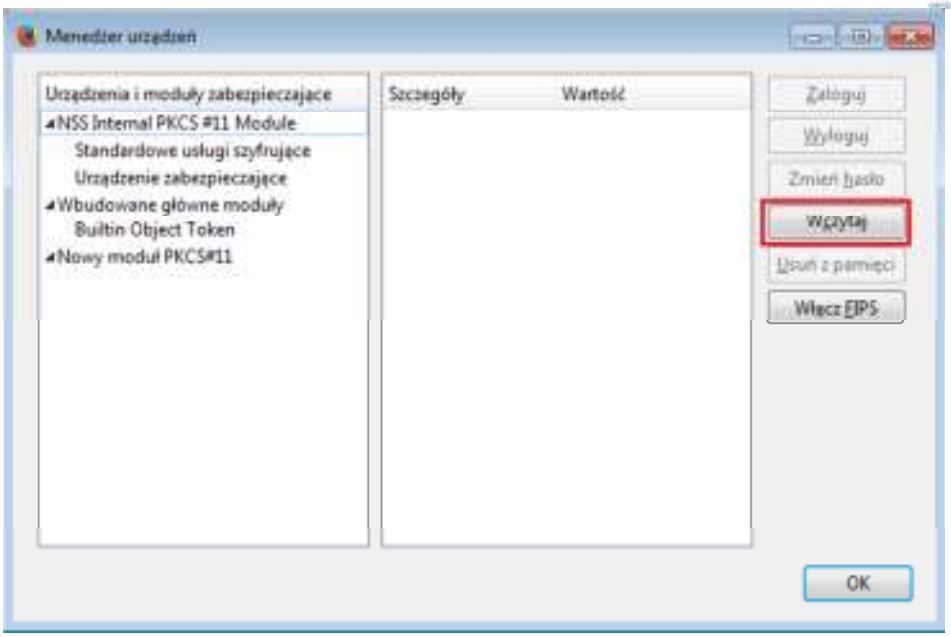
1. Zakłada się, że oprogramowanie ENCARD (9.2.2) oraz przeglądarka Mozilla Firefox są zainstalowane.
2. **Uruchom** przeglądarkę Mozilla Firefox.
3. Wejdź do ustawień wybierając **Narzędzia → Opcje**



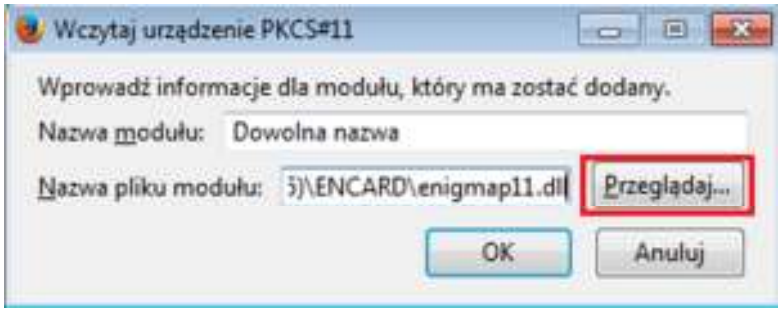
4. Wybierz z menu kartę **Zaawansowane**, następnie zakładkę **Certyfikaty** i kliknij przycisk **Urządzenia zabezpieczające**.



5. W nowo otwartym oknie kliknij przycisk **Wczytaj**.

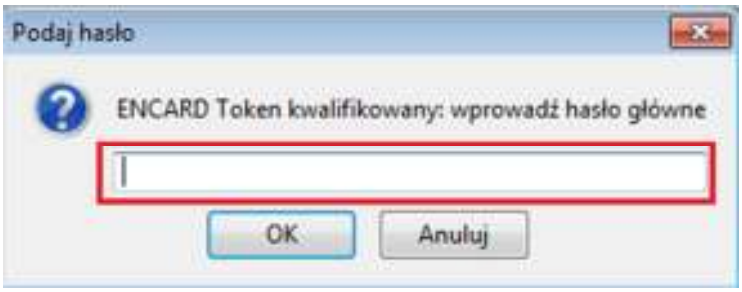


6. W nowym oknie kliknij **Przeglądaj** i z folderu, w którym zainstalowano oprogramowanie ENCARD (domyślnie C:\Program Files (x86)\ENCARD dla systemu 64-bitowego lub C:\Program Files\ENCARD dla systemu 32-bitowego) lub katalogu systemowego C:\Windows\system32\ **wybierz** plik **enigmap11.dll**.

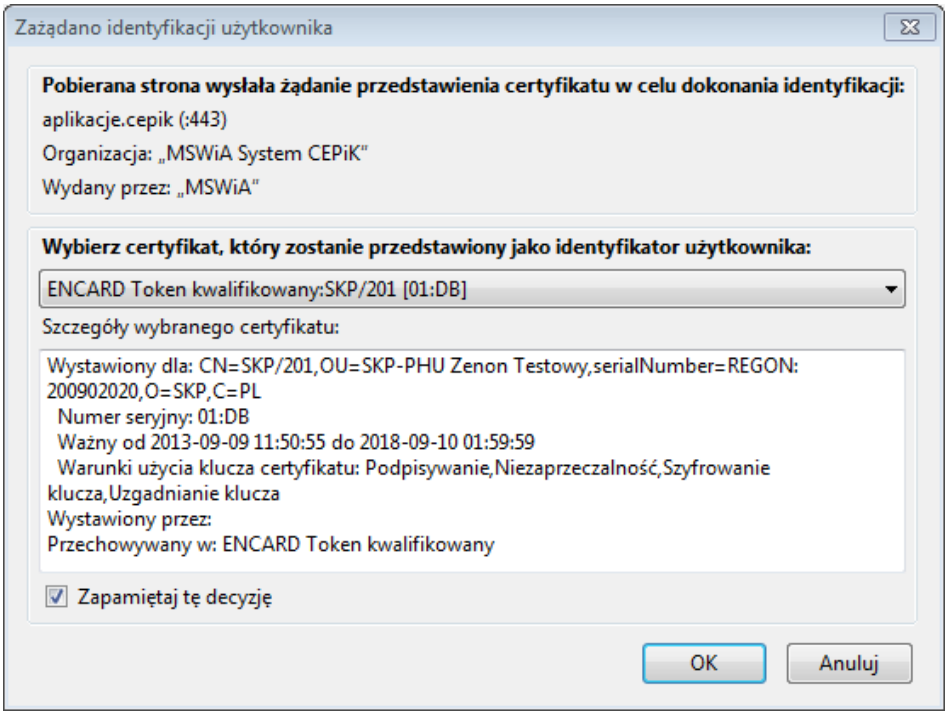


Nazwa modułu jest dowolna, natomiast nie może się powtarzać z występującymi już nazwami modułów.

7. **Potwierdź** przyciskiem **OK**. Przeglądarka potwierdzi zainstalowanie modułu.
8. **Zamknij** okna ustawień Mozilla Firefox klikając w oknach **OK**.
9. Upewnij się, że **karta znajduje się w czytniku**.
10. **Wywołaj** adres aplikacji WWW CBE (**https://cbe.cepik/cbe-web/**).
11. **Wprowadź PIN** do karty w pole zaznaczone czerwonym kwadratem i **potwierdź** klikając **OK**.



12. **Wybierz** właściwy certyfikat i **potwierdź** klikając **OK**.



13. **Potwierdź** klikając **OK**.
14. W tym momencie będziemy mieli aktywne, bezpiecznie połączenie SSL oraz zostaniemy uwierzytelnieni w aplikacji WWW CBE.

WAŻNE: W sytuacji, gdy przeglądarka zażąda dodania wyjątku bezpieczeństwa dla witryny, należy dodać wyjątek zgodnie z informacjami wyświetlanymi na ekranie (dodaj wyjątek bezpieczeństwa → potwierdź dodanie wyjątku bezpieczeństwa).

10 SYSTEMY ZEWNĘTRZNE – WEB SERVICE CBE (API)

Użytkownicy korzystający z systemów zewnętrznych (własnych rozwiązań komunikujących się z modułem CBE poprzez Web Service) otrzymują jeden certyfikat użytkownika dla całego systemu w postaci pliku. Następnie system zewnętrzny musi zostać odpowiednio skonfigurowany, tak aby wykorzystywać ten certyfikat wraz z kluczem prywatnym do nawiązania połączenia SSL przy pomocy mechanizmu client authentication.

INFORMACJA: Podmioty chcące dostosować własne systemy teleinformatyczne do komunikacji z modułem CBE systemu CEPiK (dostosowanie do komunikacji z Web Service) prosimy o kontakt z Wydziałem Utrzymania i Rozwoju Ewidencji Departamentu Ewidencji Państwowych Ministerstwa Spraw Wewnętrznych – tel. (22) 60-28-208 – w celu uzyskania szczegółowej informacji oraz otrzymania niezbędnej dokumentacji technicznej.

10.1 WEB SERVICE CBE (API)

Moduł CBE udostępnia dwa Web Serwisy pozwalające na uzyskiwanie danych z system Eucaris – synchroniczny i asynchroniczny. Pierwszy służy do uzyskiwania informacji o pojedynczym pojeździe, natomiast przy użyciu drugiego użytkownik może odpytać o dane wielu pojazdów jednocześnie (zgodnie z zawartym poniżej opisem).

Należy pamiętać, aby wartości pól senderName i senderOrganisationName dla komunikatów wysyłanych podanymi Web Serwisami były zgodne z, odpowiednio, sekcjami CN i OU pobranymi z certyfikatu. Przykładowo dla certyfikatu: CN=SKP 201, OU=SKP-PHU Zenon Testowy, O=SKP, C=PL wartość pola senderName musi być równa SKP 201, natomiast wartość pola senderOrganisationName musi być równa SKP-PHU Zenon Testowy. W przypadku, gdy pola nie będą zgodne z wartościami w certyfikatach, użytkownik nie zostanie poprawnie zautoryzowany.

10.1.1 SYNCHRONICZNY WEB SERWIS

Web Serwis synchroniczny znajduje się pod poniższym adresem:

https://cbe.cepik/cbe-ws/GenericService

Plik WSDL znajduje się pod adresem:

https://cbe.cepik/cbe-ws/GenericService?WSDL

Dla użytkownika wystawiona jest jedna metoda – GetInfo. Komunikacja poprzez ten kanał polega na wysłaniu komunikatu zgodnego z określonym schematem XSD pod wymieniony wcześniej adres. W odpowiedzi użytkownik otrzyma synchronicznie komunikat GetInfoResponse, zgodny ze specyfikacją lub informację o błędzie, np. w przypadku niepowodzenia autoryzacji użytkownika.

10.1.2 ASYNCHRONICZNY WEB SERWIS

Web Serwis asynchroniczny znajduje się pod adresem:

https://cbe-ws.cepik/cbe-ws/GenericAsyncService

Plik WSDL znajduje się pod adresem:

https://cbe-ws.cepik/cbe-ws/GenericAsyncService?WSDL

Wystawione są tutaj cztery metody, przy czym wykorzystywane są jedynie trzy: Send, Index oraz Receive. Komunikaty wysyłane muszą być zgodne z określonym schematem XSD.

Komunikacja następuje zgodnie z poniższym algorytmem:

- Przy pomocy metody Send użytkownik składa żądanie przygotowania danych o pojazdach.
- W odpowiedzi na zapytanie metodą Index użytkownik sprawdza, czy zapytanie posiada odpowiadającą mu odpowiedź.
- Jeśli zapytanie posiada odpowiadającą mu odpowiedź, użytkownik może, korzystając z metody Receive, odebrać informacje.

10.2 API MessageOfTheDay

Moduł MessageOfTheDay udostępnia Web Serwis, który umożliwia pobranie wiadomości dnia.

Web Serwis znajduje się pod adresem:

https://motd-ws.cepik/motd-ws/WiadomoscDnia

Plik WSDL znajduje się pod adresem:

https://motd-ws.cepik/motd-ws/WiadomoscDnia?WSDL

Dla użytkownika wystawiona jest metoda pobierzWiadomosci. W zapytaniu należy umieścić nazwę modułu, dla którego użytkownik chce otrzymać aktualne wiadomości dnia. Dla modułu CBE wymagana nazwa to EUCARIS_CBE. Przykładowy komunikat, którym użytkownik może odpytać o wiadomości dnia dla modułu CBE został przedstawiony poniżej:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:motd="http://motd.cepik2.msw.gov.pl/">
        <soapenv:Header/>
                <soapenv:Body>
                        <motd:pobierzWiadomosciReq>
                                <motd:modul>EUCARIS_CBE</motd:modul>
                        </motd:pobierzWiadomosciReq>
                </soapenv:Body>
</soapenv:Envelope>
```

Przykładowy komunikat zwrotny z listą aktywnych wiadomości dnia został przedstawiony poniżej:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <soap:Body>
                <pobierzWiadomosciRes xmlns="http://motd.cepik2.msw.gov.pl/"
                xmlns:ns2="http://motd.cepik2.msw.gov.pl/wiadomosc">
                        <listaWiadomosci>
                                <ns2:Wiadomosc>
                                <ns2:id>1</ns2:id>
                                <ns2:modul>EUCARIS_CBE</ns2:modul>
                                <ns2:dataOd>2013-09-26T12:34:43.944+02:00</ns2:dataOd>
                                <ns2:dataDo>2013-10-05T12:34:54.452+02:00</ns2:dataDo>
                                <ns2:tresc>Nastąpi planowana przerwa w dostepie do systemu
                                Eucaris w dniach 04-05.10.2013</ns2:tresc>
```

```
                                    </ns2:Wiadomosc>
                                    <ns2:Wiadomosc>
                                    <ns2:id>2</ns2:id>
                                    <ns2:modul>EUCARIS_CBE</ns2:modul>
                                    <ns2:dataOd>2013-09-30T12:42:13.499+02:00</ns2:dataOd>
                                    <ns2:dataDo>2013-10-06T12:42:35.561+02:00</ns2:dataDo>
                                    <ns2:tresc>Dokumentacja do modułu CBE będzie dostępna od
                                    06.10.2013</ns2:tresc>
                                    </ns2:Wiadomosc>
                                </listaWiadomosci>
                            </pobierzWiadomosciRes>
                        </soap:Body>
</soap:Envelope>
```

11 WSPARCIE UŻYTKOWNIKA

11.1 Instrukcja zgłaszania incydentów

Zgłoszenie incydentu może nastąpić za pośrednictwem następujących kanałów komunikacyjnych:

1. Telefonicznie na ogólnodostępny nr telefonu centrali serwisowej:
   Tel. **42 253-54-54**, Fax.: **42 292-07-81**.
2. Pocztą elektroniczną na adres: **service_desk_portal@coi.gov.pl**
3. Za pośrednictwem dedykowanego portalu zgłoszeniowego, dostępnego pod adresem:
   https://www.cepik.gov.pl/helpdesk

Instrukcja użytkownika portalu zgłoszeniowego dostępna jest pod adresem: **http://www.cepik.gov.pl/portal/plik/instrukcja.pdf?id=231** oraz po zalogowaniu do portalu zgłoszeniowego w nagłówku strony.

Centralny punkt zgłoszeń serwisowych (Service Desk) dla użytkowników systemu CEPIK dostępny jest w trybie 7/24 tj. przez 7 dni w tygodniu, 24 godziny na dobę.

UWAGA: Incydent może zostać zgłoszony dla usługi systemowej w okresie jej dostępności. Działanie poszczególnych usług poza ich czasami dostępności nie jest gwarantowane. Dostępność poszczególnych usług jest wskazana w dokumentacji dotyczącej danego modułu.

WAŻNE: Użytkownik jest zobligowany do przekazania wszystkich informacji określonych poniżej. Incydent należy zgłaszać niezwłocznie po jego wystąpieniu. W przypadku problemów z określeniem elementu (np. aplikacji) przez użytkownika, operator Service Desk zobligowany jest do pomocy w ustaleniu.

Informacje poniżej dotyczą zgłaszania incydentów jedynie w kanale telefonicznym lub mailowym.

11.1.1 INFORMACJE WYMAGANE DO ZGŁOSZENIA INCYDENTU

Prawidłowe zgłoszenie incydentu zawiera:

1. dane użytkownika/instytucji, dane osoby zgłaszającej lub odpowiedzialnej za pracę z daną aplikacją oraz numer telefonu umożliwiający szybki kontakt z taką osobą,
2. w miarę dokładny opis problemu, tj. w jakiej sytuacji wystąpił, w którym momencie pracy z aplikacją, jakie są objawy, etc.,
3. wersja aplikacji,
4. dane środowiska pracy, tzn. parametry stacji roboczej (jaki czytnik kart i karta kryptograficzna (producent), wersja systemu operacyjnego (dla Windows wskazanie SP), wersja przeglądarki, wersja środowiska JAVA,
5. data ostatniego poprawnego działania aplikacji, kiedy złożono ostatni wniosek czy przesyłano dane, czy uzyskano odpowiedź/potwierdzenie z SI CEPiK,
6. ewentualnie dołączony zrzut ekranu (screen) obrazujący występujące problemy (należy zamazywać dane osobowe).

Informacje te umożliwią szybsze zdiagnozowanie i rozwiązanie problemu, dlatego im więcej informacji dotyczących problemu zostanie podanych, tym lepiej.

11.2 PORTAL ZGŁOSZENIOWY

Portal zgłoszeniowy posiada następujące funkcjonalności:

- komunikowanie się z helpdeskiem za pomocą forum przypisanego do każdego z incydentów,
- możliwość przeglądania incydentów zgłoszonych przez użytkownika,
- raportowanie aktywności na portalu,
- przeglądanie ogłoszeń związanych z portalem.

11.3 ZGŁOSZENIE REKLAMACJI

Reklamacja może zostać zgłoszona w sytuacji, gdy poprzednio zgłoszony incydent nie został prawidłowo rozwiązany lub przedłuża się czas obsługi.

W przypadku pojawienia się zastrzeżeń do obsługi Service Desk uprzejmie proszę o przekazanie takiej informacji na adres mailowy: **adm.cepik@msw.gov.pl**