



## Informacje dla użytkowników korzystających z Obsługi Zapytań Zewnętrznych (OZZ) oraz dla Stacji Kontroli Pojazdów (SKP), łączących się z SI CEPiK przez sieć publiczną (Internet), dotyczące wnioskowania o wydanie / zawieszenie / uchylenie zawieszenia / unieważnienie certyfikatu

Subskrybent (użytkownik), składający do MC wniosek o wydanie / zawieszenie / uchylenie zawieszenia / unieważnienie certyfikatu powinien odpowiednio:

1) Pobrać właściwy dla użytkowników korzystających z OZZ oraz dla SKP formularz wniosku. Wzór formularza dostępny jest na portalu internetowym [www.cepik.gov.pl](http://www.cepik.gov.pl)

2) Wypełnić wniosek zgodnie z poniższymi wytycznymi co do poszczególnych pozycji:

- **Pieczęć Subskrybenta** → pieczęć podmiotu wnioskującego o wydanie certyfikatu.
- **Podstawa wnioskowania o certyfikat** → należy wpisać podstawę prawną umożliwiającą wydanie certyfikatu, tj.:
  - **w przypadku OZZ:** podstawę wnioskowania stanowi zawsze pozytywna decyzja Ministra Cyfryzacji (bądź dawniej: Ministra Spraw Wewnętrznych i Administracji lub Ministra Spraw Wewnętrznych), zezwalająca na udostępnianie danych ewidencyjnych z SI CEPiK z wykorzystaniem urządzeń teletransmisji (Subskrybent powinien wpisać numer decyzji oraz datę jej wydania);
  - **w przypadku SKP:**
    - a) *Rozporządzenie Ministra SWiA w sprawie centralnej ewidencji pojazdów;*
    - b) *Wpis wnioskodawcy do rejestru przedsiębiorców prowadzących SKP;*
    - c) *art. 80ba ust. 1 pkt 6 ustawy Prawo o ruchu drogowym.*
- **Data wypełnienia wniosku** → należy podać datę wypełnienia wniosku przez Subskrybenta w formacie DD-MM-RRRR (dzień-miesiąc-rok).
- **Rodzaj wniosku** → należy zaznaczyć 1 z 6 podanych pozycji:
  - **Wydanie certyfikatu dla nowego użytkownika** → należy wybrać, jeżeli Subskrybent ubiega się o wydanie certyfikatu po raz pierwszy lub w sytuacji, kiedy nastąpiła zmiana danych podmiotu takich jak:



- **w przypadku OZZ:**

- a) nazwa podmiotu,
- b) numer REGON podmiotu;

- **w przypadku SKP:**

- a) nazwa podmiotu,
- b) numer REGON podmiotu,
- c) identyfikator (numer) SKP, np. ABC/001/P.

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

- o ***Wydanie dodatkowego certyfikatu*** → należy wybrać w sytuacji, kiedy użytkownik dysponując już jednym bądź większą ilością certyfikatów, ubiega się o wydanie dodatkowych certyfikatów (ubieganie się o każdy dodatkowy certyfikat wiąże się z zaopatrzeniem się przez użytkownika w dodatkową kartę kryptograficzną).

**UWAGA:** Dodatkowy certyfikat jest wystawiany na identyczne dane w stosunku do certyfikatu/-ów wystawionego/-ych użytkownikowi wcześniej, dlatego też w przypadku zmiany danych podmiotu (patrz poprzedni podpunkt), nawet jeżeli użytkownik wnioskuje o dodatkowe certyfikaty, należy zaznaczyć pozycję: *Wydanie certyfikatu dla nowego użytkownika* i zaktualizować także posiadane już certyfikaty z nieaktualnymi danymi, ponieważ wydanie dodatkowego certyfikatu na inne dane niż w posiadanym już wcześniej certyfikacie uniemożliwiłoby wykorzystanie certyfikatu wcześniejszego;

- o ***Odnowienie certyfikatu / recertyfikacja*** → należy wybrać w sytuacji, 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. Certyfikaty są wystawiane każdorazowo na okres 2 lat. Każdy użytkownik ma możliwość sprawdzenia ważności swojego certyfikatu dzięki odczytowi zawartości posiadanej karty kryptograficznej przy pomocy oprogramowania otrzymanego od producenta zestawu kryptograficznego. W celu zachowania ciągłości dostępu do SI CEPiK użytkownik, zgodnie z zapisami polityki certyfikacji, powinien wystąpić o wymianę certyfikatu w okresie ważności certyfikatu dotychczasowego, z odpowiednim wyprzedzeniem czasowym, nie mniejszym niż 14 dni i nie większym niż 28 dni.

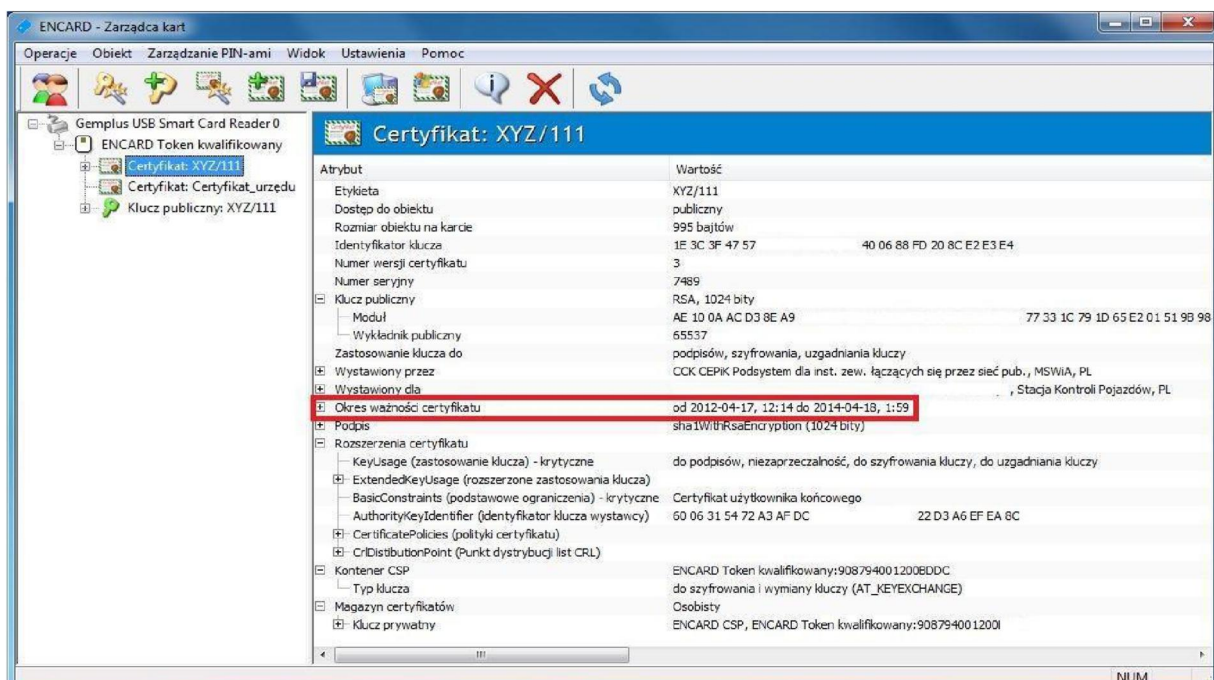
**UWAGA:** Zachowanie ciągłości w dostępie do SI CEPiK jest możliwe:



- dla użytkowników wszystkich typów kart – po przesłaniu do MC pliku z żądaniem certyfikacyjnym, przy zachowaniu odpowiedniego wyprzedzenia czasowego przed upływem terminu ważności certyfikatu oraz pod warunkiem zachowania na karcie dotychczasowego certyfikatu do momentu otrzymania z MC nowego;
- dla użytkowników kart typu ENCARD, którzy decydują się na przesłanie wraz z wnioskiem karty kryptograficznej, aby uzyskać certyfikat bezpośrednio na karcie – tylko jeżeli posiadają oni więcej niż 1 certyfikat. Wówczas użytkownik odnawiając certyfikat na jednej karcie, ma możliwość posługiwania się dodatkowym/-ymi certyfikatem/-ami – o ile są one ważne. Dlatego też zalecane jest, aby w przypadku posiadania więcej niż jednego certyfikatu, miały one różne okresy ważności. Informacje na temat możliwości uzyskania przez użytkowników dodatkowych certyfikatów zostały zamieszczone powyżej (podpunkt pt.: Wydanie dodatkowego certyfikatu).

#### **Sprawdzanie ważności certyfikatu – przykład dla kart ENCARD:**

- 1) umieszczenie karty kryptograficznej w czytniku;
- 2) uruchomienie programu ENCARD: Menu Start → Programy → ENCARD → ENCARD Zarządca Kart;
- 3) po lewej stronie okna aplikacji wybór pozycji Certyfikat z nazwą podmiotu;
- 4) po prawej stronie aplikacji pokazuje się zawartość certyfikatu → ważność certyfikatu jest wyświetlana pod pozycją „Okres ważności certyfikatu” (zaznaczona na czerwono na poniższym obrazku).





- **Zawieszenie certyfikatu numer:** ..... → należy zaznaczyć w przypadku, gdy użytkownik wnioskuje o zawieszenie aktywnego certyfikatu oraz wpisać jego numer;
- **Uchylenie zawieszenia certyfikatu numer:** ..... → należy zaznaczyć w przypadku, gdy użytkownik wnioskuje o uchylenie zawieszonoego przez MC certyfikatu oraz wpisać jego numer;
- **Unieważnienie certyfikatu numer:** ..... → należy zaznaczyć w przypadku, gdy użytkownik wnioskuje o unieważnienie certyfikatu oraz wpisać jego numer;

**UWAGA:** Zasady dotyczące zawieszenia / uchylenia zawieszenia / unieważnienia certyfikatu są opisane w polityce certyfikacji (rozdziały 3.4 oraz 4.9).

- **Uzasadnienie wniosku** → należy wpisać przyczynę wnioskowania o wydanie / zawieszenie / uchylenie zawieszenia / unieważnienie certyfikatu, np.:
  - upływ terminu ważności certyfikatu,
  - zagubienie, kradzież bądź uszkodzenie posiadanej dotychczas karty kryptograficznej,
  - zmiana danych wnioskodawcy (odpowiednio: nazwy podmiotu / numeru REGON / identyfikatora SKP),
  - ewentualnie inne informacje ułatwiające odpowiednią weryfikację wniosku po stronie MC.
- **Pełna nazwa podmiotu** → zalecane jest wpisanie nazwy podmiotu z zaświadczenia o przyznaniu numeru REGON.
- **Adres do korespondencji** → należy podać adres podmiotu, na który MC prześle wygenerowany certyfikat.
- **REGON** → należy podać numer REGON wnioskującego podmiotu, zaczynając od pierwszej kratki. Podobnie jak w przypadku nazwy podmiotu, zalecane jest przepisanie numeru z zaświadczenia o przyznaniu numeru REGON. Numer REGON może składać się z ciągu 9 lub 14 cyfr (14-cyfrowe numery REGON są nadawane podmiotom posiadającym wyodrębnione jednostki lokalne – wówczas pierwsze 9 cyfr pokrywa się z numerem REGON jednostki głównej, a 5-cyfrowe rozszerzenia identyfikują poszczególne jednostki lokalne podmiotu – w takiej sytuacji każda jednostka lokalna dysponuje odrębnym zaświadczeniem o przyznaniu numeru REGON).



**UWAGA:** W przypadku, gdy REGON jest 9-cyfrowy, pozostałych krótkich nie należy wypełniać zerami.

- **Identyfikator SKP** → kod rozpoznawczy SKP, obowiązujący na podstawie wydanego przez właściwy organ zaświadczenia potwierdzającego wpis do rejestru przedsiębiorców prowadzących SKP, np. **ABC/001/P**.

**UWAGA:** Pozycja ta nie dotyczy OZZ.

- **Dane osoby upoważnionej do reprezentowania Podmiotu** → należy podać dane osoby upoważnionej w świetle przepisów prawa do reprezentowania wnioskującego podmiotu.
- **Dane osoby upoważnionej do kontaktów z CPR, dostarczenia zgłoszeń certyfikacyjnych, odbioru certyfikatów, unieważniania, zawieszania lub uchylania zawieszenia certyfikatów** → należy uzupełnić zgodnie z opisami pól zamieszczonymi na formularzu.

**UWAGA:** Zmiana wyżej wymienionych osób nie wiąże się z wnioskowaniem o wydanie nowego certyfikatu, ponieważ certyfikaty nie są wystawiane na osobę, ale na podmiot.

- **Proszę o wydanie certyfikatu na podstawie** → należy zaznaczyć 1 z 2 podanych pozycji:
  - **wygenerowanej po stronie MC pary kluczy kryptograficznych** → należy zaznaczyć tylko w przypadku posiadania karty kryptograficznej typu ENCARD, jeżeli Subskrybent decyduje się na wygenerowanie certyfikatu przez MC bezpośrednio na karcie kryptograficznej (w takim przypadku należy dołączyć do wniosku o wydanie certyfikatu kartę kryptograficzną wraz z aktualnym PIN kodem).

**UWAGA:** Na czas przekazania karty kryptograficznej do MC użytkownik nie ma możliwości podłączenia do SI CEPiK (z wyjątkiem sytuacji, gdy posiada dodatkowy/-e ważny/-e certyfikat/-y). W związku z tym, w przypadku SKP, po otrzymaniu karty z certyfikatem, należy niezwłocznie uzupełnić wykonane, ale nieprzesłane do CEP badania techniczne;

- **zgłoszenia certyfikacyjnego w formacie PKCS#10, załączonego na nośniku/ach w liczbie .....** (**słownie**) ..... → należy zaznaczyć i wypełnić w przypadku posiadania karty kryptograficznej jakiegokolwiek innego typu niż ENCARD. Wówczas Subskrybent wnioskujący o certyfikat jest zobowiązany do samodzielnego wygenerowania pliku z żądaniem certyfikacyjnym, który prześle do MC na nośniku (płyta CD / płyta DVD / pamięć flash). W takiej sytuacji, po przeprowadzeniu certyfikacji, Subskrybent otrzyma wygenerowany przez MC certyfikat również zapisany na nośniku. Wiąże się to



z koniecznością dokonania przez Subskrybenta samodzielnego zaimportowania otrzymanego certyfikatu na posiadaną przez niego kartę kryptograficzną, z której wygenerował on wcześniej żądanie certyfikacyjne. Opisana procedura umożliwia dostęp do SI CEPiK w czasie przeprowadzania procedury certyfikacji w MC, o ile tylko wniosek o wydanie certyfikatu zostanie przesłany do MC z odpowiednim wyprzedzeniem czasowym przed momentem wygaśnięcia dotychczas aktywnego certyfikatu.

**UWAGA:** W przypadku kart typu ENCARD również istnieje możliwość przesłania do MC wygenerowanego samodzielnie pliku z żądaniem certyfikacyjnym, zamiast karty kryptograficznej z PIN kodem (Subskrybent decyduje, który sposób jest dla niego bardziej odpowiedni) → wówczas należy zaznaczyć pozycję: *Proszę o wydanie certyfikatu na podstawie zgłoszenia certyfikacyjnego w formacie PKCS#10 [...]*, a procedura wygląda tak, jak opisano w powyższym punkcie dotyczącym przesyłania pliku z żądaniem certyfikacyjnym.

- **Proszę o wydanie ..... szt. certyfikatu/ów** → należy wpisać liczbę certyfikatów, o jaką wnioskuje Subskrybent. W przypadku korzystania z więcej niż 1 karty kryptograficznej, możliwe jest wnioskowanie o więcej niż 1 certyfikat (na 1 karcie może być zapisany tylko 1 certyfikat):

- użytkownicy kart typu ENCARD, decydujący się na wygenerowanie certyfikatu przez MC bezpośrednio na karcie, przesyłają zatem tyle kart kryptograficznych wraz z PIN kodami, o ile certyfikatów wnioskuje;

- użytkownicy kart typu ENCARD, decydujący się na przesłanie do MC żądania certyfikacyjnego oraz użytkownicy pozostałych typów kart (CERTUM/UNIZETO, CRYPTOTECH bądź inne, spełniające wymagania zgodności z SI CEPiK) przesyłają natomiast tyle plików z żdaniami certyfikacyjnymi, o ile certyfikatów wnioskuje. MC wygeneruje wówczas odpowiednią liczbę certyfikatów i odeśle je do Subskrybenta, który będzie mógł je samodzielnie zaimportować na posiadane karty kryptograficzne.

**UWAGA:** W przypadku wnioskowania o więcej niż 1 certyfikat dla jednego użytkownika, pliki ze zgłoszeniami certyfikacyjnymi zapisywane na nośniku należy jednoznacznie opisać, podając jako nazwę każdego z plików numer seryjny karty kryptograficznej, z której dany plik został wygenerowany.



- **Zakres zastosowania certyfikatu** → należy zaznaczyć wszystkie 4 wymienione pozycje tj.:
  - podpis cyfrowy,
  - niezaprzeczalność podpisu cyfrowego,
  - szyfrowanie kluczy sesyjnych, - uzgadnianie klucza.
- **Miejscowość i data** → miejscowość, w której wypełniany jest wniosek oraz data wypełnienia wniosku w formacie DD-MM-RRRR (dzień-miesiąc-rok).
- **Pieczęć i podpis wnioskodawcy lub osoby upoważnionej do reprezentowania wnioskodawcy** → pieczęć oraz podpis osoby upoważnionej w świetle przepisów prawa do reprezentowania wnioskującego podmiotu.

### 3) Do wniosku załączyć nośnik:

- w przypadku posiadania karty kryptograficznej typu ENCARD, jeżeli Subskrybent decyduje się na wygenerowanie certyfikatu przez MC bezpośrednio na karcie kryptograficznej → załączyć należy kartę kryptograficzną wraz z aktualnym PIN kodem;  
**UWAGA:** Ze względów bezpieczeństwa przesyłanie karty kryptograficznej wraz z PIN kodem do niej w jednej kopercie jest możliwe tylko w sytuacji, kiedy karta kryptograficzna jest pusta lub zapisany na niej certyfikat stracił już ważność; **LUB**
- w przypadku posiadania karty kryptograficznej typu: CERTUM/UNIZETO, CRYPTOTECH, bądź inne (ewentualnie ENCARD, jeżeli użytkownik decyduje się na samodzielne zaimportowanie certyfikatu na kartę) → załączyć należy nośnik (płyta CD / płyta DVD / pamięć flash) z zapisanym na nim żądaniem certyfikacyjnym.  
**UWAGA 1:** Karty kryptograficzne ww. typów (ENCARD, CERTUM/UNIZETO, CRYPTOTECH) zostały przetestowane pod kątem poprawności współpracy z aplikacją portalową SI CEPiK. W przypadku korzystania przez użytkowników z kart kryptograficznych innego typu, MC nie ponosi odpowiedzialności za ewentualne problemy techniczne.  
**UWAGA 2:** W celu uniknięcia problemów z logowaniem do aplikacji portalowej, zaleca się, aby karta kryptograficzna przeznaczona do podłączenia do SI CEPiK, nie zawierała jakichkolwiek innych certyfikatów, oprócz certyfikatu do SI CEPiK.  
**UWAGA 3:** Prosimy **nie przysyłać** do MC:
  - **czytników** do kart kryptograficznych,





- **plyt z oprogramowaniem** otrzymanych od producentów zestawów kryptograficznych,
- **oryginalnych dokumentów z kodami PIN** otrzymanych od producentów zestawów kryptograficznych.

**4) Wypełniony wniosek wraz z załączonym do niego nośnikiem przesłać do MC na adres:**

**Ministerstwo Cyfryzacji**  
**Departament Infrastruktury Państwa**  
**ul. Królewska 27**  
**00-060 Warszawa**

**UWAGA 1:** Zgodnie z obowiązującą polityką certyfikacji, wniosek certyfikacyjny powinien być przesłany do MC listem poleconym za potwierdzeniem odbioru.

**UWAGA 2:** Czas realizacji wniosku przez MC jest zgodny z zapisami Kodeksu Postępowania Administracyjnego oraz obowiązującej polityki certyfikacji. Datą rozpoczynającą upływ czasu realizacji wniosku jest data jego wpływu do MC.