**Podłączenie do systemu CEPiK 2.0**

**Wymagania techniczne**

**13 listopada 2015 r.**

**wersja 1.2**

Spis treści

[1. Cel i zakres dokumentu 3](#_Toc435169682)

[2. Podłączenie podmiotów do systemu SI CEPiK – informacje ogólne 3](#_Toc435169683)

[2.1. Węzeł Internet 3](#_Toc435169684)

[2.2. Węzeł WAN 4](#_Toc435169685)

[2.3. Wykorzystane protokoły 5](#_Toc435169686)

[2.4. Certyfikaty 5](#_Toc435169687)

[2.4.1. Certyfikat do połączeń VPN 5](#_Toc435169688)

[2.4.2. Certyfikat SSL do autoryzacji, uwierzytelniania i podpisywania 5](#_Toc435169689)

[3. Kanały dostępu 5](#_Toc435169690)

[3.1. Połączenie System-System 5](#_Toc435169691)

[3.1.1. Wymagania dla systemu zewnętrznego 6](#_Toc435169692)

[3.2. Aplikacje z interfejsem graficznym (aplikacje WWW) 6](#_Toc435169693)

[3.2.1. System operacyjny 6](#_Toc435169694)

[3.2.2. Przeglądarka internetowa 7](#_Toc435169695)

[3.2.3. Mikroprocesorowa karta kryptograficzna 7](#_Toc435169696)

[4. Uwierzytelnianie, autoryzacja, rozliczalność, integralność, poufność danych 8](#_Toc435169697)

[4.1. Uwierzytelnianie i autoryzacja 8](#_Toc435169698)

[4.2. Poufność transmisji danych 8](#_Toc435169699)

[4.3. Rozliczalność i integralność 8](#_Toc435169700)

# Cel i zakres dokumentu

Celem dokumentu jest dostarczenie podmiotom zewnętrznym i użytkownikom końcowym informacji niezbędnej do przeprowadzenia integracji w tym zakresie z systemem CEPiK 2.0. Dokument zawiera niezbędne informacje dotyczące technicznych aspektów i minimalnych wymagań dotyczących połączenia z SI CEPiK.

# Podłączenie podmiotów do systemu SI CEPiK – informacje ogólne

Dostęp dla podmiotów zewnętrznych do Systemu CEPiK 2.0 realizowany będzie poprzez dwa węzły do obsługi sieci:

* WAN (wide area network) – sieć o wysokim stopniu zaufania,
* Internet – sieć o niskim stopniu zaufania.



*Rysunek 1 Architektura węzła WAN i Internet*

Niezbędne informacje, w tym adresy pod którymi dostępne są usługi są zawarte w dokumentacji dotyczącej poszczególnych usług.

## Węzeł Internet

Połączenie poprzez sieć o niskim poziomie zaufania odbywać się będzie za pomocą połączenia VPN. Dodatkowo wszystkie transakcje wykonywane w systemie CEPiK 2.0, niezależnie od metody połączenia, używać będą szyfrowanej transmisji wykorzystującej protokół SSL oraz symetryczny klucz szyfrujący.

Do poprawnej komunikacji z systemem tym kanałem wymagane będzie posiadanie wydanego przez MSW certyfikatu niezbędnego do połączenia. Certyfikat ten zostanie wygenerowany w postaci pliku.

Zalecane są następujące minimalne parametry łącz po stronie podmiotów:

1. symetryczne łącze ze stałym adresem publicznym,
2. łącze o przepustowości minimum 512KB/s

W przypadku gdy podmiot posiada więcej niż jedną stację dostępową zalecane jest, aby bezpieczny kanał VPN zestawiany był na poziomie urządzenia (routera) o następujących parametrach:

1. Możliwość zestawienia tunelu VPN (IPSec) do urządzenia Cisco ASA 55xx z wykorzystaniem certyfikatu wystawionego przez MSW w postaci pliku,
2. możliwość zestawienia tunelu VPN „na żądanie”,
3. dedykowany interfejs sieciowy (lokalny) do połączenia z wydzieloną siecią LAN,
4. możliwość definiowania reguł ograniczających ruch pomiędzy interfejsami,
5. możliwość definiowania reguł ograniczających dostęp do tunelu VPN.

Dla podmiotu korzystającego z typu połączenia L2L potrzebny będzie jeden certyfikat do zestawienia połączenia VPN.

W przypadku połączeń pojedynczych stacji dostępowych możliwe jest wykorzystanie wyłącznie połączenia VPN typu Remote Access, które wymaga zastosowania oprogramowania instalowanego bezpośrednio na stacji dostępowej oraz certyfikatu VPN dla każdej stacji.

Do uwierzytelnienia, autoryzacji i podpisywania komunikatów niezbędny będzie certyfikat SSL wydany przez MSW:

* W przypadku połączenia system – system, certyfikat będzie wystawiony dla systemu zewnętrznego i może być zainstalowany w systemie zewnętrznym, w urządzeniu HSM lub na mikroprocesorowej karcie kryptograficznej.
* W przypadku korzystania z aplikacji WWW udostępnianych przez MSW, wystawione certyfikaty będą personalizowane. Certyfikaty takie muszą być zainstalowane na mikroprocesorowych kartach kryptograficznej, w zależności od przyjętych przez dany podmiot założeń technicznych dla swojego systemu.

Zakup kart oraz czytników jest po stronie podmiotów zewnętrznych. Wymagania związane z mikroprocesorowymi kartami kryptograficznymi są określone w rozdziale 3.2.3.

## Węzeł WAN

W sieci WAN, podobnie jak przy połączeniach z siecią Internet, wymagane będzie szyfrowanie transmisji z wykorzystaniem protokołu SSL oraz symetrycznego klucza szyfrującego do szyfrowania komunikatów. Do poprawnej komunikacji z systemem CEPiK 2.0 tym kanałem wymagane będzie posiadanie certyfikatu wystawionego przez MSW.

* W przypadku korzystania z aplikacji systemu CEPiK 2.0 certyfikaty te muszą zostać umieszczone na mikroprocesorowych kartach kryptograficznych zabezpieczonych kodem PIN.
* W przypadku komunikacji system-system (korzystanie z interfejsów API systemu CEPiK 2.0) certyfikat dostarczany będzie w postaci pliku i będzie mógł być zainstalowany w systemie zewnętrznym, w urządzeniu HSM lub na mikroprocesorowej karcie kryptograficznej.

Zakup kart oraz czytników jest po stronie podmiotów zewnętrznych. Wymagania związane z mikroprocesorowymi kartami kryptograficznymi są określone w rozdziale 3.2.3.

**Ważne:** W przypadku podmiotów, które posiadają już połączenie z obecnie eksploatowanym systemem CEPiK przez sieć wydzieloną (np. OST112, GOVNET, sTESTA (TESTA NG) lub inną, dostęp do systemu CEPiK 2.0 planowany jest w ramach obecnie zestawionych połączeń.

## Wykorzystane protokoły

Komunikacja systemu zewnętrznego z udostępnionym interfejsem realizowana będzie z użyciem protokołu SOAP. Specyfikacja metod udostępnianych przez API CEPiK 2.0 będzie realizowana za pomocą języka WSDL opartego na konstrukcji XML-a, który służy do definiowania usług internetowych.

Jako protokół transportowy pomiędzy systemem zewnętrznym, a systemem CEPiK 2.0 wykorzystywany jest protokół HTTPS.

## Certyfikaty

### Certyfikat do połączeń VPN

Użytkownicy komunikujący się z systemem CEPiK 2.0 przez sieć publiczną Internet musza posiadać certyfikaty wydane przez MSW w *Polityce certyfikacji dla urządzeń systemu CEPiK*.

**Ważne:** Użytkownicy posiadający certyfikaty VPN w celu korzystana z aplikacji WWW CBE mogą wykorzystać te certyfikaty przy innych usługach i aplikacjach systemu CEPiK 2.0, nie jest wymagane wnioskowanie o nowy certyfikat VPN.

### Certyfikat SSL do autoryzacji, uwierzytelniania i podpisywania

Użytkownicy muszą posiadać certyfikaty SSL wydane przez MSW w *Polityce certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK, łączących się przez sieć publiczną*.

**Ważne:** Użytkownicy posiadający certyfikaty SSL w celu korzystania z aktualnie eksploatowanych aplikacji OZZ, SKP lub ADR mogą wykorzystać te certyfikaty przy innych usługach i aplikacjach systemu CEPiK 2.0, nie jest wymagane wnioskowanie o nowy certyfikat SSL.

# Kanały dostępu

W zależności od usługi połączenie z CEPiK 2.0 może być realizowane na dwa sposoby:

* połączenie system CEPiK 2.0 – system podmiotu zewnętrznego,
* aplikacja z interfejsem graficznym dostarczanym przez CEPiK 2.0.

## Połączenie System-System

Komunikacja systemu zewnętrznego z udostępnionym interfejsem (API) odbywać się będzie z użyciem protokołu komunikacyjnego SOAP. Specyfikacja metod udostępnianych przez API będzie realizowana za pomocą języka WSDL opartego na konstrukcji XML, który służy do definiowania usług internetowych. API udostępniać będzie usługi działające w trybie **synchronicznym lub asynchronicznym**.

Udostępnianie danych w trybie **synchronicznym** odbywać się będzie w następujący sposób:

* Użytkownik podmiotu żądającego informacji formułuje zapytanie i wysyła je do systemu CEPiK 2.0 za pośrednictwem systemu eksploatowanego przez instytucję, której jest pracownikiem.
* System CEPiK wyszukuje potrzebne informacje, formułuje i odsyła odpowiedź.
* Użytkownik podmiotu żądającego informacji odbiera i odczytuje komunikat z odpowiedzią.

Komunikacja w tym procesie jest synchroniczna, całość procesu realizowana jest w bardzo krótkim czasie.

Przy udostępnianiu danych w trybie **asynchronicznym**:

* Użytkownik podmiotu żądającego informacji formułuje zapytanie i wysyła je do systemu CEPiK 2.0 za pośrednictwem systemu eksploatowanego przez instytucję, której jest pracownikiem.
* System CEPiK 2.0 wyszukuje potrzebne informacje, formułuje i odsyła odpowiedź.
* Użytkownik podmiotu żądającego informacji odbiera i odczytuje komunikat z odpowiedzią.

Komunikacja w procesie realizowana jest w sposób asynchroniczny, a całość procesu jest rozciągnięta w czasie (tj. użytkownik po wysłaniu zapytania porzuca proces i dopiero po pewnym czasie do niego powraca sprawdzając, czy nadszedł komunikat z odpowiedzią systemu). Czas oczekiwania na odpowiedź może być długi.

Tryb asynchroniczny oferuje szersze możliwości formułowania zapytań.

### Wymagania dla systemu zewnętrznego

#### Wymagania dotyczące oprogramowania i sprzętu

Wszystkie wymagania dotyczące zarówno sprzętu jak i systemu operacyjnego oraz innego oprogramowania powinien wskazać producent oprogramowania łączącego się z systemem CEPiK 2.0.

#### Podpisywanie komunikatów

W celu podpisywania komunikatów wykorzystywany jest mechanizm XML Signature. Podpisywany jest element „body” koperty SOAP. Podpis – zgodny ze standardem XML Signature dołączony jest do nagłówka (elementu „header”) koperty SOAP. Do podpisu dołączony jest certyfikat z kluczem publicznym służącym do weryfikacji podpisu.

#### Sprawdzanie dostępności serwisu

Najszybszą metodą weryfikacji dostępności serwisu jest pobranie pliku WSDL poprzez wywołanie z użyciem protokołu https adresu usługi: np. <https://adres_IP_uslugi:port/url_uslugi_nazwa_uslugi?wsdl>

Adresy usług będą określone w dokumentacji dla każdego modułu (usługi).

W przypadku gdy usługa jest dostępna plik zostanie pobrany a transfer zakończy się ze statusem 200.

W przypadku niedostępności usługi zwrócony zostanie inny status (np.: 404, 500).

## Aplikacje z interfejsem graficznym (aplikacje WWW)

### System operacyjny

Aby móc skorzystać z aplikacji WWW udostępnianych przez system CEPiK 2.0, możliwe jest wykorzystanie dowolnego systemu operacyjnego umożliwiającego zainstalowanie jednej z przeglądarek, o których mowa w rozdziale 3.2.2. Aby uniknąć problemów z instalacją sterowników do czytników kart mikroprocesorowych sugeruje się, aby był to system wspierany przez producenta posiadanego zestawu kryptograficznego.

Ze względów bezpieczeństwa zaleca się, aby korzystać z systemów operacyjnych posiadających ważne wsparcie techniczne producenta.

### Przeglądarka internetowa

Aplikacje systemu CEPiK 2.0 z graficznym interfejsem graficznym udostępnione zostaną w trybie tzw. „cienkiego klienta” przez przeglądarkę internetową. Wymagania niezbędne do umożliwienia pracy z aplikacją:

* Przeglądarki, wersja nie starsza niż:
  + Internet Explorer 9
  + Firefox 27
  + Chrome 32

### Mikroprocesorowa karta kryptograficzna

Obecnie wydane i certyfikowane przez urząd certyfikacji MSW karty mikroprocesorowe będą mogły być wykorzystane również do dostępu do systemu CEPiK 2.0 – wymaganiem jest posiadanie certyfikatu wystawionego w *Polityce certyfikacji dla instytucji zewnętrznych korzystających z systemu CEPiK, łączących się przez sieć publiczną*.

**Ważna informacja związana z mikroprocesorowymi kartami kryptograficznymi:** docelowo MSW uruchomi nowe urzędy certyfikacji, klucze kryptograficzne w nowych politykach certyfikacji zostaną podniesione do wielkości co najmniej 2048 KB, dlatego też użytkownicy muszą przewidzieć po swoje stronie wymianę posiadanych kart na takie, które obsłużą większy klucz, o czym zostaną odpowiednio wcześniej poinformowani.

Podmioty nie posiadające obecnie karty z ważnym certyfikatem powinny zaopatrzyć się w czytnik oraz kartę spełniającą poniższe wymagania:

* + - 1. Karta kryptograficzna wyposażona w interfejs zgodny z normami: ISO 7816, ISO 14443.
      2. Karta kryptograficzna wyposażona w procesor o pojemności min 32 kb.
      3. Karta kryptograficzna zgodna ze standardem Java Card w wersji min 2.2.1.
      4. Napięcie zasilania karty kryptograficznej musi mieścić się w zakresie 1,62 - 5,5 V.
      5. Gwarantowana ilość cykli zapisu/kasowania karty kryptograficznej nie może być mniejsza niż 500 000.
      6. Karta kryptograficzna ma być wspierana przez następujące algorytmy kryptograficzne i szyfrujące: AES (128, 192, 256), RSA (2048 bit), SHA-1, SHA-256, SHA-512.
      7. Karta kryptograficzna ma generować klucze kryptograficzne: AES (128, 192, 256), RSA(2048 bit), SHA-1, SHA-256, SHA-512.
      8. Karta kryptograficzna ma posiadać wsparcie dla: MS terminal Services, logowania w domenie, pracy wieloaplikacyjnej.
      9. Karta kryptograficzna ma zapewniać wsparcie dla różnych kodów PIN, PUK.
      10. Karta kryptograficzna ma zapewniać wsparcie dla PKCS #11 dla systemów Windows w wersji językowej polskiej lub angielskiej, 32 lub 64 bity (Server, Vista, Windows 7, Windows 8) oraz Unix /Linux 32 lub 64 bity.
      11. Karta kryptograficzna ma zapewniać wsparcie dla CSP dla systemu operacyjnego Windows w wersji językowej polskiej lub angielskiej, 32 lub 64 bity (Server, Vista, Windows 7, Windows 8).
      12. Karta musi posiadać certyfikat bezpieczeństwa układu mikroprocesorowego na poziomie ITSEC E3 lub Fips 140-2 level 3 lub Common Criteria EAL4+.

# Uwierzytelnianie, autoryzacja, rozliczalność, integralność, poufność danych

## Uwierzytelnianie i autoryzacja

Uwierzytelnianie odbywać się będzie na dwa sposoby:

1. uwierzytelnienie użytkownika (operatora) w aplikacji WWW systemu CEPiK 2.0 z użyciem dostarczanego na karcie prywatnego certyfikatu zabezpieczonego kodem PIN,
2. uwierzytelnianie użytkownika w systemie zewnętrznym (systemu zewnętrznego) – w tym przypadku uwierzytelnianie użytkownika końcowego w danym podmiocie odbywa się w jego systemie zewnętrznym, dopiero w przypadku działań użytkownika związanych z wymianą danych z systemem CEPiK 2.0 system zewnętrzny uwierzytelnia się w systemie CEPiK 2.0 z użyciem posiadanego certyfikatu wystawionego przez MSW.

## Poufność transmisji danych

Połączenia pomiędzy systemem zewnętrznym korzystającym z interfejsu a systemem CEPiK 2.0 używają szyfrowanej transmisji wykorzystującej protokół SSL oraz symetryczny klucz szyfrujący.

## Rozliczalność i integralność

1. W przypadku gdy z SI CEPiK komunikuje się system zewnętrzny podmiotu, uwierzytelnianiu i autoryzacji podlega jedynie serwer komunikacyjny systemu zewnętrznego, do którego przypisany jest odpowiedni profil uprawnień. Interfejs wymaga, aby jednym z parametrów zapytania był identyfikator użytkownika, w imieniu którego system zewnętrzny przekazał zapytanie.

Zapewnienie rozliczalności działań użytkowników oraz ograniczenie zwracanego im zakresu informacyjnego w zależności od przysługujących im uprawnień spoczywa jednak na systemie zewnętrznym. System CEPiK 2.0 zwraca pełny zakres danych, do którego dany podmiot ma uprawnienia.

Uwierzytelnienie polega na sprawdzeniu certyfikatu którym podpisany jest komunikat. Jego podpisanie przez system zewnętrzny zapewnia integralność komunikatu. Do podpisu komunikatu konieczny będzie certyfikat SSL różny od certyfikatu wykorzystywanego do zabezpieczenia połączenia VPN pomiędzy systemem zewnętrznym a systemem CEPiK 2.0.

1. W przypadku, gdy użytkownik korzysta z aplikacji WWW udostępnianej przez MSW w ramach systemu CEPiK 2.0, rozliczalność jest zapewniana przez system CEPiK 2.0.