Specyfikacja techniczna interfejsu do obsługi badań technicznych.

25 lipca 2017 r.

Dotyczy umowy z dn. 27.09.2013r. w sprawie realizacji projektu „CEPiK 2.0”
Nr MSW: 8/DEP/2013
Nr COI: 6/U/COI/MSW/2013

ul. Suwak 3 | 02-676 Warszawa | tel.: +48 22 250 28 83 | fax: +48 22 250 29 87 | e-mail: coi@coi.gov.pl | www.coi.gov.pl

Spis treści

Metryka dokumentu **3**

Historia zmian **3**

Słownik podstawowych pojęć **4**

1. Cel i zakres dokumentu **5**

2. Ogólna charakterystyka interfejsu udostępniania danych dotyczących Stacji Kontroli Pojazdów **5**

3. Podłączenie do systemu SI CEPiK **6**

3.1. Podłączenie podmiotów do systemu CEPiK 6

3.1.1. Podłączenie bezpośrednie SKP z CEPiK 2.0 6

3.1.1. Podłączenie SKP poprzez aplikację centralną 7

3.2. Wykorzystane protokoły 9

4. Uwierzytelnianie, autoryzacja, rozliczalność, integralność transakcji i poufność danych **9**

4.1. Uwierzytelnianie i autoryzacja 10

4.2. Poufność transmisji danych 10

4.3. Rozliczalność i integralność 10

5. Wymagania dla systemu zewnętrznego **11**

5.1. Podpisywanie komunikatów 11

5.2. Walidacja pól w API 11

5.3. Sprawdzanie dostępności serwisu 11

5.4. Obsługa tokenu aktualności 11

6. Specyfikacja metod usługi SkpService **12**

6.1. Metoda pytanieOPojazd 13

6.2. Metoda pytanieOBadanieTechniczne 14

6.3. Metoda zapisPojazduPrerejestrowanego 14

6.4. Metoda zapisBadaniaTechnicznego 14

6.4.1. Zapis nowego badania technicznego 14

6.4.2. Modyfikacja badania technicznego 15

6.4.3. Przerwanie badania technicznego 15

6.4.4. Obsługa trybu awaryjnego 16

6.5. Metoda anulowanieBadaniaTechnicznego 16

6.6. Metoda anulowaniePrerejestracji 16

7. Komunikaty błędów **17**

Metryka dokumentu

Tytuł: Specyfikacja techniczna interfejsu wymiany danych - SKP.		
Opis: Specyfikacja techniczna interfejsu wymiany danych z systemem CEPiK dla systemów zewnętrznych - SKP.		Data utworzenia: 2017-04-12
Autor:	*Centralny Ośrodek Informatyki*	

Historia zmian

Data	Autorzy	Opis zmian
2015-05-15	Grzegorz Krupiński Marcin Dłubakowski Tomasz Buraczyński	Utworzenie dokumentu
2015-05-15	Magda Gałach	Aktualizacja i zatwierdzenie dokumentu
2015-05-19	MSW	Uwagi
2015-05-27	Grzegorz Krupiński Marcin Kubarek Magda Gałach	Aktualizacja dokumentu; uwzględnienie uwag MSW
2015-06-11	Marcin Dłubakowski	Uzupełnienie opisu metod; aktualizacja tabeli błędów; korekty wsdl
2015-08-07	Grzegorz Krupiński	Korekta wsdl i dokumentacji, załączniki w oddzielnym pliku zip.
2015-09-09	Magda Gałach	Aktualizacja dokumentu
2015-10-30	Grzegorz Krupiński	Aktualizacja dokumentu
2016-01-29	Grzegorz Krupiński	Korekta wsdl i dokumentacji
2017-03-24	Michał Wudarczyk	Modyfikacja dokumentacji po refaktoringu modelu dziedziny Centralnej Ewidencji Pojazdów
2017-03-28	Michał Wudarczyk	Uzupełnienie dokumentu o opis komunikacji SKP z systemem CEPIK 2.0 poprzez aplikacje centralnie dostarczane przez zewnętrzne podmioty oraz naniesienie zmian zgodnie z uwagami architektów i administratorów CEPIK 2.0
2017-04-12	Michał Wudarczyk	Modyfikacja w rozdziale 6.1 dla minimalnych kryteriów wyszukiwania pojazdu: numerRejestracyjny + marka
2017-07-25	Mirosław Smoczyński	Modyfikacja w rozdziale 6.1 dla minimalnych kryteriów wyszukiwania pojazdu pod najnowsza tabelę walidacyjną.

Słownik podstawowych pojęć

Nazwa / skrót	Opis
Broker komunikacyjny	Aplikacje centralne dostarczane przez niezależnych dostawców dla Stacji Kontroli Pojazdów, pełniące rolę pośrednika w komunikacji pomiędzy SKP a CEPiK 2.0.
Identyfikator systemowy transakcji	Unikalny identyfikator w ramach instytucji nadawany każdemu komunikatowi wysyłanemu do SI CEPiK przez system informatyczny instytucji zewnętrznej.
Magistrala serwisowa	Rozwiązanie w warstwie pośredniczącej w dostępie do usług w architekturze zorientowanej na usługi
SKP	Stacja Kontroli Pojazdów
SOAP	Simple Object Access Protocol – protokół zdalnego dostępu do obiektów bazujący na wykorzystaniu XML (protokół komunikacyjny, wykorzystujący XML do kodowania wywołań jak również wykorzystania protokołu HTTP do ich przenoszenia, jest standardem W3C.
System Centralny	System Informatyczny Centralnej Ewidencji Pojazdów i Kierowców (SI CEPiK).
Systemy zewnętrzne	Autonomiczne systemy informatyczne wykorzystywane przez instytucje, uprawnione do komunikowania się z Systemem Centralnym.
WSDL	Web Service Definition Language – plik definicji usługi sieciowej.
Wywołanie synchroniczne	W wywołaniu synchronicznym system żądający wykonania danej operacji jest blokowany do momentu jej zakończenia. Rezultatem wywołania synchronicznego jest odpowiedź z danymi ewidencji (ew. o braku takich danych)

1. Cel i zakres dokumentu

Celem dokumentu jest dostarczenie podmiotom zewnętrznym korzystającym z interfejsu do obsługi badań technicznych w Centralnej Ewidencji Pojazdów i Kierowców szczegółowej informacji niezbędnej do przeprowadzenia integracji w tym zakresie z systemem CEPiK. Dokument zawiera niezbędne informacje dotyczące technicznych aspektów połączenia systemów zewnętrznych z SI CEPiK oraz szczegółowy opis metod udostępnianych przez usługę.

W dokumencie znajdują się zatem:

- podstawowe informacje na temat interfejsu (Rozdział 2),
- opis założeń przyjętych przy tworzeniu niniejszego interfejsu (Rozdział 3),
- podstawowe informacje na temat architektury interfejsu (Rozdział 4),
- opis wymagań technicznych, które muszą zostać spełnione przez system zewnętrzny aby korzystać z interfejsów do udostępniania danych Centralnej Ewidencji Pojazdów i Kierowców (Rozdział 5),
- opis metod usługi, zakresu zwracanych danych oraz minimalnego zestawu parametrów niezbędnych do ich wywołania (Rozdział 6).

2. Ogólna charakterystyka interfejsu udostępniania danych dotyczących Stacji Kontroli Pojazdów

Interfejs udostępnia następujące informacje dotyczące Stacji Kontroli Pojazdów:

- dane o SKP
- dane o pojazdach
- dane o badaniach technicznych pojazdów

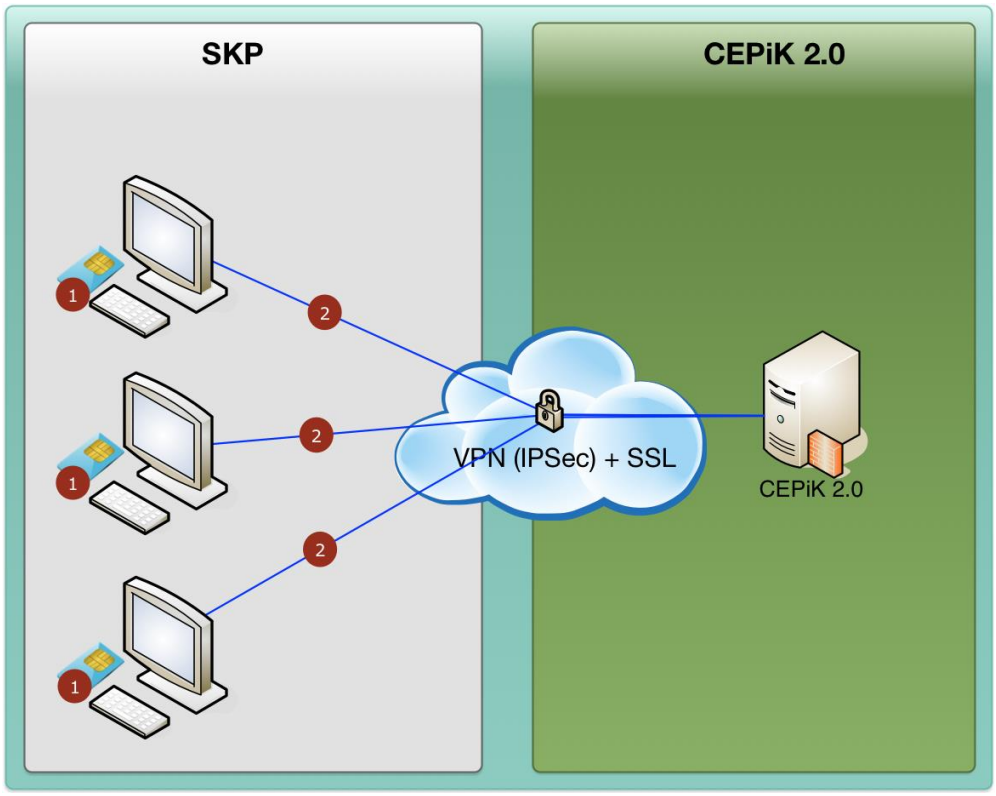
Komunikacja podmiotów zewnętrznych z API odbywać się będzie z użyciem protokołu komunikacyjnego SOAP. API udostępniać będzie dane w trybie **synchronicznym**, w następujący sposób: Użytkownik podmiotu żądającego informacji formułuje zapytanie i wysyła je do systemu CEPiK za pośrednictwem systemu eksploatowanego 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. Architektura API zapewni możliwość rozwoju i budowy przyrostowej – przewiduje się, że część nowych (wersji) funkcji będzie dodawana z zachowaniem działania istniejących. Ma to na celu zapewnienie gładkiego dostosowywania systemów Instytucji zewnętrznych do zmienianej (rozwijanej) funkcjonalności API.

3. Podłączenie do systemu SI CEPiK

3.1. Podłączenie podmiotów do systemu CEPiK

3.1.1. Podłączenie bezpośrednie SKP z CEPiK 2.0

Podłączenie bezpośrednie SKP do systemu CEPiK 2.0, jest standardową metodą komunikacji Stacji kontroli Pojazdów z systemem CEPiK 2.0. Poniżej przedstawiono schemat niniejszej komunikacji:



Schemat podłączenia bezpośredniego SKP do systemu CEPiK 2.0

Dostęp do Systemu CEPiK 2.0 dla SKP realizowany będzie poprzez sieć Internet za pomocą połączenia VPN (2). Dodatkowo wszystkie komunikaty wymieniane pomiędzy systemami używać będą szyfrowanej transmisji wykorzystującej protokół SSL oraz symetrycznych kluczy szyfrujących (1). Do poprawnej komunikacji z systemem tym kanałem wymagane więc będzie posługiwanie się wydanym przez MSW certyfikatem niezbędnym do połączenia VPN.

Zalecane są następujące minimalne parametry połączenia:

1. łącze internetowe o przepustowości minimum 512Kb/s

Łącze internetowe powinno być zakończone urządzeniem (routerem) o parametrach:

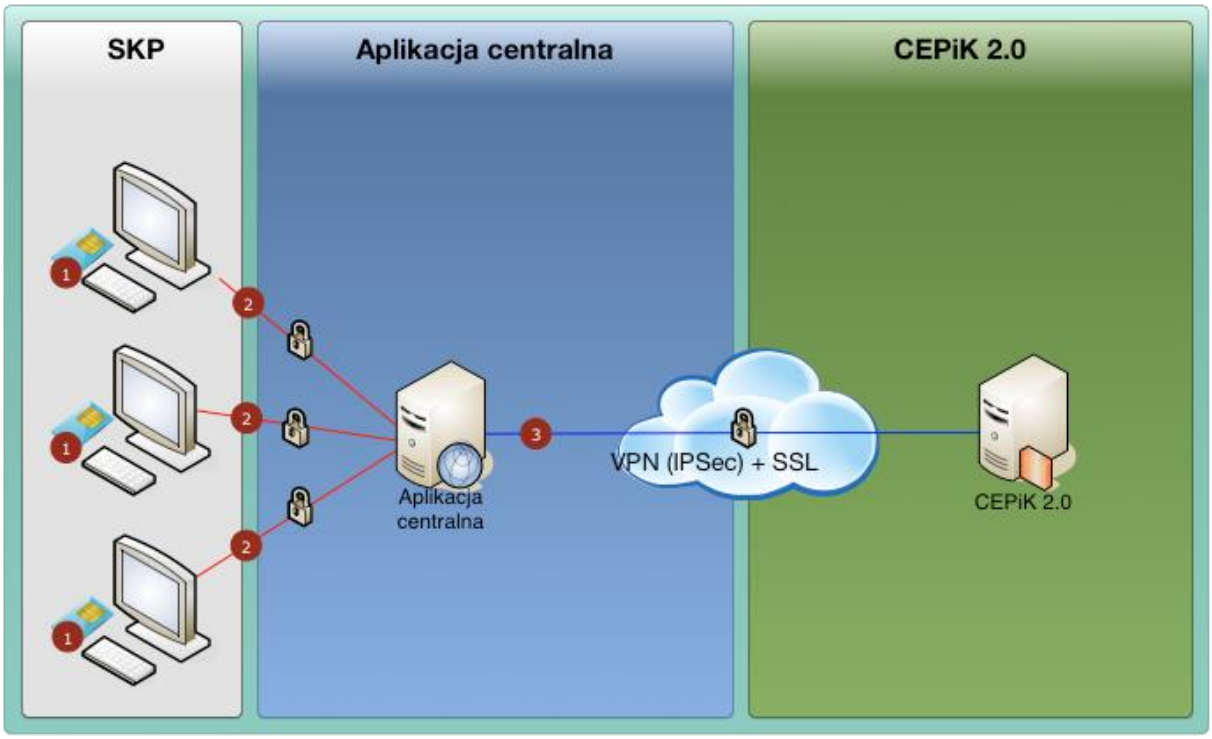
1. możliwość zestawienia tunelu VPN (IPSec) z wykorzystaniem certyfikatu do urządzenia Cisco ASA 55xx,
2. możliwość zestawienia tunelu VPN „na żądanie”,
3. dedykowany interfejs sieciowy (lokalny) do połączenia z wydzieloną siecią LAN,
4. możliwość definiowania reguł ograniczających ruch pomiędzy interfejsami,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

W przypadku połączeń pojedynczych użytkowników indywidualnych możliwe jest wykorzystanie połączenia VPN typu Remote Access. Wymaga to zastosowania specjalnego oprogramowania instalowanego bezpośrednio na stacji roboczej.

Procedura konfiguracji kanału VPN stanowi załącznik do niniejszego dokumentu.

3.1.2. Podłączenie SKP poprzez aplikację centralną

W komunikacji SKP z systemem CEPiK 2.0 dopuszczono aplikacje centralne pełniące rolę brokera komunikacji pomiędzy SKP a CEPiK 2.0. Schemat komunikacji z wykorzystaniem aplikacji centralnych przedstawiono na rysunku poniżej :



Schemat połączenia SKP do systemu CEPiK 2.0 przez Aplikację centralną

W przypadku komunikacji SKP poprzez aplikację centralną pełniącej rolę brokera komunikacyjnego wymagane są certyfikaty SSL, wystawiane przez MC dla Stacji Kontroli Pojazdów na kartach kryptograficznych zabezpieczonych kodem PIN. Certyfikat SSL w SKP wykorzystywany będzie do podpisywania komunikatów przesyłanych do systemu CEPiK 2.0 zgodnie z polityką bezpieczeństwa. Karta kryptograficzna jest własnością SKP i nie może zostać przekazana lub użyczona podmiotowi trzeciemu. Certyfikaty (w szczególności – klucz prywatny) znajdujące się na karcie kryptograficznej nie mogą być wyeksportowane do pliku.

Wymagane jest zabezpieczenie połączenia SSL pomiędzy stanowiskiem SKP a aplikacją centralną (2). Za zabezpieczenie połączenia odpowiada dostawca aplikacji centralnej.
Połączenie pomiędzy aplikacją centralną a terminalem końcowym (w rozumieniu – cienki/gruby klient, połączenie terminalowe, itp.) wymaga zabezpieczenia połączenia SSL z kluczem nie krótszym niż 2048bity. Certyfikat kliencki, którym będzie szyfrowana komunikacja – nie będzie certyfikatem zbiorczym – każda stacja łącząca się do aplikacji centralnej będzie posiadała swój wygenerowany certyfikat.

Wymagane jest zabezpieczone połączenie VPN (IPSec) (3) na podstawie certyfikatu wydanego przez MC dla dostawcy aplikacji centralnej jako brokera komunikatów do systemu CEPiK 2.0.
Wymagane jest, aby certyfikaty produkcyjne dla dostawców wydawane były po formalnym zapewnieniu przez tych dostawców aplikacji centralnej:

- bezpiecznego połączenia pomiędzy Stacją Kontroli Pojazdów a brokerem / aplikacją centralną – SSL 2048bit z funkcją skrótu SHA-256,
- spełniania wymagań bezpieczeństwa dla SKP określonych w polityce bezpieczeństwa, m.in. w zakresie polityki haseł (złożoność, termin zmiany),
- Zapewnienie pełnej rozliczalności wszystkich zapytań przesyłanych i odbieranych z systemu CEPiK 2.0 przez dostawcę aplikacji centralnej w tym zapewnienie należytych zabezpieczeń logów w zakresie niezaprzeczalności oraz kompletności logów zgodnie w zakresie:
    - Czas wykonania operacji – czas jest zapisywany w oparciu o ogólnie dostępny serwer czasu NTP.
    - Publiczny adres IP po którym następuje połączenie do serwera centralnego.
    - Prywatny adres IP terminala operatorskiego (w rozumieniu – cieki/gruby klient) pozwalający na jednoznaczne zidentyfikowanie stanowiska roboczego.
    - Dane operatora który pracował w danym momencie na terminalu.

- Zapis wykonanych operacji z uwzględnieniem logowania całych nieprzetworzonych wysłanych i otrzymanych komunikatów (rozumiane w sensie – logowania wszystkich wysłanych i otrzymanych komunikatów SOAP) do systemu CEPiK 2.0.

- Przesyłanie komunikatów poprzez system centralny dostawcy wymaga aby każdy komunikat przesyłany i odbierany z systemu CEPiK 2.0 był podpisany certyfikatem diagnosty (1) – nie obejmuje to metod do pobierania danych słownikowych.

Każda Stacja Kontroli Pojazdów jeśli planuje korzystać z centralnej aplikacji do przekazywania informacji musi zgłosić ten fakt do MC wskazując dostawcę oprogramowania z którego korzysta. Informacja ta będzie konieczna do poprawnego uwierzytelnienia użytkownika w systemie CEPiK 2.0 (bez podania tej informacji SKP nie zostaną nadane uprawnienia w systemie).

Niezależne od przyjętego sposobu połączenia (połączenie bezpośrednio, połączenie SKP), zakres informacyjny i specyfikacja techniczna interfejsu pozostają niezmienne. Zmianie ulega jedynie adres URI usługi.

3.2. Wykorzystane protokoły

Komunikacja systemu zewnętrznego z udostępnionym interfejsem realizowana będzie z użyciem protokołu SOAP. Specyfikacja metod udostępnianych przez API SI CEPiK będzie realizowana za pomocą języka WSDL opartego na konstrukcji XML-a, który służy do definiowania usług internetowych.
Jako protokół transportowy pomiędzy systemem zewnętrznym, a Centralną Ewidencją Pojazdów i kierowców wykorzystywany jest protokół HTTPS.

4. Uwierzytelnianie, autoryzacja, rozliczalność, integralność transakcji i poufność danych

Wszystkie operacje realizowane przez użytkownika w systemie CEPiK będą logowane do logów AUDYT i SLA, a w przypadku danych osobowych również do logu GIODO.

Uwierzytelnienie użytkownika w systemie CEPiK odbywać się będzie z użyciem dostarczanego na karcie prywatnego certyfikatu zabezpieczonego kodem PIN, rozliczalność transakcji zapewnia SI CEPiK.
Na potrzeby korzystania z systemu przewidziany jest jeden spójny interfejs dostępowy, ograniczanie zakresu informacyjnego odbywać się będzie na podstawie danych autoryzacyjnych użytkownika

przechowywanych w repozytorium tożsamości systemu CEPiK. Obecnie posiadane przez podmioty karty i certyfikaty będą mogły być wykorzystane w zmodernizowanym systemie.
Instrukcja podpisywania komunikatów stanowi, wraz z przykładem konfiguracji narzędzia SOAP UI, na potrzeby testów integracyjnych stanowi załącznik do niniejszego dokumentu.

4.1. Uwierzytelnianie i autoryzacja

Uwierzytelnienie użytkownika w systemie CEPiK odbywać się będzie z użyciem dostarczanego na karcie prywatnego certyfikatu zabezpieczonego kodem PIN, rozliczalność transakcji zapewnia SI CEPiK.
Na potrzeby korzystania z systemu przewidziany jest jeden spójny interfejs dostępowy, ograniczanie zakresu informacyjnego odbywać się będzie na podstawie danych autoryzacyjnych użytkownika przechowywanych w repozytorium tożsamości systemu CEPiK. Obecnie posiadane przez podmioty karty i certyfikaty będą mogły być wykorzystane w zmodernizowanym systemie.
Instrukcja podpisywania komunikatów stanowi, wraz z przykładem konfiguracji narzędzia SOAP UI, na potrzeby testów integracyjnych stanowi załącznik do niniejszego dokumentu.

4.2. Poufność transmisji danych

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

4.3. Rozliczalność i integralność

W przypadku gdy z SI CEPiK integruje się system zewnętrznym 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.
Uwierzytelnienie polega na sprawdzeniu certyfikatu którym podpisany jest komunikat. Jego podpisanie przez system zewnętrzny zapewnia integralność komunikatu. Do podpisu komunikatu konieczny będzie certyfikat różny od certyfikatu wykorzystywanego do zabezpieczenia połączenia pomiędzy systemem zewnętrznym a SI CEPiK.

5. Wymagania dla systemu zewnętrznego

5.1. 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.

5.2. Walidacja pól w API

Parametry zapytań walidowane są pod kątem :

- Pola typu *date* i *dateTime* są walidowane pod kątem poprawności na poziomie WSDL. Prawidłowy format danych to: *date* (YYYY-MM-DD) i *dateTime* (YYYY-MM-DDThh:mm:ss).
- Długość pól tekstowych jest weryfikowana na poziomie WSDL
- Pola typu *boolean* (wartości true/false) są walidowane pod kątem poprawności na poziomie WSDL
- Weryfikacja poprawności wypełnienia pól wskazanych jako wymagane.

5.3. Sprawdzanie dostępności serwisu

Najszybszą metodą weryfikacji dostępności serwisu jest pobranie pliku WSDL z opisem usługi. Poprzez wywołanie z użyciem protokołu https adresu usługi z Internetu:

https://skp.cepik **adres IP:185.41.93.106, port 443**

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).

Dokładny adres usługi będzie określony w momencie uruchomienia usługi.

5.4. Obsługa tokenu aktualności

Podczas wywoływania usługi udostępniania wraz z danymi zostanie przekazany token aktualności danych pojazdu. Są to unikalne identyfikatory w postaci łańcucha znaków, które służą do sprawdzenia podczas procesu zasilania czy w między czasie dane nie zostały zmienione przez innego użytkownika systemu. W przypadku niezgodności tokenu zwracany jest komunikat o nieaktualności tokenu. W takiej sytuacji należy wykonać ponowne pobranie danych z bazy z aktualnym tokenem i przeprowadzić operacje zapisu raz jeszcze na aktualnych danych.

6. Specyfikacja metod usługi SkpService

Dane udostępniane przez interfejs SKP dotyczą prezentacji stanu aktualnego. Historia zmian danych nie jest dostępna za pośrednictwem tego interfejsu.

Komunikaty wejściowe i wyjściowe w usługach prezentuje poniższa tabela.

Usługa	Komunikat wejściowy	Komunikat wyjściowy
pytanieOPojazd	pytanieOPojazd	pytanieOPojazdRezultat
pytanieOBadanieTechniczne	pytanieOBadanieTechniczne	pytanieOBadanieTechniczneRezultat
zapisPojazduPrerejestrowanego	zapisPojazduPrerejestrowanego	zapisPojazduPrerejestrowanegoRezultat
zapisBadaniaTechnicznego	zapisBadaniaTechnicznego	zapisBadaniaTechnicznegoRezultat
zapisAnulowaniaBadaniaTechnicznego	zapisAnulowaniaBadaniaTechnicznego	zapisAnulowaniaBadaniaTechnicznegoRezultat
zapisAnulowaniaPrerejestracji	zapisAnulowaniaPrerejestracji	zapisAnulowaniaPrerejestracjiRezultat

6.1. Metoda pytanieOPojazd

Metoda przyjmuje na wejściu dane pojazdu. Możliwe zakresy danych wejściowych to:

- identyfikatorSystemowyPojazdu lub
- numerPodwoziaNadwoziaRamy
- numerRejestracyjny + dataPierwszejRejestracji lub
- numer rejestracyjny + marka lub
- dokumentSeriaNumer lub
- zagranicznyNumerRejestracyjny

Opcjonalnie można wypełnić pole „dataDanych" i wyszukać pojazd na określony moment czasu.

Metoda zwraca dane znalezionego pojazdu, czyli informacje:

- o dokumencie wraz z adnotacjami urzędowymi i oznaczeniami pojazdu,
- o szkodach istotnych wraz z listą kategorii szkód istotnych,
- o aktualnym stanie pojazdu,
- o ostatniej rejestracji pojazdu,
- o ostatnim pozytywnym badaniu technicznym pojazdu oraz o wszystkich badaniach technicznych negatywnych, wykonanych od ostatniego pozytywnego, wraz z wykazem wykrytych usterek, stanami licznika oraz terminie kolejnego badania technicznego,
- o danych technicznych pojazdu,
- o danych pierwszej rejestracji,
- o homologacji pojazdu,
- o danych pojazdu sprowadzonego,
- o aktualnym wyrejestrowaniu,
- o aktualnym czasowym wycofaniu i zmianie okresu czasowego wycofania.

W razie znalezienia w bazie CEPiK więcej niż jednego pojazdu spełniającego warunki wyszukiwania, zwracane są informacje o wielu pojazdach. Jeżeli liczba pojazdów spełniających kryteria wyszukiwania jest większa od maksimum określonego parametrem konfiguracyjnym, przekazywana jest informacja o błędzie.

Parametr „dataDanych" powinien być zawsze ustawiany na moment rozpoczęcia badania technicznego – należy na to zwrócić uwagę przy zapisie badania technicznego w trybie awaryjnym.

6.2. Metoda pytanieOBadanieTechniczne

Metoda przyjmuje na wejściu następujące dane:

- identyfikatorSystemowyBadaniaTechnicznego, numerBadaniaTechnicznego.

Metoda zwraca informacje o przeprowadzonym badaniu technicznym, o ile badanie o podanych parametrach zostało znalezione w bazie CEPiK i nie było anulowane. Zakres udostępnianych danych obejmuje miedzy innymi:

- szczegółowe dane badania technicznego,
- termin kolejnego badania technicznego,
- stan licznika,
- wykaz stwierdzonych usterek,
- dane niezidentyfikowanego zatrzymanego dokumentu pojazdu

6.3. Metoda zapisPojazduPrerejestrowanego

Metoda przyjmuje na wejściu dane pojazdu prerejestrowanego, w tym podstawowe dane opisujące pojazdu, dane techniczne pojazdu, dane pojazdu sprowadzonego oraz dane pierwszej rejestracji za granicą. Minimalny zakres danych wejściowych to:

- numerPodwoziaNadwoziaRamy, marka, model, rodzaj, Kod czynności „SKP.WRI.CAR.POUT” oraz niektóre dane rejestracyjne, zgodnie z załączoną strukturą komunikatu xsd.

Metoda zwraca nadany identyfikatorSystemowyPojazdu i tokenAktualnosci.

6.4. Metoda zapisBadaniaTechnicznego

Usługa zapis badania technicznego umożliwia:

- zapis nowego badania technicznego
- modyfikację badania technicznego
- przesłanie danych związanych z przerwaniem badania technicznego

6.4.1. Zapis nowego badania technicznego

Wymagane wypełnione pola dla tej czynności:

- kodCzynnosci - „SKP.WRI.BT.P” (dla pozytywnego badania technicznego) lub „SKP.WRI.BT.N” (dla negatywnego badania technicznego)
- podany stan licznika pojazdu
- przynajmniej 1 usterka z grupy usterek istotnych w przypadku negatywnego badania technicznego

- przynajmniej 1 usterka z grupy usterek stwarzających zagrożenie w przypadku negatywnego badania technicznego z zatrzymaniem dokumentu rejestracyjnego

Niedozwolone wypełnienie pola dla tej czynności:

- identyfikatorSystemowyBadaniaTechnicznego
- przyczynaPrzerwaniaBadaniaTechnicznego
- dataGodzWykonaniaBadaniaTechnicznego w trybie online
- żadna z podanych usterek nie jest w grupie usterek istotnych lub stwarzających zagrożenie w przypadku pozytywnego wyniku badania technicznego

6.4.2. Modyfikacja badania technicznego

Wymagane wypełnione pola dla tej czynności:

- identyfikatorSystemowyBadaniaTechnicznego
- kodCzynnosci - „SKP.WRI.BT.P" (dla pozytywnego badania technicznego) lub „SKP.WRI.BT.N" (dla negatywnego badania technicznego)
- dataGodzWykonaniaBadaniaTechnicznego
- podany stan licznika pojazdu
- przynajmniej 1 usterka z grupy usterek istotnych w przypadku negatywnego badania technicznego
- przynajmniej 1 usterka z grupy usterek stwarzających zagrożenie w przypadku negatywnego badania technicznego z zatrzymaniem dokumentu rejestracyjnego

Niedozwolone wypełnienie pola dla tej czynności:

- przyczynaPrzerwaniaBadaniaTechnicznego
- żadna z podanych usterek nie jest w grupie usterek istotnych lub stwarzających zagrożenie w przypadku pozytywnego wyniku badania technicznego

UWAGA: modyfikacja badania technicznego możliwa jest wyłącznie dla tego samego pojazdu, wyjątkiem jest sytuacja, kiedy zostało wykonane anulowanie badania technicznego, wówczas możliwy jest zapis badania technicznego pod tym samym numerem badania technicznego

6.4.3. Przerwanie badania technicznego

Wymagane wypełnione pola dla tej czynności:

- kodCzynnosci - „SKP.INT.BT„
- przyczynaPrzerwaniaBadaniaTechnicznego

6.4.4. Obsługa trybu awaryjnego

W trybie awaryjnym wymagane jest wypełnienie pola dataGodzWykonaniaBadaniaTechnicznego i trybAwaryjny=”true”.

W trybie online pole dataGodzWykonaniaBadaniaTechnicznego powinno być puste i trybAwaryjny=”false”, wyjątkiem jest modyfikacja badania technicznego, w którym pole dataGodzWykonaniaBadaniaTechnicznego jest wymagane.

Wymagalność pozostałych pól danych w komunikatach jest zgodna z załączoną strukturą komunikatu xsd.

6.5. Metoda anulowanieBadaniaTechnicznego

Minimalny zakres danych wejściowych:

- identyfikatorSystemowyBadaniaTechnicznego
- kodCzynnosci „SKP.CAN.BT”

Użytkownik musi posiadać uprawnienia do zmiany danych badania technicznego. W szczególności dana SKP nie może anulować badania technicznego wykonanego przez inną SKP.

Metoda zwraca pola identyfikatorSystemowyPojazdu i tokenAktualnosci oraz identyfikatorSystemowyBadaniaTechnicznego. W przypadku nieudanej próby anulowania zostanie zwrócony błąd zgodny ze strukturą z rodziału 7.

6.6. Metoda anulowaniePrerejestracji

Minimalny zakres danych wejściowych to:

- identyfikatorSystemowyPojazdu
- toeknAktualności
- kodCzynnosci „SKP.CAN.CAR.POUT”

Użytkownik musi posiadać uprawnienia do zmiany danych pojazdu. W szczególności dana SKP nie może anulować prerejestracji wykonanej przez inną SKP.

Metoda zwraca pola identyfikatorSystemowyPojazdu i tokenAktualnosci. W przypadku nieudanej próby anulowania zostanie zwrócony błąd zgodny ze strukturą z rodziału 7.

7. Komunikaty błędów

Struktura komunikatu błędu jest jednakowa dla błędów biznesowych i technicznych. Tabela kodów i komunikatów błędów znajduje się w pliku xls w załączniku.

Poniżej przedstawiono przykładowy komunikat błędu:

```
<S:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Body>
    <env:Fault><faultcode>envServer</faultcode>
          <faultstring>Server fault</faultstring>
          <faultactor>actor</faultactor>
          <detail>
                <exc:cepikException xmlns:exc="http://exceptions.api.cepik.coi.gov.pl">
                      <komunikaty>
                            <typ>WARN</typ>
                            <kod>string</kod>
                            <komunikat>string</komunikat>
                            <szczegoly>string</szczegoly>
                            <identyfikatorBledu>string</identyfikatorBledu>
                      </komunikaty>
                </exc:cepikException>
          </detail>
        </env:Fault>
    </env:Body>
  </env:Envelope>
```

W znaczniku „faultstring” przekazywany jest kod błędu i komunikat rozdzielone dwukropkiem. W przypadku wystąpienia błędu nietypowego zwracany jest ogólny kod błędu -20999. Głównym powodem wystąpienia tego błędu mogą być dane w komunikacie wejściowym, które naruszają ograniczenia w bazie danych. W przypadku zwrócenia kilku błędów, komunikaty są rozdzielone znakiem „|”. Poniżej przykład zawartości znacznika „faultstring” z dwoma zwróconymi błędami:

<faultstring>-20003: Nieznany kod usterki.|-20002: Brak wymaganego stanu licznika pojazdu.</faultstring>