Specyfikacja techniczna interfejsu do obsługi Profilu Kandydata na Kierowcę.

(OE OSK)

12 styczeń 2017 r.

wersja 2.2.0

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 **5**

1. **Cel i zakres dokumentu** **6**
2. **Ogólna charakterystyka interfejsu udostępniania danych dotyczących Profilu Kandydata na Kierowcę** **6**
3. Podłączenie do systemu SI CEPiK **6**
   - 3.1. Podłączenie podmiotów do systemu CEPiK 7
     - 3.1.1. Węzeł Internet 7
     - 3.1.2. Węzeł WAN 8
     - 3.1.3. Połączenie poprzez aplikację centralną dostarczaną dla OSK 8
   - 3.2. Wykorzystane protokoły 8
4. **Uwierzytelnianie, autoryzacja, rozliczalność, integralność transakcji i poufność danych** **9**
   - 4.1. Uwierzytelnianie i autoryzacja 9
   - 4.2. Poufność transmisji danych 9
   - 4.3. Rozliczalność i integralność 9
5. **Wymagania dla systemu zewnętrznego** **10**
   - 5.1. Podpisywanie komunikatów 10
   - 5.2. Walidacja pól w API 10
   - 5.3. Komunikaty błędów 10
   - 5.4. Sprawdzanie dostępności serwisu 11
   - 5.5. Obsługa tokenów aktualności danych 12
6. Specyfikacja metod usługi **12**
   - 6.1. Metoda pytanieOPkk 13
   - 6.2. Metoda zapisRezerwacjaPkk 13
   - 6.3. Metoda zapisUwolnieniePkk 14
   - 6.4. Metoda zapisPrzekazanieDanychKursuKnk 14
   - 6.5. Metoda zapisPrzekazanieDanychEgzaminuKnk 15
7. Słowniki **15**
8. Załączniki **15**

Metryka dokumentu

Tytuł: Specyfikacja techniczna interfejsu wymiany danych - PKK.		Wersja: 2.2.0
Opis: Specyfikacja techniczna interfejsu wymiany danych z systemem CEPiK dla systemów zewnętrznych – OE OSK.		Data utworzenia: 2017-01-12
Autor:	*Centralny Ośrodek Informatyki*	Data wydruku:
Sygnatura:		
Załączniki:	Plik „pkk-oeosk.zip”, zawartość określona jest w p. 8. dokumentu.	

Historia zmian

Wersja	Data	Autorzy	Opis zmian
1.0	2015-07-17	Grzegorz Krupiński Marcin Dłubakowski Adam Kołaciński Radosław Starczynowski	Utworzenie dokumentu
1.1	2015-09-18	Adam Kołaciński Marcin Kubarek	Aktualizacja
1.2	2015-11-10	Adam Kołaciński Artur Szybiak	Aktualizacja opisu komunikatów błędów
1.3	2015-12-21	Magda Gałach	Aktualizacja po uwagach PWPW
1.5.1	2016-02-15	Magda Gałach	Aktualizacja po uwagach PWPW
1.5.2	2016-03-15	Magda Gałach	Aktualizacja po uwagach PWPW
1.6.1	2016-04-08	Magda Gałach	Aktualizacja po uwagach PWPW
1.6.2	2016-04-20	Magda Gałach	Aktualizacja po uwagach PWPW
1.6.3	2016-05-06	Michał Wudarczyk	Aktualizacja dokumentu zgodnie z plikiem PKK_release_notes_06_05_2016
1.9.2	2016-06-01	Michał Wudarczyk	Uspójnienie numeracji dokumentu z aktualną wersją aplikacji
2.1.0	2016-10-24	Michał Wudarczyk	Uspójnienie numeracji dokumentu z aktualną wersją aplikacji

Wersja	Data	Autorzy	Opis zmian
2.2.0	2016-11-23	Michał Wudarczyk	Uspójnienie numeracji dokumentu z aktualną wersją aplikacji
2.2.0	2017-01-12	Michał Wudarczyk	Aktualizacja zapisów w punkcie 3.1.3 Połączenie poprzez aplikację centralną dostarczaną dla OSK

Słownik podstawowych pojęć

Nazwa / skrót	Opis
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
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 Profilu Kandydata na Kierowcę 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 Profilu Kandydata na Kierowcę

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.

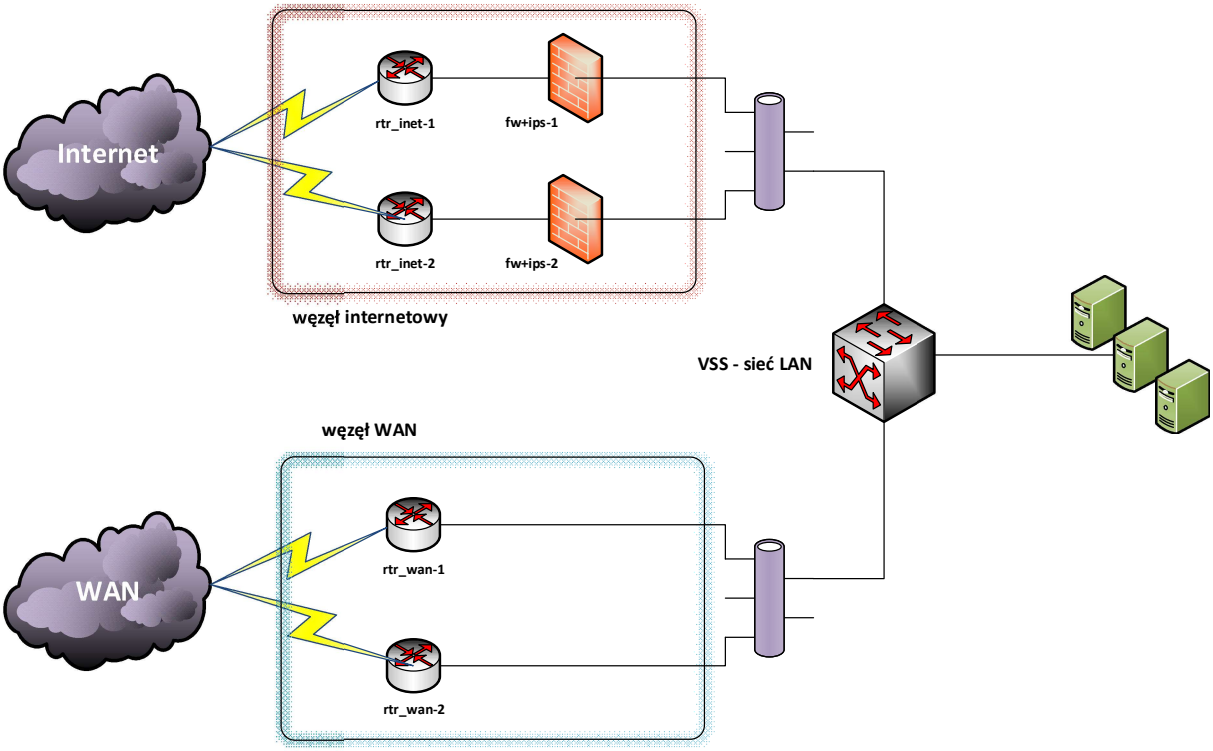
3. Podłączenie do systemu SI CEPiK

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.

3.1. Podłączenie podmiotów do systemu CEPiK

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 (obsługa placówek samorządowych),
- Internet – sieć o niskim stopniu zaufania (obsługa pozostałych podmiotów).



Rysunek 1 Architektura węzła WAN i Internet

3.1.1. 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 użytej metody połączenia, używać będą szyfrowanej transmisji wykorzystującej protokół SSL oraz symetryczny klucz szyfrujący. Do poprawnej komunikacji z systemem tym kanałem wymagane więc będzie wydanie przez MSW certyfikatu niezbędnego do połączenia.

Zalecane będą następujące minimalne parametry połączenia:

1. łącze ze stałym adresem publicznym,
2. łącze symetryczne 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.

3.1.2. Węzeł WAN

W sieci WAN, podobnie jak przy połączeniach z siecią internet, wymagane będzie szyfrowanie transmisji z wykorzystaniem protokołu SSL oraz symetryczny klucz szyfrujący. Do poprawnej komunikacji z systemem tym kanałem wymagane więc będzie wydanie przez MSW certyfikatu niezbędnego do połączenia.

3.1.3. Połączenie poprzez aplikację centralną dostarczaną dla OSK

Połączenie realizowane będzie centralnie pomiędzy CPD dostawcy oprogramowania dla OSK a CPD CEPiK 2.0. Pomiędzy aplikacją centralną dostawcy oprogramowania dla OSK a CEPIK2.0 zestawione zostanie połączenie SSL, zabezpieczone centralnym certyfikatem dostępowym wystawionym dla Portalu. W przypadku podpisów użytkownika utrzymane zostanie obecne rozwiązanie wykorzystujące podpisy kwalifikowane/własne CA SI WORD.

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.

4.1. Uwierzytelnianie i autoryzacja

Uwierzytelnianie odbywać się będzie na dwa sposoby:

1. uwierzytelnienie użytkownika w systemie CEPiK z użyciem dostarczanego na karcie prywatnego certyfikatu zabezpieczonego kodem PIN – w tym przypadku rozliczalność transakcji zapewnia SI CEPiK,
2. uwierzytelnianie użytkownika w systemie zewnętrznym – w tym przypadku uwierzytelnianie odbywa się w systemie zewnętrznym, a następnie system zewnętrzny uwierzytelnia się w SI CEPiK z użyciem wystawionego przez MSW certyfikatu. W przypadku tego typu uwierzytelniana rozliczalność transakcji spoczywa na systemie zewnętrznym, musi więc on zapewnić logowanie wszystkich operacji skutkujących wymianą danych z SI CEPiK wraz z danymi umożliwiającymi jednoznaczne identyfikacje użytkownika w systemie zewnętrznym. Format komunikatu przesyłanego do SI CEPiK wymuszać będzie przekazanie identyfikatora użytkownika (podpisu użytkownika) w systemie zewnętrznym.

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.

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 zewnętrzny 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. 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:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <ns0:Fault xmlns:ns1="http://www.w3.org/2003/05/soap-envelope" xmlns:ns0="http://schemas.xmlsoap.org/soap/envelope/">
      <faultcode>ns0:Server</faultcode>
      <faultstring>-20325: Nie można dodać osoby do CEPIK, ponieważ już istnieje. Spróbuj wyszukać ją po Id podmiotu i numerze wariantu</faultstring>
      <detail>
        <ns0:blad xmlns:ns0="http://pkk.api.cepik.msw.gov.pl">
          <kod>-20325</kod>
          <komunikat>Nie można dodać osoby do CEPIK, ponieważ już istnieje. Spróbuj wyszukać ją po Id podmiotu i numerze wariantu</komunikat>
        </ns0:blad>
```

```
      </detail>
    </ns0:Fault>
  </S:Body>
</S: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:

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <ns0:Fault xmlns:ns1="http://www.w3.org/2003/05/soap-envelope" xmlns:ns0="http://schemas.xmlsoap.org/soap/envelope/">
      <faultcode>ns0:Server</faultcode>
      <faultstring>-20913: KomunikatWalidacjiMiekkiej walidacji miękkiej. Jeżeli jesteś pewny, że pomimo poniższych błedów chcesz dokonać operacji to wyślij te same dane ponownie || -20213 Kandydat nie posiada uprawnień wymaganych kategorii: DICT099_C</faultstring>
      <detail>
        <ns0:bledyWalidacjiMiekkiej xmlns:ns0="http://pkk.api.cepik.msw.gov.pl">
          <bladWalidacjiMiekkiej>
            <kod>-20913</kod>
            <komunikat>KomunikatWalidacjiMiekkiej walidacji miękkiej. Jeżeli jesteś pewny, że pomimo poniższych błedów chcesz dokonać operacji to wyślij te same dane ponownie</komunikat>
          </bladWalidacjiMiekkiej>
          <bladWalidacjiMiekkiej>
            <kod>-20213</kod>
            <komunikat>Kandydat nie posiada uprawnień wymaganych kategorii: DICT099_C</komunikat>
          </bladWalidacjiMiekkiej>
        </ns0:bledyWalidacjiMiekkiej>
      </detail>
    </ns0:Fault>
  </S:Body>
</S:Envelope>
```

5.4. Sprawdzanie dostępności serwisu

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

https://pkk.cepik IP: 185.41.93.105, 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.

5.5. Obsługa tokenów aktualności danych

Tokeny są unikalnymi identyfikatorami w postaci łańcucha znaków, które służą do sprawdzenia podczas zapisu lub modyfikacji, czy dane nie uległy zmianie przez modyfikację danych wykonaną przez innego użytkownika. W przypadku niezgodności tokenu zwracany jest komunikat o nieaktualności tokenu. W takiej sytuacji należy ponowne pobrać dane i dopiero po weryfikacji wykonać zapis lub modyfikację danych przekazując prawidłowy komunikat do usługi. Mechanizm tokenów gwarantuje, że zapis danych możliwy jest wyłącznie w sytuacji, kiedy użytkownik pracował na aktualnych danych .

6. Specyfikacja metod usługi

Dane udostępniane przez interfejs PKK dotyczą prezentacji stanu aktualnego. Historia zmian danych nie jest dostępna za pośrednictwem tego interfejsu. Szczegóły typów danych w komunikatach wejściowych i wyjściowych znajdują się w dokumentach załączonych w punkcie 8.2.

Komunikaty wejściowe i wyjściowe w usługach prezentuje poniższa tabela.

Usługa	Komunikat wejściowy	Komunikat wyjściowy
pytanieOPkk	pkk:pytanieOPkk	pkk:pytanieOPkkRezultat
zapisRezerwacjaPkk	pkk:zapisRezerwacjaPkk	pkk:zapisRezerwacjaPkkRezultat
zapisUwolnieniePkk	pkk:zapisUwolnieniePkk	pkk:zapisUwolnieniePkkRezultat
zapisPrzekazanieDanychKursuKnk	pkk:zapisPrzekazanieDanychKursuKnk	pkk:zapisPrzekazanieDanychKursuKnkRezultat
zapisPrzekazanieDanychEgzaminuKnk	pkk:zapisPrzekazanieDanychEgzaminuKnk	pkk:zapisPrzekazanieDanychEgzaminuKnkRezultat

6.1. Metoda pytanieOPkk

Minimalny zakres danych wejściowych to:

- Numer PKK i numer PESEL kandydata lub
- Numer PKK i data urodzenia kandydata

Dla sprawdzenia można dodatkowo podawać datę urodzenia kandydata.

Metoda zwraca pełną informację o PKK, w tym:

- Dane osobowe kandydata
- Dane o posiadanych uprawnieniach
- Dane o orzeczeniach lekarskich i psychologicznych
- Informacje o przebiegu szkolenia
- Informacje o przebiegu egzaminów
- Kategoria prawa jazdy, której dotyczy PKK
- Powód generowania PKK (np. skierowanie na kontrolne sprawdzenie kwalifikacji)
- Informacje o pozwoleniach opiekunów, zaświadczeniach ze szkół itp.
- Informacja o rezerwacji PKK
- Token aktualności danych PKK.

6.2. Metoda zapisRezerwacjaPkk

Metodę stosuje się zmiany statusu PKK z „Wolny” na „Zarezerwowany do szkolenia” lub „Zarezerwowany do egzaminu”. Dany podmiot może zarezerwować PKK tylko we własnym imieniu.

Minimalny zakres danych wejściowych:

- Rodzaj czynności biznesowej (PKK.Z.PKK.REZ), numer PKK i token aktualności danych PKK

Metoda zwraca:

- Numer PKK
- Nowy token aktualności danych PKK.

6.3. Metoda zapisUwolnieniePkk

Metodę stosuje się zmiany statusu PKK z „Zarezerwowany do szkolenia” lub „Zarezerwowany do egzaminu” na „Wolny”. PKK uwalnia ten podmiot, który go zarezerwował. W szczególnych przypadkach może tego dokonać również starostwo.

Minimalny zakres danych wejściowych:

- Rodzaj czynności biznesowej (PKK.Z.PKK.UWO), numer PKK i token aktualności danych PKK

Metoda zwraca:

- Numer PKK
- Nowy token aktualności danych PKK.

6.4. Metoda zapisPrzekazanieDanychKursuKnk

Metodę stosuje się wprowadzenia danych egzaminu na PKK, w przypadku gdy nie może tego zrobić podmiot egzaminujący.

Minimalny zakres danych wejściowych:

- Rodzaj czynności biznesowej (PKK.Z.KUR.PRZ), dane szkolenia, numer i token aktualności danych PKK.

Dane szkolenia obejmują:

- Numer ewidencyjny instruktora
- Numer ewidencyjny wykładowcy (o ile ma zastosowanie)
- Data rozpoczęcia i zakończenia szkolenia
- Liczbę godzin szkolenia teoretycznego i praktycznego
- Informację o szkoleniu uzupełniającym

Metoda zwraca:

- Numer PKK
- Nowy token aktualności danych PKK.

6.5. Metoda zapisPrzekazanieDanychEgzaminuKnk

Metodę stosuje się wprowadzenia danych egzaminu na PKK przez Ośrodek Egzaminacyjny.

Minimalny zakres danych wejściowych:

- Rodzaj czynności biznesowej: PKK.Z.EGZ.PRZ-PRAK(Przekazanie danych egzaminu części praktycznej KnK) lub PKK.Z.EGZ.PRZ-TEOR(Przekazanie danych egzaminu części teoretycznej KnK), dane egzaminu, numer i token aktualności danych PKK.

Dane egzaminu obejmują:

- Numer ewidencyjny egzaminatora
- Rodzaj egzaminu
- Data przeprowadzenia egzaminu
- Wynik egzaminu

Metoda zwraca:

- Numer PKK
- Nowy token aktualności danych PKK.

7. Słowniki

Specyfikacja słowników i interfejsu odczytu słowników, używanych w API PKK będzie określona w oddzielnym dokumencie.

8. Załączniki

Wszystkie załączniki znajdują się w oddzielnym pliku „pkk-oeosk.zip”, który zawiera następujące składniki:

- PKK-OE-OSK-API.wsdl – specyfikacja usług sieciowych
- pkk-oeosk.xsd i pkk-common.xsd – specyfikacja typów danych użytych w komunikatach
- pkk-oeosk-dokumentacja.html – dokumentacja xsd w postaci html