Ministerstwo Finansów

Krajowa Administracja Skarbowa

Wymogi techniczne i zasady przekazywania danych geolokalizacyjnych niezbędnych do poboru opłaty elektronicznej dla Operatorów OBU i ZSL

Warszawa 21.03.2023

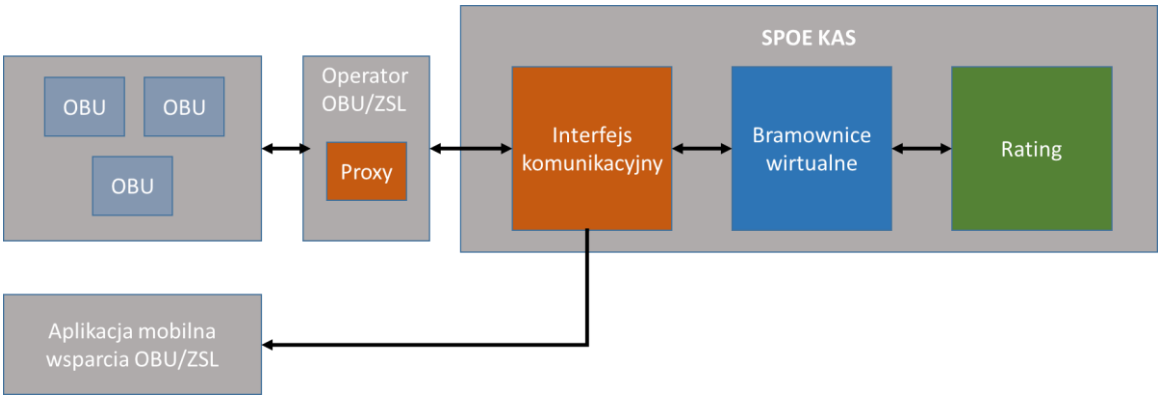
Spis treści

Słownik pojęć

Pojęcie	Opis
Base64	Służy do kodowania ciągu bajtów. Zdefiniowane w RFC 4648.
CSR	(ang. Certificate Signing Request) – prośba o podpisanie certyfikatu, szyfrowana wiadomość przesyłana do wystawcy w procesie starania się o Certyfikat SSL. Podczas generowania CSR tworzony jest także klucz prywatny.
EGNOS	(ang. European Geostationary Navigation Overlay Service) – europejski system wspomagający systemy GPS i GLONASS, a w przyszłości Galileo.
GNSS	(ang. Global Navigation Satetellite System) – globalny system nawigacyjny obejmujący swoim zasięgiem całą Ziemię. Przykładem jest system GPS.
GPS	(ang. Global Positioning System) – amerykański radiowy system nawigacyjny oparty na satelitach.
Jamming	Zagłuszanie sygnału GNSS przez urządzenia elektroniczne.
JSON	(ang. JavaScript Object Notation) – format wymiany danych.
JSON Schema	Definiuje strukturę danych w JSON.
MCC	(ang. Mobile Country Code) – unikatowy numer identyfikujący kraj, w którym działa dana sieć telefonii bezprzewodowej.
MNC	(ang. Mobile Network Code) – unikatowy w obrębie danego kraju numer, identyfikujący sieć (operatora) telefonii bezprzewodowej.
OBE	(ang. On Board Equipment) – komponent systemu poboru opłat zlokalizowany w poruszającym się pojeździe. Może być nim: urządzenia mobilne (wyposażone w nieodpłatne oprogramowanie udostępnione przez KAS), urządzenie nadające do zewnętrznego systemu lokalizacyjnego (ZSL) oraz urządzenia pokładowe (OBU), wykorzystujące technologie pozycjonowania satelitarnego i transmisji danych.
OBU	(ang. On Board Unit) – urządzenie zainstalowane w pojeździe w celu poboru Opłaty Elektronicznej, nadające do systemu Operatora OBU.
Operator	Operator ZSL i/lub Operator OBU.
Operator OBU	Firma zarządzająca usługami OBU.
Operator ZSL	Firma zarządzająca usługami ZSL.
PEM	(ang. Privace Enhanced Mail) – format pliku służący do zapamiętywania i wysyłania kluczy kryptograficznych, certyfikatów i innych danych zdefiniowane w RFC 7468.
PUESC	Platforma Usług Elektronicznych Skarbowo-Celnych
SENT	System Elektronicznego Nadzoru Transportu
SPOE KAS	System Poboru Opłaty Elektronicznej Krajowej Administracji Skarbowej; e-TOLL
Spoofing	Ataki na system teleinformatyczny poprzez podszywanie się pod inny element systemu informatycznego.
SSL	(ang. Secure Socket Layer) – standardowy protokół kryptograficzny wykorzystywany do bezpiecznej transmisji dokumentów przez sieci komputerowe.
TLS	(ang. Transport Layer Security) – protokół kryptograficzny będący standardem w Internecie, zapewnia poufność i integralność transmisji danych, uwierzytelnianie serwera, czasami klienta. Jest rozwinięciem protokołu SSL.
ZSL	Zewnętrzny System Lokalizacji - niezależny od SPOE KAS system, który dostarcza informacji o lokalizacji pojazdów. Są to rozwiązania firm komercyjnych służące do śledzenia położenia i ruchu flot pojazdów.

1 Wstęp

SPOE KAS służy do poboru opłat w oparciu o techniki GNSS. Ustawa z dnia 6 maja 2020 r. o zmianie ustawy o drogach publicznych oraz niektórych innych ustaw definiuje zasady poboru opłat z wykorzystaniem urządzeń mobilnych, zewnętrznych systemów lokalizacyjnych (ZSL) oraz urządzeń pokładowych (OBU). W pojeździe muszą być zainstalowane urządzenia pokładowe OBE (On-Board Equipment). Dane z urządzeń OBE są przekazywane do SPOE KAS za pośrednictwem Operatora OBU lub Operatora ZSL. Możliwe jest również przekazywanie danych lokalizacyjnych za pomocą aplikacji mobilnej **(aplikacja nie jest omawiana w tym dokumencie)**. Na Rys.1 wskazana jest wspomagająca aplikacja mobilna, która może być wykorzystana do wyświetlania informacji zwrotnej z SPOE KAS do kierowcy, np. stan salda. W przypadku OBU z wyświetlaczem jest możliwe przesyłanie komunikatów zwrotnych do OBU poprzez system Operatora. Komunikaty wysyłane są do Operatora OBU, który przesyła je na odpowiednie urządzenia OBU, do których są adresowane. Dane z urządzeń lokalizacyjnych są przesyłane do Serwera Proxy Operatora a następnie przekazywane na interfejs wejściowy SPOE KAS.



Rys. 1 Główne komponenty systemu związane z przekazywaniem danych geolokalizacyjnych

Niniejszy dokument opisuje wymogi techniczne przekazywania danych geolokalizacyjnych niezbędnych do poboru opłaty elektronicznej, w szczególności specyfikację techniczną interfejsu, protokoły komunikacyjne i szyfrujące oraz sposób uwierzytelnienia komunikacji przez Operatora OBU lub Operatora ZSL.

2 Interfejsy rejestracji

Proces rejestracji usług i urządzeń będzie realizowany zgodnie z zasadami szczegółowo opisanymi w Specyfikacjach Technicznych Komunikatów i Interfejsów Komunikacyjnych Operatora ZSL/OBU Specyfikacja dopuszcza rejestrację i aktualizację danych za pośrednictwem interfejsu wizualnego HTML (dedykowane formularze) lub za pośrednictwem usługi niewizualnej web service (SOAP). Komunikacja z wykorzystaniem usług niewizualnych oparta jest o ustrukturyzowane komunikaty xml, zgodne ze specyfikacją wymiany danych z portalem PUESC.

2.1 Rejestracja usług przesyłania danych lokalizacyjnych przez Operatorów

Operator może wybrać zakres świadczonej usługi pod kątem dwóch systemów: SENT oraz SPOE KAS. Usługa może być świadczona na rzecz SENT, SENT oraz SPOE KAS bądź jedynie SPOE KAS. Rejestracja Operatora ZSL lub Operatora OBU składa się z następujących kroków:

a) Operator przesyła do SPOE KAS (za pomocą interfejsu):
   i. wykaz numerów IP serwerów, z których będzie w przyszłości przesyłał dane,
   ii. żądanie wydania certyfikatu SSL/TLS klienta,
   iii. opcjonalnie kompletny adres interfejsu zwrotnego (głównego oraz przeznaczonego do uzyskania tokena JWT autoryzującego komunikację zwrotną według standardu OAuth2.0) oraz dane uwierzytelniające: client id (login), client secret (hasło)), scope (zasięg uprawnień), grant type (rodzaj uprawnień). Szczegóły komunikacji zwrotnej zostały omówione w punkcie 3.10.
   iv. dane kontaktowe do administratora usługi po stronie Operatora,

b) Operator otrzymuje zwrotnie:
   i. zarejestrowany w SPOE KAS numer usługi Operatora,
   ii. adres URL usługi SPOE KAS dedykowany do komunikacji z usługą Operatora (jest to adres indywidualnego interfejsu służącego do wymiany danych z SPOE KAS). W przypadku rejestracji SENT przekazywany jest drugi niezależny interfejs do przekazywania danych geolokalizacyjnych według reguł opisanych w specyfikacji technicznej podłączania urządzeń do tego systemu
   iii. certyfikat SSL/TLS klienta wystawiony przez centrum certyfikacji usługi SPOE KAS;

2.2 Rejestracja przez Operatora urządzeń lokalizacyjnych

Operator dokonuje rejestracji urządzeń lokalizacyjnych ZSL lub OBU w SPOE KAS wykorzystując ich identyfikatory techniczne. W tym celu Operator OBU/ZSL:

a) przesyła do SPOE KAS identyfikatory techniczne urządzeń lokalizacyjnych powiązane z usługą Operatora, przy czym identyfikatory te nie mogą zaczynać się lub kończyć spacją lub innymi białymi znakami,
b) otrzymuje zwrotnie numery biznesowe urządzeń lokalizacyjnych powiązane z identyfikatorami technicznymi tych urządzeń (powiązanie 1 identyfikator techniczny = 1 numer biznesowy urządzenia) oraz hasło (PIN) umożliwiające połączenie urządzenia z aplikacją SPOE KAS.

Operator podczas nadawania w polu „serialnumber" podaje numer techniczny, dla którego został otrzymany identyfikator biznesowy. **Nie należy** wysyłać w polu „serialnumber" wartości otrzymanych identyfikatorów biznesowych. Wartość identyfikatora nie może zawierać spacji ani białych znaków. Zarejestrowanie urządzenia umożliwia skuteczne przekazywanie danych do SPOE KAS (urządzenia są w systemie aktywne i dane poprawnie są przetwarzane przez SPOE KAS). Każdy nowo wygenerowany identyfikator biznesowy (jeżeli usługa została zarejestrowana również jako źródło danych dla systemu SENT) jest propagowany do systemu SENT. Tam oczekuje on na aktywację, która odbywa się poprzez wysłanie (przez przewoźnika) dokumentu przewozowego SENT, w którym w polu lokalizator główny

bądź zapasowy znajdzie się ten numer biznesowy. Do tego momentu dane w SENT będą przez system SENT odrzucane z komunikatem „unknown-device”.

3 Komunikacja Proxy Serwer <-> SPOE KAS

3.1 Przekazywanie przez Operatora ZSL lub Operatora OBU danych lokalizacyjnych z urządzeń wskazanych przez Użytkownika końcowego do SPOE KAS

Operator ZSL lub Operator OBU przekazuje do SPOE KAS dane lokalizacyjne z urządzeń wskazanych przez Użytkownika końcowego:

a) do usługi dostępnej pod adresem przekazanym zwrotnie w trakcie rejestracji usługi lokalizacyjnej Operatora,
b) za pomocą protokołu HTTPS autoryzując się wydanym certyfikatem klienta,
c) z użyciem mechanizmu REST i metody HTTP POST w formacie JSON, zgodnym z aktualnym schematem zwanym dalej JSON Schema.

Koszty transmisji danych pozostają po stronie użytkownika i są zależne od wybranego Operatora.
Operator ZSL lub Operator OBU zobowiązuje się przekazywać dane zgodnie z niniejszymi wymogami technicznymi, jednocześnie przyjmuje do wiadomości, że nie spełnienie tych wymogów może skutkować stwierdzeniem naruszenia przepisów przez użytkowników urządzeń udostępnianych przez Operatora, a w konsekwencji regresji opłat z tytułu w/w naruszeń.

3.2 Przekazywane dane lokalizacyjne

Rekord danych lokalizacyjnych składa się z parametrów zawartych w tabeli (Tabela 1).

Tabela 1 Zestawienie parametrów wchodzących w skład rekordu lokalizacyjnego – Szczegółowe informacje o dopuszczalnych wartościach parametrów znajdują się w Tabeli 2

Parametr	Opis	Status parametru
dataID	identyfikator rekordu danych lokalizacyjnych (unikalny dla urządzenia)	obowiązkowy
serialNumber	identyfikator techniczny urządzenia	obowiązkowy
latitude	szerokość geograficzna	obowiązkowy
longitude	długość geograficzna	obowiązkowy
altitude	wysokość nad poziomem morza	opcjonalny (uwaga 1)
fixTimeEpoch	stempel czasu zebrania danych lokalizacyjnych (czas bezwzględny UTC)	obowiązkowy
gpsSpeed	prędkość	obowiązkowy
accuracy	błąd przekazania danych lokalizacyjnych	opcjonalny (uwaga 1)
gpsHeading	azymut	obowiązkowy

eventType	klasa zdarzenia, (jedna z poniższych wartości): ○ lokalizacja (location), ○ włączenie urządzenia (turnon) - zazwyczaj wiąże się z wciśnięciem przycisku; jeżeli takiego przycisku nie ma, często włączeniem jest podłączenie do zasilania; czasem urządzenie jest zawsze włączone, wtedy zalecane jest generowanie zdarzenia „*startjourney*" po zmianie pozycji pojazdu po dłuższym czasie bezruchu, ○ wyłączenie urządzenia (turnoff) – analogicznie do włączenia urządzenia, ○ początek trasy (startjourney) - wykrycia zmiany pozycji po okresie bezruchu, najczęściej jest to pół godziny, ○ zakończenie trasy (endjourney) - dotarcie do punktu docelowego, może to być również jednoznaczne z wyłączeniem stacyjki, ○ odłączenie od zasilania (plugout), ○ podłączenie do zasilania (plugon), ○ GSM online (gsmonline) – zasięg GSM większy od 0, ○ GSM offline (gsmoffline) – zasięg GSM równy 0, ○ GNSS online (gpsonline) – liczba widocznych satelitów co najmniej 3, ○ GNSS offline (gpsoffline) – liczba widocznych satelitów poniżej 3, ○ jamming, ○ spoofing – zdarzenie oznaczająca próbę podania się za inne urządzenie i wysyłania nieprawdziwych danych; z uwagi, iż nie każde urządzenie jest w stanie wykryć takie włamanie	opcjonalny (uwaga 2)
lac	lac - Location Area Code (identyfikator obszaru, w ramach którego Cell id jest unikalne)	opcjonalny (uwaga 1)

mcc	mcc – Mobile Country Code	opcjonalny (uwaga 1)
mnc	mnc – Mobile Network Code	opcjonalny (uwaga 1)
mobileCellId	cid - identyfikator obszaru komórki GSM (Cell id)	opcjonalny (uwaga 1)
satellitesForFix	liczba satelitów użytych do ustalenia pozycji	obowiązkowy
satellitesInView	liczba widocznych satelitów	opcjonalny (uwaga 1)

Uwaga 1: zgodnie z pkt 3.4 pole nie jest obowiązkowe, jednak należy je zawrzeć w rekordzie danych jeśli jest taka możliwość.
Uwaga 2: parametr nie jest wymagany o ile ma wartość inną niż **lokalizacja (location), która jest obowiązkowa do podania w ramach klas zdarzeń** lub wartość **spoofing**, która jest opcjonalna, ale zalecana do umieszczenia w rekordzie.

Dokładna specyfikacja pól została przedstawiona w rozdziale 3.4.
Naliczenia opłaty za przejazd odcinkiem płatnym są generowane wyłącznie na podstawie śladu pojedynczych lokalizacji odebranych z interfejsu (zdarzeń typu „**location**). Dane muszą posiadać stempel czasowy UTC odpowiadający momentowi pobrania współrzędnych lokalizacji. Dane lokalizacyjne powinny być przekazywane niezwłocznie po ich pobraniu. W przypadku wystąpienia awarii, która skutkuje przerwą w przesyłaniu danych geolokalizacyjnych, konieczne jest ich niezwłoczne przesłanie po usunięciu awarii. Wymaga to uprzedniego przekazania informacji o takim zdarzeniu na skrzynkę operatorzyOBUZSL@mf.gov.pl.
Dane lokalizacyjne przekazane do SPOE KAS przez Operatora ZSL/OBU **w czasie dłuższym niż 10 dni po ich pobraniu NIE BĘDĄ PRZETWARZANE** do naliczenia opłat za przejazdy odcinkami dróg płatnych. Operator ZSL/OBU posiadający skonfigurowaną komunikację zwrotną, w przypadku przesłania danych w czasie powyżej 10 dni od daty wygenerowania zdarzenia, otrzyma komunikat: „the data will not be used for billing users”.

3.3 Częstotliwość przesyłania danych

Operator ZSL, Operator OBU **MUSI** przekazywać dane do SPOE KAS z częstotliwością **1 pakiet danych na jedną minutę (60 sekund)**. Pakiet danych zawiera dane lokalizacyjne oraz wygenerowane na poziomie OBE zdarzenia (takie jak włączenie zapłonu, rozpoczęcie jazdy, zatrzymanie, wyłączenie itp., zgodnie z pkt. 3.2). Dane lokalizacyjne **MUSZĄ** być zbierane z częstotliwością **1 lokalizacja na 5 sekund**. Operator w jednym pakiecie może wysyłać dane wielu urządzeń.
Częstotliwość zbierania i przekazywania danych jest warunkiem koniecznym i nie podlega zmianom.

3.4 Struktura JSON

Dane przekazywane będą w postaci tablicy JSON, w której poszczególne elementy są obiektami JSON zawierającymi pojedyncze punkty zapisu trasy. Opis poszczególnych pól, reguły walidacji i informacja o wymagalności pól w Schema_SPOE_v_1_0 przedstawia Tabela 2.

Tabela 2. Schema_SPOE_v_1_0

Nazwa	Opis	Reguła walidacji	Wymagane
dataId		"type": "string",	Tak

Nazwa	Opis	Reguła walidacji	Wymagane
	Unikalny i inkrementowany (na poziomie OBE) identyfikator rekordu w systemie źródłowym, zmienna stosowana dla potrzeb weryfikacji w okresie testów oraz przydatna do sortowania – uzupełniania danych gdy paczki nie będą wysyłane w kolejności.	minLength": 1,"maxLength": 32, "examples": ["1", "1960472"]	
serialNumber	Unikalny identyfikator lokalizatora, dozwolona maksymalna długość 50 znaków, dozwolone są małe i wielkie litery łacińskie z przedziałów (a-z) i (A-Z), cyfry (0-9) oraz znaki myślnik-minus (ang. hyphen-minus) (-) i podkreślenie (ang. underscore) (_), które stanowią podzbiór znaków ASCII (ang. American Standard Code for Information Interchange). Wielkość liter nie jest rozróżniana.	"type": "string", "minLength": 1, "maxLength": 50, "pattern": "^[a-zA-Z0-9\-_]{1,50}$", "examples": ["00000000000B1", "35A058060495422C7934"]	Tak
latitude	Szerokość geograficzna pobrana z nadajnika GNSS, system odniesienia WGS 84, zalecana minimalna liczba miejsc po przecinku: 6, dozwolona maksymalna liczba miejsc po przecinku: 10.	"type": "number","minimum": -90.0, "maximum": 90.0, "multipleOf": 0.0000000001, "examples": [52.0375868826, 52.172644]	Tak
longitude	Długość geograficzna pobrana z nadajnika GNSS, system odniesienia WGS 84, zalecana minimalna liczba miejsc po przecinku: 6, dozwolona maksymalna liczba miejsc po przecinku: 10.	type": "number","minimum": -180.0, "maximum": 180.0, "multipleOf": 0.0000000001, "examples": [21.1956136, 20.026094]	Tak
altitude	Wysokość elipsoidalna pobrana z nadajnika GNSS, jednostka [m], dozwolona maksymalna liczba miejsc po przecinku: 2.	"type": ["number", "null"], "minimum": -1000.0, "maximum": 4000.0, "multipleOf": 0.01, "examples": [10.0, 200.02]	Nie
fixTimeEpoch	Stempel czasowy zawierający datę i czas pobrane z nadajnika GNSS, skojarzone z pozycją geograficzną z danego rekordu, strefa czasowa UTC, stempel czasowy SPOE KAS posiada format zbliżony do Epoch / Unix Timestamp, ale podany z dokładnością do mikrosekundy (16 cyfr), jest to zatem liczba mikrosekund, które upłynęły od '00:00:00 Coordinated Universal Time (UTC), Czwartek, 1 Stycznia 1970', minimalna wartość wskazuje na 2017.09.20 00:00:00 UTC, liczba całkowita.	type": "integer", "minimum": 1505865600000000, "examples": [1506086623000000, 1511273867317000]	Tak

Nazwa	Opis	Reguła walidacji	Wymagane
gpsSpeed	Prędkość przemieszczania się pobrana z nadajnika GNSS - jednostka [m/s], dozwolona maksymalna liczba miejsc po przecinku: 2.	"type": "number", "minimum": 0.0, "maximum": 56.0, "multipleOf": 0.01, "examples": [3.21, 20.0]	Tak
accuracy	Dokładność lokalizacji pobrana z nadajnika GNSS - promień okręgu w metrach, dozwolona maksymalna liczba miejsc po przecinku: 2.	"type": "number", "minimum": 0.0, "multipleOf": 0.01, "examples": [10.14, 30.0]	Nie
gpsHeading	Azymut - jednostka [stopień], dozwolona maksymalna liczba miejsc po przecinku: 2.	"type": "number", "minimum": 0.0, "maximum": 360.0, "multipleOf": 0.01, "examples": [40.14, 230.0]	Tak
eventType	typ zdarzenia	„type”: „string” „enum”: ['turnon', 'turnoff', 'startjourney', 'endjourney', 'plugout', 'plugon', 'gsmonline', 'gsmoffline', 'gpsonline', 'gpsoffline', 'jamming', 'spoofing', ‘location’]	Tak
lac	Identyfikator obszaru stacji bazowej GNSS	„type”: „string” „pattern”: "^[A-Fa-f0-9]{4}$"	Nie
mcc	identyfikator kraju operatora GSM	„type”: „string” „pattern”: "^[0-9]{3}$"	Nie
mnc	identyfikator sieci operatora GSM	„type”: „string” „pattern”: "^[0-9]{2,3}$"	Nie
mobileCellId	identyfikator komórki sieci GNSS	„type”: „string” „pattern”: "^[A-Fa-f0-9]{ 9}$"	Nie
satellitesForFix	liczba satelitów użytych do ustalenia pozycji	„type”: „integer „maximum”: 90 „minimum”: 0	Tak
satellitesInView	liczba widocznych satelitów podczas ustalenia pozycji	„type”: „integer” „maximum”: 90 „minimum”: 0	Nie

Dane lokalizacyjne muszą być przesyłane z urządzeń pokładowych wykorzystujących EGNOS (European Geostationary Navigation Overlay Service). System ten znacznie zwiększa dokładność i wiarygodność pozycji uzyskiwanej z GPS, co ma szczególne znaczenie dla SPOE KAS. Ponadto odrzucane są dane, których współrzędne są poza obszarem Polski. Reguły przedstawiono w **Tabela 3**.

Tabela 3. Reguły odrzucania danych spoza Polski

Kod reguły	Reguła	Uwagi
B-W06	Jeśli lon < 14.116667	Odrzucanie danych gdy długość geograficzna jest mniejsza niż 14.116667. Dotyczy granicy zachodniej.
B-S06	Jeśli lat <49.0	Odrzucanie danych gdy szerokość geograficzna jest mniejsza niż 49.0. Dotyczy granicy południowej.
B-E06	Jeśli lon>24.15	Odrzucanie danych gdy długość geograficzna jest większa niż 24.15 dotyczy granicy wschodniej

B-N06	Jeśli lat > 54.835778	Odrzucanie danych gdy szerokość geograficzna jest większa niż 54.835778. Dotyczy granicy północnej.
L-SSW-CZ	Jeśli współrzędne geograficzne spełniają warunek: 54.9 - lat - 0.3 * lon > 0	Odrzucanie danych na południowym-zachodzie. Dotyczy granicy z Czechami.
L-ESE-UA	Jeśli współrzędne geograficzne spełniają warunek: 1.25 * lon + 20.375 - lat > 0	Odrzucanie danych na południowym-wschodzie. Dotyczy granicy z Ukrainą.
S-NE-RU	Jeśli współrzędne geograficzne spełniają warunek: lon > 19 AND lat > 54.5	Odrzucanie na danych na północnym –wschodzie. Dotyczy granicy z Federacją Rosyjską.

3.5 Metoda przekazywania danych

Dane do interfejsu danych SPOE KAS przesyłane będą z użyciem mechanizmu REST przy użyciu HTTPS i metody HTTP POST. Przesyłane dane należy zawrzeć w strukturze JSON zgodnej ze schematem JSON opisanym w niniejszym dokumencie. Każda próbka danych zebrana podczas pojedynczego pomiaru, która zawiera dane lokalizacyjne zebrane w tym samym czasie (data i godzina pozyskania współrzędnych – stempel czasowy zawierający datę i czas) jest przekazywana jako pojedynczy obiekt JSON. W celu ograniczenia liczby przekazywanych pakietów danych, dane z jednego pojazdu lub z różnych pojazdów zapisane w ramach obiektu JSON przesyła się jako elementy tablicy JSON, która tworzy pojedynczy pakiet danych. Pojedyncza tabela JSON może zawierać od jednego do 10.000 obiektów JSON.

Maksymalna dopuszczalna wielkość pojedynczego pakietu wyrażona w bajtach wynosi 5 MB (słownie: pięć megabajtów). Natomiast po otrzymaniu pakietu, którego wielkość przekracza 2 MB, przesyłane jest zwrotnie do Operatora ZSL/OBU ostrzeżenie (umieszczone w potwierdzeniu otrzymanego pakietu danych). Ostrzeżenie to informuje Operatora, że powinien on przygotować się do optymalizacji mechanizmu wysyłki danych lokalizacyjnych do SPOE KAS, aby uniknąć przekroczenia maksymalnej wielkości pojedynczego pakietu, jeśli wzrośnie liczba przesyłanych danych lokalizacyjnych.

3.6 Bezpieczeństwo przesyłanych danych

Przesyłanie danych do interfejsu wejściowego (pierwszy etap przetwarzania strumieniowego) SPOE KAS realizowane będzie tylko z użyciem certyfikatów. Zestaw zabezpieczeń obejmuje:

- dedykowany interfejs URL,
- ograniczenie w dostępie dla wskazanych IP,
- TLS 1.2 oraz TLS 1.3 (komunikacja zwrotna realizowana jest z wykorzystaniem TLS 1.2),
- autoryzacje z użyciem certyfikatu klienta.

3.7 Walidacja danych - obowiązki po stronie Operatora ZSL i Operatora OBU

Operator jest zobowiązany do walidacji pakietu danych z użyciem aktualnie obowiązującego schematu JSON przed przystąpieniem do jego przekazywania do interfejsu danych SPOE KAS. Walidację należy przeprowadzić z użyciem oprogramowania obsługującego walidację opartą o schematy zgodne z wersją specyfikacji JSON Schema podaną w Schemacie JSON interfejsu danych SPOE KAS. Aktualnie obowiązujący schemat JSON interfejsu danych SPOE KAS jest zgody ze specyfikacją Schema JSON Draft-06 (http://json-schema.org/draft-06/schema#).

Ponadto, Operator samodzielnie musi weryfikować reguły z Tabela 3 i odrzucać dane niespełniające kryteriów zawartych w Tabela 3. Tym samym Operator powinien separować zbędne dane i wysyłać do systemu SPOE KAS **tylko** dane z Polski.
Nie dopuszcza się powtórnego przesyłania danych lokalizacyjnych przez Operatora w przypadku, gdy wcześniej odbiór tych danych został potwierdzony ze strony SPOE KAS. Wyjątkiem od tej zasady są awarie zgłoszone przez Operatora na adres operatorzyOBUZSL@mf.gov.pl.
Dane lokalizacyjne powinny być przesyłane do SPOE KAS w kolejności ich wytworzenia. Powtórne przekazanie danych wiąże się z możliwością wielokrotnego naliczenia opłaty za przejazd.

3.8 Lista komunikatów dla Operatora ZSL i Operatora OBU

Jeżeli chodzi o walidacje danych, to podstawową zasadą jest, że dowolny pakiet, który nie został przyjęty powinien zostać przesłany ponownie, o ile nie jest sprzeczny z JSON Schema, a wówczas należy go poprawić (o ile jest to możliwe) i przesłać ponownie (pakiety nienaprawialne należy pominąć).

Tabela 4 zawiera najczęściej występujące komunikaty w procesie walidacji danych.

Tabela 4. Lista najczęściej pojawiających się komunikatów

Komunikat	Reguła/ Ostrzeżenie	Działanie Operatora
HTTP 200 JSON: {"result": "OK"}	potwierdzenie poprawnej walidacji przesłanego pakietu JSON	Nie wymagane.
400 Bad Request	dostarczony pakiet danych nie jest zgodny z obowiązującym schematem JSON lub nie spełnia żadnych innych wymagań	Cały pakiet jest odrzucony, Operator musi wyeliminować ramki danych nie spełniające schematu JSON oraz przesłać pakiet ponownie
	Pakiet przesłany jest jako pojedynczy obiekt JSON	Obiekt należy przesłać jako listę
	jeżeli któryś z pojedynczych pakietów zostanie odrzucony,	to należy go przesłać po skorygowaniu błędu lub pominąć.
401 Unauthorized	dane nie zostały dostarczone z powodu błędu autoryzacji	Operator musi sprawdzić co się stało.
	Nie znaleziono certyfikatu do uwierzytelniania	Należy dołączyć certyfikat
	Błędny klucz prywatny użyty do weryfikacji certyfikatu	Należy dołączyć odpowiedni klucz użyty do wygenerowania żądania wygenerowania certyfikatu
	Błędny protokół użyty do komunikacji (http zamiast https)	Należy użyć odpowiedniego protokołu transmisji
415 Unsupported media type	Błąd walidacji ramki	Należy poprawić strukturę ramki danych przychodzących
500 Internal Server Error -		należy ponawiać próbę do skutku. Zespół SPOE KAS musi zostać poinformowany o takim przypadku.
503 Service Unavailable —	usługa niedostępna	Operator powinien powtarzać próbę dostarczenia danych aż

		do skutku. Zespół SPOE KAS powinien zostać powiadomiony w takiej sytuacji.
404 Błędny adres	Zasób niedostępny	Należy zweryfikować adres docelowy interfejsu wejściowego

UWAGA:
"result": "OK" informuje, że dane są poprawne w sensie składniowym (spełniają schemę).
Każdy z warningów (ostrzeżeń) jest niezależnym wynikiem reguły biznesowej. Pole „action" określa, jaki skutek na dane wskazane w ostrzeżeniu ma dana reguła. Reguły z akcją „drop" mają wyższy priorytet niż te z akcją „pass". Otrzymanie zwrotnego komunikatu „result": „OK" jest równoznaczne ze skutecznym przesłaniem danych do SPOE KAS.

Reguły „drop" występują w przypadku:
1) niezarejestrowanych urządzeń (brak przypisanego identyfikatora biznesowego),
2) danych spoza Polski.

W przypadku niespełnienia jednej z wyżej wymienionych reguł należy traktować dane jako niespełniające wymagań do przetwarzania. Jest to równoznaczne z brakiem przekazywania danych geolokalizacyjnych do SPOE KAS.

3.9 Informacje konieczne do podłączenia Operatora ZSL lub Operatora OBU do SPOKE KAS

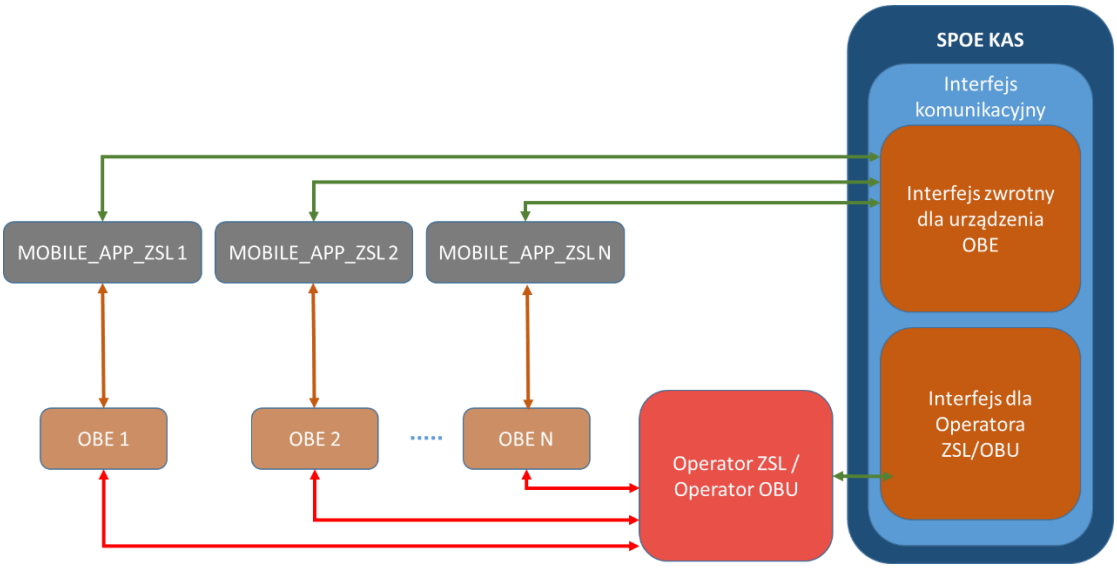
Podłączenie Operatora ZSL lub Operatora OBU do SPOE KAS wykorzystuje certyfikaty i oparte jest o formularze dedykowanego portalu SPOE KAS.

Podsumowanie niektórych szczegółów technicznych, które należy przekazać Operatorowi ZSL lub Operatorowi OBU:

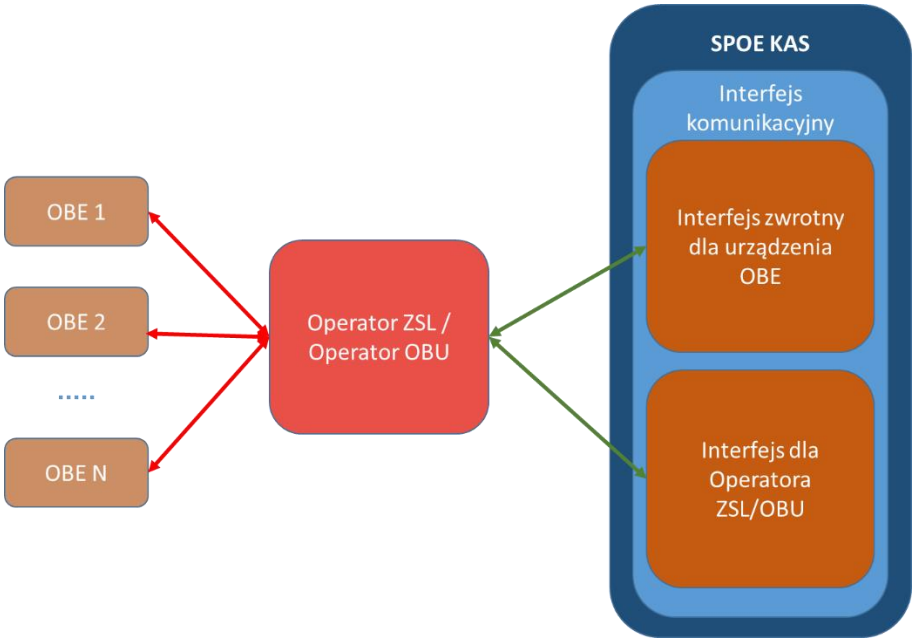
A. interfejsy danych SPOE KAS akceptują dane geolokalizacyjne dostarczane przez mechanizm REST-JSON oparty na protokole HTTPS z metodą HTTP POST;
B. dostarczone dane muszą być wyposażone w struktury danych JSON, które są kompatybilne z aktualnym schematem JSON – SPOE KAS. Interfejs danych SPOE KAS sprawdza poprawność dostarczonych danych względem obowiązkowego schematu JSON i odrzuca wszelkie niezgodne dane;
C. JSON Schema pozwala dostarczać dane w pakietach danych, każdy pakiet może zawierać do 10.000 (słownie dziesięć tysięcy) pozycji geolokalizacyjnych dla różnych urządzeń geolokalizacyjnych lub dla tego samego urządzenia geolokalizacyjnego.

3.10 Komunikacja zwrotna pomiędzy SPOE KAS a Operatorami ZSL i Operatorami OBU

W komunikacji zwrotnej rozróżniane są dwa podstawowe kanały: kanał z Operatorem ZSL lub Operatorem OBU oraz kanał z użytkownikiem końcowym. W przypadku kiedy OBE wyposażone jest w wyświetlacz, komunikaty przekazywane są do Operatora, który według podanego identyfikatora, przekierowuje wiadomości na odpowiednie urządzenie. Gdy OBE nie posiada wyświetlacza, możliwe jest powiązanie OBE z aplikacją mobilną SPOE KAS odbierającą komunikaty i wyświetlającą je użytkownikowi, zwłaszcza w przypadku urządzeń ZSL. Powiązanie to jest realizowane po stronie backend-u aplikacji mobilnej. W tym przypadku komunikaty przekazywane są do aplikacji mobilnej.



Rys. 2a Komunikacja zwrotna – OBE bez wyświetlacza



Rys. 2b Komunikacja zwrotna – OBE z wyświetlaczem

W SPOE KAS przewidziano wdrożenie kanału niewizualnego pozwalającego na odbiór komunikatów zwrotnych. Jako protokół transmisji jest w tym celu wykorzystywany asynchroniczny interfejs oparty na protokole HTTPS, który wykorzystuje uwierzytelnianie przy wykorzystaniu standardu OAuth 2.0. Komunikaty wysyłane są na zdefiniowany adres IP, który po stronie Operatora ZSL / Operatora OBU jest dedykowany w tym celu.

3.10.1 Komunikaty zwrotne na OBE – struktura komunikatów o ostrzeżeniu

Każdorazowo po otrzymaniu ramki z danymi, dane są walidowane. W przypadku kiedy każda dana lokalizacyjna przejdzie poprawnie walidację zwracany jest komunikat ogólny klasy 200. W przypadku kiedy wybrany rekord wygeneruje kod błędu, zwracana jest dodatkowo dla każdego błędnego rekordu informacja o błędzie. Błąd może powodować odrzucenie danej („action”: „drop”), lub ostrzeżenie które umożliwia dalsze przetwarzanie danej („action”: „pass”). Komunikacja zwrotna ma na celu przekazanie informacji o saldzie oraz komunikaty ostrzeżeń wykryte podczas przetwarzania strumieniowego

systemu. Komunikat o wykrytym ostrzeżeniu posiada strukturę przedstawioną poniżej (format YAML OpenAPI 3.0).

```
WarningResponse:
    type: object
    additionalProperties: true
    required:
    - subcode
    - message
    properties:
     subcode:
       type: string
       format: string20
     message:
       type: string
       format: string4096
     objectExample:
       type: object
       required:
       - eventType
       - fixTimeEpoch
       - gpsHeading
       - gpsSpeed
       - latitude
       - longitude
       - mcc
       - mnc
       - satellitesForFix
       - serialNumber
       - dataId
       - altitude
       properties:
         eventType:
           type: string
           format: enumEventType
           enum: [
             location,
             turnon,
             turnoff,
             startjourney,
             endjourney,
             plugout,
             plugon,
             gsmonline,
             gsmoffline,
             gpsonline,
             gpsoffline,
             jamming,
             soofing
           ]
           description: typ zdarzenia
         fixTimeEpoch:
```

```
  type: integer
  format: int64
  example: [1506086623000000, 1511273867317000]
  description: stempel czasowy zebrania danej lokalizacyjnej w postaci Epoch
  minimum: 1500000000
gpsHeading:
  type: number
  format: numberP5S2
  minimum: 0
  maximum: 360
  description: azymut astronomiczny
gpsSpeed:
  type: number
  format: numberP5S2
  minimum: 0
  maximum: 56
  description: prędkość
latitude:
  type: number
  format: numberP13S10
  description: szerokość geograficzna
  example: 58.0123456789
longitude:
  type: number
  format: numberP13S10
  description: długość geograficzna
  example: 21.0123456789
lac:
  type: string
  format: string20
  description: identyfikator stacji bazowej GSM
mcc:
  type: string
  format: string3
  pattern: "^[0-9]{3}$"
  description: identyfikator kraju operatora GSM
mnc:
  type: string
  format: string3
  pattern: "^[0-9]{2,3}$"
  description: identyfikator sieci operatora GSM
mobileCellId:
  type: string
  format: string11
  pattern: "^[A-Fa-f0-9]{9}$"
  description: identyfikator komórki sieci GSM
satellitesForFix:
  type: integer
  format: int64
  description: liczba satelitów użytych do ustalenia pozycji
satellitesInView:
  type: integer
```

```
  format: int64
  description: liczba widocznych satelitów podczas ustalenia pozycji
serialNumber:
  type: string
  format: string50
  maxLength: 50
  description: identyfikator OBE unikalny w ramach NKSPO
dataId:
  type: string
  format: string50
  maxLength: 50
  description: identyfikator pojedynczej danej lokalizacyjnej unikalny na poziomie OBE
accuracy:
  type: number
  format: numberP13S8
  minimum: 0
  example: [10.14, 30.0]
  description: dokładność pomiaru wyliczona na poziomie urządzenia
altitude:
  type: number
  format: numberP13S8
  minimum: -1000
  maximum: 4000
  example: [10.0, 200.0]
  description: dokładność pomiaru wyliczona na poziomie urządzenia
```

3.10.2 Komunikaty zwrotne na OBE – struktura informacji o saldzie

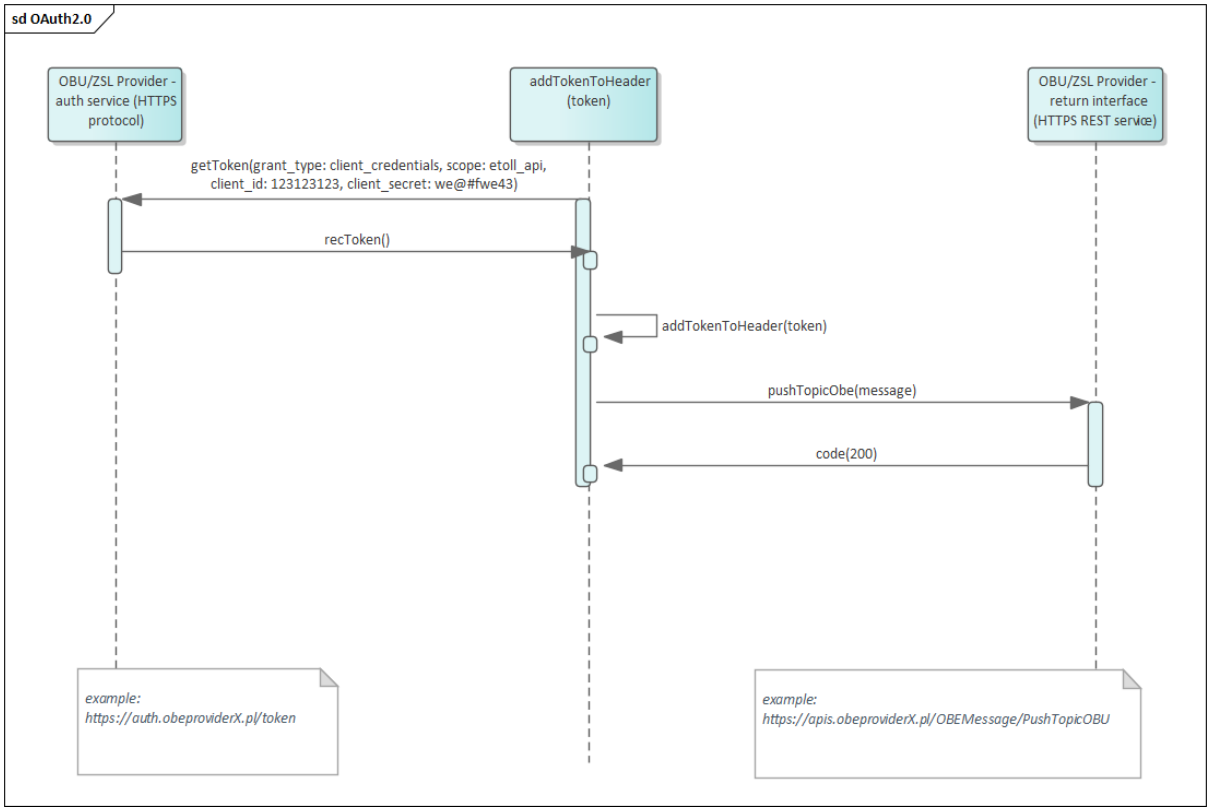
Urządzenie OBE, które nie posiada możliwości wyświetlania komunikatów, może być powiązane z aplikacją mobilną SPOE KAS umożliwiającą odbiór i wyświetlanie komunikatów kierowanych do tego urządzenia. Komunikaty dotyczą aktualnego stanu salda, informacji o przejechanym odcinku płatnym czy statusu rejestracji urządzenia. Powiązanie jest realizowane na poziomie usług związanych z modułem obsługi klienta, gdzie poprzez portal internetowy użytkownik logując się na swoje konto dokonuje powiązania OBE z aplikacją mobilną SPOE KAS, która posiada swój unikalny identyfikator biznesowy. W przypadku, gdy urządzenie nadające jest wyposażone w wyświetlacz, według odpowiedniej specyfikacji komunikat zawierający wiadomość dla odpowiedniego OBE jest wysyłany do Operatora ZSL lub Operatora OBU, skąd wiadomość jest przekazywana na docelowe urządzenie. Zawartość komunikatu zwrotnego opisana jest według następującego schematu:

```
{
        "priority": {
                "type": "string",
                "maxLength": 8,
                "description": "atrybut określający wagę/istotność komunikatu"
        },
        "serialNumber": {
                "type": "integer",
                "format": "int64",
                "description": "identyfikator OBE unikalny w ramach SPOE KAS "
        },
        "systemId": {
                "type": "integer",
```

```
                "format": "int64",
                "maximum": 2000,
                "description": "identyfikator systemu w ramach którego nadaje OBE"
        },
        "message": {
                "type": "string",
                "maxLength": 50,
                "description": "treść komunikatu na urządzenie zawierająca informacje na temat
zdarzenia naliczenia opłaty oraz stanu salda dla umów typu pre-paid"
        },
        "billingAccountId":{
                "type": "integer",
                "format": "int64",
                "example": 1,
                "multipleOf": 1,
                "description": "identyfikator konta bilingowego"
        },
        billingAccountBalance:{
                "type": "string"
                "format": "money"
                "description": "kwota pieniężna wartości salda po naliczeniu opłaty"
                "example": "7.85"
                "minLength": 4
                "maxLength": 16
                "pattern": "^-{0,1}\d{1,12}\.\d{2}$"
        }
}
```


3.10.3 Komunikaty zwrotne na OBE – specyfikacja i konfiguracja OAuth2.0

W celu udrożnienia komunikacji zwrotnej należy po stronie Operatora skonfigurować zabezpieczenia komunikacji zgodne ze standardami OAuth2.0. Diagram sekwencji dla komunikacji został przedstawiony poniżej:



Rys. 3 Diagram sekwencji wymiany wiadomości z wykorzystaniem standardu OAuth 2.0

Na etapie rejestracji usługi Operator deklaruje, czy będzie wykorzystywał komunikację zwrotną oraz uzupełnia niezbędne dane, jak opisano w punkcie 2.1. W celu zestawienia połączenia dla komunikacji zwrotnej należy podać adresy URL dla:

- endpoint-u docelowego dla komunikacji zwrotnej
- endpoint-u do wygenerowania tokena

Wartości dla parametrów dla usługi generującej token:

- grant_type (wartość „client_credentials”)
- scope (wartość „etoll_api”)
- client_id (max 100 znaków)
- client_secret (max 100 znaków)

Przykład (x-www-form-urlencoded):
curl -vv -k -X POST -H "Content-Type: application/x-www-form-urlencoded" -d "grant_type=client_credentials&scope=etoll_api&client_id=my_client_id&client_secret=my_client_secret" https://operator/token/endpoint/

Atrybuty które powinny zostać zwrócone w strukturze json:

- - access_token (w standardzie JWT (header oraz w payload wymagany jest atrybut ‘exp’ w formacie Epoch w przyszłości, na przykład 1634639693))
- - expires_in (najlepiej stały czyli 3600 co odpowiada 1h)
- - token_type (najlepiej stały Bearer)
- - scope (dowolny)

Przykład (json):

response.json : {‘access_token’:’
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJPbmxpbmUgSldUIEJ1aWxkZXIiLCJpYXQiOjE2Mzg
xOTAwMDEsImV4cCI6MTY2OTcyNjAwMSwiYXVkIjoid3d3LmV4YW1wbGUuY29tIiwic3ViIjoianJvY2tldE
BleGFtcGxlLmNvbSJ9.w36F0KPrHoM76_MaQLAPzkDiHb_FyxZ9dvGz09h6F3Y’, ‘expires_in’:3600,
‘token_type’:’Bearer’, ‘scope’:’etoll_api’}

{"access_token":"xxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxxxtokentokenxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxtokenxxxxxxxxxxtokenxxxxxxxxxxxx","expires_in":8640
0,"token_type":"Bearer","scope":"etoll_api"}

Przykładowy poprawny token :
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJPbmxpbmUgSldUIEJ1aWxkZXIiLCJpYXQiOjE2Mzg
xOTAwMDEsImV4cCI6MTY2OTcyNjAwMSwiYXVkIjoid3d3LmV4YW1wbGUuY29tIiwic3ViIjoianJvY2tldE
BleGFtcGxlLmNvbSJ9.w36F0KPrHoM76_MaQLAPzkDiHb_FyxZ9dvGz09h6F3Y

Jego zdekodowana struktura jest następująca:

```
HEADER:ALGORITHM & TOKEN TYPE
{
  "typ": "JWT",
  "alg": "HS256"
}
PAYLOAD:DATA
{
  "iss": "Online JWT Builder",
  "iat": 1638190001,
  "exp": 1669726001,
  "aud": "www.example.com",
  "sub": "jrocket@example.com"
}
VERIFY SIGNATURE
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) [ ]secret base64 encoded
```

Dane przesyłane z systemu do Operatora spełniają schemat zawarty w poniższej definicji interfejsu.

```
--- YAML FILE BEGIN ---
openapi: 3.0.1
info:
  version: '3.0'
  title: 'PushTopicOBU'
  description: 'Interfejs PushTopicObu służy do przesyłania informacji o stanie salda konta bilingowego powiązanego z danym OBE oraz rodzaj obowiązującej umowy (pre-paid czy post-paid) w celu przekazania jej do urządzenia OBE. Informacja wysyłana jest po każdym naliczeniu opłaty za przejazd drogą płatną.  Wraz z informacją o stanie salda przekazywany jest znacznik czy wysokość salda jest poniżej minimalnego progu i wkrótce powinno być doładowane. Fakt niskiego lub zerowego stanu salda powinien być zaprezentowany na urządzeniu OBE odpowiednim komunikatem i sygnałem dźwiękowym. Moduł inicjujący: MPDS (interfejs komunikacyjny), moduł odbierający: endpoint opearatora OBU.'
paths:

  /PushTopicOBU:
    post:
      tags:
      - PushTopicObu
      summary: Przekazanie komunikatu na urządzenie OBE działające w ramach odpowiedniego systemu
      description: Wiadomość jest przygotowana w postaci tekstowej. W ramach wiadomości znajduje się informacja o przejechaniu odcinka płatnego oraz naliczeniu opłaty jak również w przypadku umowy pre-paid inforamcji na temat aktualnego stanu salda
      operationId: PushTopicOBU

      requestBody:
        description: wiadomość przekazywana jest w postaci kompletnego obiektu
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/OBEMessage'
        required: true
      parameters:
        - $ref: 'header_parameters.yaml#/components/parameters/X-Client-BusinessUser'
        - $ref: 'header_parameters.yaml#/components/parameters/X-Client-GlobalProcessId'
        - $ref: 'header_parameters.yaml#/components/parameters/X-Client-LocalOrderId'
        - $ref: 'header_parameters.yaml#/components/parameters/X-Client-RequestTimestamp'
        - $ref: 'header_parameters.yaml#/components/parameters/X-Client-RetryTry'
        - $ref: 'header_parameters.yaml#/components/parameters/X-Client-SystemName'
      requestBody:
        description: wiadomość przekazywana jest w postaci kompletnego obiektu
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/OBEMessage'
        required: true
      responses:
        200:
          $ref: '#/components/responses/200'
```

```
      400:
        $ref: '#/components/responses/400'
      401:
        $ref: '#/components/responses/401'
      404:
        $ref: '#/components/responses/404'

components:
  responses:
    200:
      description: OK
      content:
        application/json:
          schema:
            type: object
            properties:
              code:
                type: string
                enum: ["200"]
      headers:
        X-Provider-BusinessUser:
          $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-BusinessUser'
        X-Provider-LocalOrderId:
          $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-LocalOrderId'
        X-Provider-ResponseTime:
          $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-ResponseTime'

    400:
      description: Bad request
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/ErrorResponse'

      headers:
        X-Provider-BusinessUser:
          $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-BusinessUser'
        X-Provider-LocalOrderId:
          $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-LocalOrderId'
        X-Provider-ResponseTime:
          $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-ResponseTime'

    401:
      description: Unauthorized
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/ErrorResponse'

      headers:
        X-Provider-BusinessUser:
          $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-BusinessUser'
```

```
      X-Provider-LocalOrderId:
        $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-LocalOrderId'
      X-Provider-ResponseTime:
        $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-ResponseTime'

  404:
    description: Not found
    content:
      application/json:
        schema:
          $ref: '#/components/schemas/ErrorResponse'
    headers:
      X-Provider-BusinessUser:
        $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-BusinessUser'
      X-Provider-LocalOrderId:
        $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-LocalOrderId'
      X-Provider-ResponseTime:
        $ref: 'headers_responses.V1.yaml#/components/headers/X-Provider-ResponseTime'


schemas:
  OBEMessage:
    required:
    - priority
    - serialNumber
    - systemBusinessId
    - message
    - billingAccountId
    - billingAccountBalance
    type: object
    properties:
      priority:
        type: string
        format: enumPriority
        enum: ['info','warning','fault','lowbalance','zerobalance']
        description: atrybut określający wagę/istotność komunikatu
      serialNumber:
        type: string
        format: string50
        description: identyfikator OBE unikalny w ramach systemu, w którym nadaje
        example: '000410001858840'
        maxLength: 50
      systemBusinessId:
        type: string
        format: string10
        description: identyfikator biznesowy usługi OBU/ZSL do której przypisany jest identyfikator
biznesowy urządzenia
        example: 'ZSL-AZEA-7'
        maxLength: 10
      message:
        type: string
        format: string50
```

```
        maxLength: 50
        description: treść komunikatu na urządzenie zawierająca inforamcje na temat zdarzenia
naliczenia opłaty oraz stanu salda dla umów typu pre-paid
      billingAccountId:
        type: integer
        format: int64
        example: 1
        multipleOf: 1
        description: identyfikator konta bilingowego
      billingAccountBalance:
        type: string
        format: money
        description: kwota pieniężna wartości salda po naliczeniu opłaty
        example: '7.85'
        minLength: 4
        maxLength: 16
        pattern: '^-{0,1}\d{1,12}\.\d{2}$'

  ErrorResponse:
    type: object
    additionalProperties: true
    required:
    - subcode
    - message
    properties:
     subcode:
       type: string
       format: string20
     message:
       type: string
       format: string4096

--- YAML FILE END ---
```

3.11 Zarzadzanie certyfikatami

W celu uzyskania certyfikatu dla domeny wykorzystywanej przez Operatora OBU lub Operatora ZSL do wysyłki danych lokalizacyjnych do SPOE KAS w ramach usługi e-TOLL, uprawniony przedstawiciel Operatora powinien użyć konta w serwisie https://puesc.gov.pl/. Po zalogowaniu i wyświetleniu głównego okna tego portalu, przedstawiciel Operatora wybiera w menu Formularze → Formularze SPOE KAS.
Następnie, w zakładce Rejestracja usług dla Operatora ZSL lub Operatora OBU i urządzeń GPS w ramach usług wybiera formularz: REJESTRACJA USŁUG ZEWNĘTRZNYCH SYSTEMÓW LOKALIZACYJNYCH (ZSL) OPERATORA.

Użytkownik wypełnia pola formularza. W polu **Żądanie podpisania i wystawienia certyfikatu dla domeny wskazanej przez Operatora ZSL lub Operatora OBU** wkleja CSR (ang. Certificate Signing Request). CSR generuje się na podstawie swojego klucza prywatnego. Można do tego użyć openssl'a (www.openssl.org). Jeżeli użytkownik posiada już klucz prywatny (np. plik private.key), to w środowisku Linux polecenie ma następującą budowę:

- Openssl req –new –key private.key –out certificate.csr

Jeżeli użytkownik nie ma klucza prywatnego można go wygenerować na przykład:

- openssl genrsa -des3 -out tech-private.key 4096

(długość 4096 bitów daje lepszy poziom zabezpieczeń niż klucz 2048)

Przykład pliku zawierającego klucz prywatny prezentuje Rys. 4.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAua
SvEsSeMUYYdw4fC0WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB
1mKuux1XP0tCsHXgPJOezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMRlD4G3cPBD
dOOZqSmX7tHp97q+PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7
KGFjwEl+UxDgsNaSp7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyf
kW4k8gvltwueKScsc9/Ordlr6YopGg5xwQr+TQIDAQABAoIBAQDePSF9cqTf9X4I
TVqkl6cqkQQqSU5sokTQSidbkRQmK1S/JCrqQ5VZ6Ldz+l260DCYiiA2glpdcy7a
zCz0lldhtHsWfVBI5HdTleu2iJO/8Ig2DGQOgC8chQbpQ8HQ1WqVIBaF+ha3W64d
VJlH7f4ctfxoGi8S5XH8Jtgq3JoLdeH9YqaNzQ2LKSx91/PxO6J7sLya82KKUBrp
M3AOumtEt0YRy57JkV7j1YeYUFLpWT7cR5rh2cZs5r1fQTGQjQorWBu/e4Po7PMn
Vbp/qDBqnifemd/dxDWydtXtJukp1mLdUSK15jAXApr2ZSXZ56espTnuIxkkvuzZ
mnyl5mItAoGBAP34wh8DZwvUeKIn408osSQzHEtMnefIMB0u0yoj94RQZuv8VwAR
eoTeFIEPOQqgdB7MSgkgZpNuyYxW+OrQI4mMl9Wh9DyHwnWTxNO7pDJEb6BCukQb
/+bdjLSytmDyVhkGMlMQ1E0l7MdncrQRSURvByNRXbDzzoP7wlL2bASTAoGBAPGb
HIDDlxcHZkdOWNof2RDE+UbgaU86aI3dtGSsoTo6bmPkXxfe6PJPu8pLwzhVOafZ
EXH4qJ9CiOE4r6PelyA944KDwx8mlBsU7E6fEchJaR6xykW8u25Nr5P304szxCTI
987eJmQq+BGUUp7LgC/QlcpiR7yyP+h5CNNkAp2fAoGAEcSaiCLrzacSvX1+6KXX
Jsowm5ADqBiYTSJegZ88jNQ3LyFbUNToNm13D8Rp4DVzikgOke7jXkMs9JWNGphv
NAtTAA4xkR6KW0F4Trvc8+tXx+WDNIqk75jmZCnwmn25ykxlruwJflA97YFuQ+zF
rHT8Edt6a4vTEebGJJm62uMCgYA06NMFH9AmqugrFW0/11mh4oD0lJB7WT8sUjD/
Gw7zwXgLSCfLAnXhGrT1SEIoRAGsUE0RuHK07c0sBU3xhP1zghogqtpAKCKnC530
WcF7KxhqMGUrgHlLXpfkv5EEGwIJTDl4hA3EQeSxdNnjDI216ufiukMbf62fK2JT
aMNp4QKBgDxQkHSX8E7FhlUijf3C8IMZsZ7frzCbdIfNX6/PcVrcx3UKSVWmB9/v
auOMEHZmoo/FRZXdcZPI0wzcGb4oz4few2Dp2savew5QEGq4v3DZDEhGK5X7Yc+M
skL3MCgqGqVN1+fV4uFHzGqPpMKMXZHUKlpLTVWNvswe0SBfZ5U5
-----END RSA PRIVATE KEY-----
```

Rys. 4. Przykład pliku z kluczem prywatnym

Z kolei przykład pliku zawierającego CSR przedstawia Rys. 5.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1zCCAb8CAQAwgZExCzAJBgNVBAYTAlBMMRQwEgYDVQQIDAtNQVpPV0lFQ0tJ
RTERMA8GA1UEBwwIV0FSU1pBV0ExDDAKBgNVBAoMA05JVDELMAkGA1UECwwCWjYx
FzAVBgNVBAMMDnd3dy5pdGwud2F3LnBsMSUwIwYJKoZIhvcNAQkBFhZlLmtsaW1h
c2FyYUBpdGwud2F3LnBsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAuaSvEsSeMUYYdw4fC0
WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB1mKuux1XP0tCsHXg
PJOezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMRlD4G3cPBDdOOZqSmX7tHp97q+
PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7KGFjwEl+UxDgsNaS
p7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyfkW4k8gvltwueKScs
c9/Ordlr6YopGg5xwQr+TQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBADjODu11
Wqp2GJ/8nam/bjnh2WNSczQ0FjQ6IiK/+rh1BfOREky0J9cz+hRsZt5m9D8UVWkC
u4a/iJicrMZHPhTbC9tKuAk2c29ErxKJeSXr/anRKg9EbD7AB4RFmEjsJo/yRauL
oHetcTqxNPDBspkCmo2eRrKb2LdhCGFQRG4Wx/Gg6iuzd7zZKnOVKMuELpOP/vTz
Gu6QUDi2kpg/cr5A1rwq4d5uIEag1vi9G8YXNa/wkqOrNsuP660Wj8u9QgIWpWdV
ikYJShaHRHFxk3Qr//3P3lg0vgc4AuDcs/r4aOlET7dzuIt0qZymoQKPuOwXpfgY
gxjEmtwLRv5BgM8=
-----END CERTIFICATE REQUEST-----
```

Rys. 5. Przykład pliku zawierającego CSR

Więcej szczegółów można znaleźć pod adresem:
https://tech-itcore.pl/2012/07/04/generowanie-wlasnego-certyfikatu-ssl/
https://uk.godaddy.com/help/apache-generate-csr-certificate-signing-request-5269

W formularzu **musi być możliwość** podania **adresu e-mail**, na który użytkownik otrzyma formularz z odpowiedzią.

W formularzu z odpowiedzią Operator ZSL, Operator OBU otrzymuje Certyfikat klienta zakodowany w formacie base64.
Należy go rozkodować. **Nie należy dodawać do niego linii BEGIN/END CERTIFICATE**, trzeba tylko użyć narzędzia potrafiącego odkodować tekst zakodowany w Base64, np.:

- Notepad++ > Wtyczki > Mime Tools > Base64 Decode
- openssl base64 -d -in plik_z_zakodowanym_certyfikatem.txt -out certyfikat.pem
- Strona https://www.base64decode.org/
- Certutil -decode plik_z_zakodowanym_certyfikatem.txt certyfikat.pem (dla Windows korzystając z linii poleceń).

Przykład certyfikatu w base64 prezentuje Rys. 6.

Rys. 6. Certyfikat zakodowany w Base64

Natomiast przykład certyfikatu odkodowanego w formacie PEM (ang. Privacy-Enhaced Mail) pokazano na Rys. 7.

```
-----BEGIN CERTIFICATE-----
MIIIdjCCBF6gAwIBAgICBEQwDQYJKoZIhvcNAQELBQAwge4xCzAJBgNVBAYTAlBM
MRQwEgYDVQQIDAttYXpvd2llY2tpZTE9MDsGA1UECgw0SW5zdHl0dXQgxYHEhWN6
bm/Fm2NpIC0gUGHFhHN0d293eSBJbnN0eXR1dCBCYWRhd2N6eTE8MDoGA1UECwwz
WmFrxYJhZCBaYWF3YW5zb3dhbnljaCBUZWNobmlrIEluZm9ybWFjeWpueWNoICha
LTYpMSkwJwYDVQQDDCBTRU5UIEdFTyBJVEwgWlNMIFRlc3QgTGV2ZWwgMSBDQTEh
MB8GCSqGSIb3DQEJARYSc2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIw
NFoXDTE5MTAxODA3MDIwNFowgZExCzAJBgNVBAYTAlBMMRQwEgYDVQQIDAtNQVpP
V0lFQ0tJRTERMA8GA1UEBwwIV0FSU1pBV0ExDDAKBgNVBAoMA05JVDELMAkGA1UE
CwwCWjYxFzAVBgNVBAMMDnd3dy5pdGwud2F3LnBsMSUwIwYJKoZIhvcNAQkBFhZl
LmtsaW1hc2FyYUBpdGwud2F3LnBsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAuaSvEsSeMU
YYdw4fC0WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB1mKuux1X
P0tCsHXgPJOezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMRlD4G3cPBDdOOZqSmX
7tHp97q+PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7KGFjwEl+
UxDgsNaSp7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyfkW4k8gvl
twueKScsc9/Ordlr6YopGg5xwQr+TQIDAQABo4IBdzCCAXMwCQYDVR0TBAIwADAd
BgNVHQ4EFgQUgzh3qIG1qOBurhVB9SH5iJ4nIUswDgYDVR0PAQH/BAQDAgXgMBMG
A1UdJQQMMAoGCCsGAQUFBwMCMIIBIAYDVR0jBIIBFzCCARoAFCwa4gqUtt+fYqFf
dRdBtFwmNS1poYH2pIHzMIHwMQswCQYDVQQGEwJQTDEUMBIGA1UECAwLbWF6b3dp
ZWNraWUxETAPBgNVBAcMCFdhcnN6YXdhMT0wOwYDVQQKDDRJbnN0eXR1dCDFgcSF
Y3pub8WbY2kgLSBQYcWEc3R3b3d5IEluc3R5dHV0IEJhZGF3Y3p5MTwwOgYDVQQL
DDNaYWvFgmFkIFphYXdhbnNvd2FueWNoIFRlY2huaWsgSW5mb3JtYWN5am55Y2gg
KFotNikxHTAbBgNVBAMMFFNFTlQgR0VPIElUTCBSb290IENBMRwwGgYJKoZIhvcN
AQkBFg16NkBpdGwud2F3LnBsggIQAzANBgkqhkiG9w0BAQsFAAOCBAEABn/BJ7HT
zSV+69+Q2uzWos+6tubKzJ8Eqv74s28lWPhCGrYED2FID/3qLCN8kV+CpUoVaYoz
PWwr/o0ednRDE/AIf2WnYb13UDxeWIFuSKx+kty+NvqCaq9JflrmjZWs6evZaRMs
xbYj0pju/cIg2PPj6UNH0hwdX6yjvO8vRS25JWY4UFOekT5I6BMjfAEUbi75YXyK
yHkdhLriwgRlHeQ4RVcodrPpn3+ojf07eidv3omHgQ7JmsGYCKu5ut4H7sGdOp28
tCuE0/IsrL7y4Suxo2uAR5RcW4COEPMtBkJh3XVvAYqKtH9dhGHu3ncR3F3TlqCO
NSxRJ5JoNPxKTH4Pc8y/Ewa1p+YX3wVijzeE8t2blb6aZOcY+Hj2RA9Yl3uG8ODb
kRFcwP40Ht449Z2R/cZXkt23oC80uG1WQmzkz5BH6ZPuacQLdqEZ9ImTpcyUWE2A
rblxdNRBl5QnzvFVBaXvBhzROgB8l2tArfMCIfVxlYwCTZvajnDyWbm5lQwWcXUv
jdZn3vwsPYru0/ImhN0ulP+YB1/XA09nfcTUax8pWmoJJvSgYLx8Y5fnYsEGD+Be
vbOI6JnX3ENhDo0Ewx5J2EEwxIVSrNjQ+cTIaYOjXLfoXWyZvwjiACzuoUNfBhMd
oewlndkKjaOJFonsjprXzQOUqxwff87nnW/ALq/mbBK+YRQNA3MZhrS437En57Z/
GGbopAOl3SzYMqVXQ8BNgpPadYX/jCYX5x3C9S7QQMeWLzFj7CuR+U7KckDjNqhi
vOnYclygaL4ofzZHwAEznYmlnyoLcNUDnNBmiGSSMRWp9n1+WMhD6VJJjKLn8Tpi
lUV1EwvYubuOL4kX/56PxBa9ePXE/I4tYbF+9AGNsoHEslE1D5qN3yd13SgpHnR7
ueqBsmX+7yCq6KaNFmiiJhKHkO+Lq+6WY1hjcNUh7pp8cOZdAVFDNOiaOYdhCxU3
9u+FkpDYb01/sYjoVtKatwk+FEOmoa/fQIcrmllAbvmk/J8XYf+SHmUR5h9pU0sv
hHmTUharftgtUjrktgBWW1tNHqP+Fwk8tpsWh4M4r6cMJ1ShxJ+Xc+cfgTiJwcvE
otXX6ScZqlFm0gwUM1LNvJmN3zaycaaYjaHvIgiz8CVPomVaAtsaG7Oe9jKY74Ol
1kE47PRG3yGG456Rny1Wv38XBNpiWtTe+6NwlIEHSOPGIIpIuJnxsniO7bR1terY
i7m2nzPvbI9Qn/bFMlLNVjU51UR5RcFtb/p++pvlQuX5cf/rNAnStBJT5mxdP7Du
m+TyEWxCMZWZI+h+0okJWmPqKBnG4tsTQhceiP7W2qZis0jZkl62u/V6+ooQP89l
AEtZaGkLC+Y/lg==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIKwjCCBqqgAwIBAgICEAMwDQYJKoZIhvcNAQELBQAwgfAxCzAJBgNVBAYTAlBM
MRQwEgYDVQQIDAttYXpvd2llY2tpZTERMA8GA1UEBwwIV2Fyc3phd2ExPTA7BgNV
BAoMNEluc3R5dHV0IMWBxIVjem5vxZtjaSAtIFBhxYRzdHdvd3kgSW5zdHl0dXQg
QmFkYXdjenkxPDA6BgNVBAsMM1pha8WCYWQgWmFhd2Fuc293YW55Y2ggVGVjaG5p
```

Rys. 7. Przykład odkodowanego certyfikatu

Po odkodowaniu otrzymuje się plik zawierający maksymalnie trzy certyfikaty w formacie PEM:

- Certyfikat klienta,
- Certyfikat CA (Centrum Autoryzacji) poziomu 1, które wystawiło certyfikat klienta,
- Certyfikat CA (Centrum Autoryzacji) poziomu 0, które wystawiło certyfikat CA poziomu 1.

Każdy certyfikat rozpoczyna się i kończy liniami:
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
Powyższe linie oznaczają początek i koniec poszczególnych certyfikatów.

Zakres i sposób użycia danych, które są stosowane do zabezpieczenia komunikacji TLS, jest różny i zależy od użytkowanego przez podmiot systemu / aplikacji. Niemniej, typowe wymagania narzędzi /komponentów SSL/TLS obejmują wykorzystanie w trakcie uwierzytelniania SSL następujących elementów:

- certyfikatu klienta;
- klucza prywatnego – który zabezpiecza możliwość użycia certyfikatu klienta wyłącznie przez podmiot będący jego dysponentem;
- łańcuch certyfikacji / łańcuch certyfikatów (ang. certificate chain), który uwierzytelnia certyfikat klienta jako certyfikat wystawiony przez właściwe CA i zawiera:
  - certyfikat CA (Centrum Autoryzacji) poziomu 1, które wystawiło certyfikat klienta,
  - certyfikat CA (Centrum Autoryzacji) poziomu 0, która wystawiło certyfikat CA poziomu 1.

W środowisku Linux połączenie z SPOE KAS można przetestować z wykorzystaniem narzędzia curl. Sekwencję komend przedstawiono poniżej. Certyfikat.pem oznacza otrzymany certyfikat, który został odkodowany z formatu base64 do formatu PEM. Natomiast fd1.key oznacza klucz prywatny (odszyfrowany) użyty do generowania CSR.

curl -X POST --cert ./certyfikat.pem --key ./fd1.key -H 'Content-Type: application/json' -H 'cache-control: no-cache' -d '[{"dataid": "1960472", "serialNumber": "ALBS8_74718", "latitude": 52.17264488, "lonitude": 21.1956136, "altitude": 140.0, "fixTimeEpoch": 1505893301000000, "gpsSpeed": 0.0, "accuracy": 15.17, "gpsHeading": 0.0},{"dataid": "1960473", " serialNumber": "ALBS8_74718", "latitude": 52.17264546, "longitude": 21.195608, "altitude": 138.0, "fixTimeEpoch": 1505896249000000, "gpsSpeed": 10.0, "accuracy": 15.17, "gpsHeading": 0.0}]' https://cloud.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001

Uwaga 1: Adres https://cloud.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001 należy zastąpić otrzymanym adresem z formularza otrzymanego pocztą elektroniczną, chodzi o zawartość pola **Adres URL usługi SPOE KAS dedykowany do komunikacji z usługą Operatora ZSL lub Operatora OBU**.

Uwaga 2: Certyfikat X.509 klienta SSL/TLS po stronie Operatora ZSL lub Operatora OBU

Do obowiązków Operatora ZSL lub Operatora OBU należy:

1. uzyskanie w/w certyfikatu:
   a. pierwszego - w wyniku rejestracji usługi,
   b. każdego kolejnego przed upływem 365 dni od wystawienia poprzedniego certyfikatu;
2. stosowanie aktualnego certyfikatu X.509 klienta SSL/TLS do uwierzytelnienia komunikacji z interfejsem danych SPOE KAS.

Pierwszy certyfikat X.509 klienta SSL/TLS jest wydawany w odpowiedzi na przesłanie do SPOE KAS poprzez dedykowany portal żądania wydania certyfikatu X.509 klienta SSL/TLS za pośrednictwem jednego z dwóch dostępnych form komunikacji:

1. dokumentu XML;
2. formularza rejestracji usługi wypełnianego na stronie usługi SPOE KAS w dedykowanym portalu SPOE KAS.

Kolejny certyfikat można uzyskać poprzez przesłanie do SPOE KAS za pośrednictwem dedykowanego portalu żądania wydania certyfikatu X.509 klienta SSL/TLS za pośrednictwem jednego z dwóch dostępnych form komunikacji:

1. dokumentu XML;
2. formularza aktualizacji danych usługi wypełnianego na stronie usługi e-TOLL w dedykowanym portalu.

Certyfikat X.509 klienta SSL/TLS służący do uwierzytelniania Operatora ZSL lub Operatora OBU w trakcie komunikacji z interfejsem danych SPOE KAS jest pierwszym z certyfikatów zwracanych przez SPOE KAS w odpowiedzi na przesłanie formularza/dokumentu XML. Każdy ze zwróconych certyfikatów rozpoczyna się od linii „-----BEGIN CERTIFICATE-----" a kończy się linią „-----END CERTIFICATE-----".

Datę ważności certyfikatu X.509 klienta SSL/TLS można podejrzeć za pomocą bezpłatnego pakietu narzędzi OpenSSL przy użyciu następującego polecenia:

openssl x509 -inform PEM -enddate –noout –in plik_z_certyfikatem_klienta_x509.pem

gdzie:

- plik_z_certyfikatem_klienta_x509.pem - stanowi przykładową nazwę pliku zawierającego certyfikat X.509 klienta SSL/TLS wystawiony przez SPOE KAS.

Poniżej podano przykładową odpowiedź na w/w polecenie:

notAfter=Sep 30 08:30:58 2020 GMT

gdzie:

- notAfter - etykieta pola „nie później" z certyfikatu X.509, które zawiera ostateczny termin ważności certyfikatu, po którym, nie należy ani go używać ani mu ufać;
- Sep – trzy literowy skrót nazwy miesiąca, w tym przypadku to skrót od September , czyli Wrzesień;
- 30 – dzień;
- 08:30:58 – godzina, minuta i sekunda;
- 2020 – rok;
- GMT – trzy literowy skrót nazwy strefy czasowej, oznaczenie strefy czasowej, w tym przypadku jest to skrót od Greenwich Mean Time, oznaczający, że aby uzyskać godzinę dla strefy czasowej Europa/Warszawa należy do podanej godziny dodać 2 godziny w przypadku czasu letniego i jedną godzinę w przypadku czasu zimowego.

Uwaga 3: Konfiguracja „mutual TLS"
W przypadku konfiguracji mutual TLS należy zwrócić uwagę, że zmiana certyfikatu serwera uniemożliwi poprawną autentykację komunikacji. Informacja o zmianie certyfikatu serwera będzie propagowana do Operatorów, natomiast w przypadku jakichkolwiek problemów z weryfikacją certyfikatu serwera można wykorzystać komendy umożliwiające podgląd certyfikatu, tj.:

openssl s_client -showcerts -connect communication.etoll.gov.pl:443
openssl s_client -showcerts -connect communication.etoll.gov.pl:443 2>&1 |openssl x509 -text -noout | more

4 Ogólne wymagania dla Systemu Operatora i urządzeń OBU/ZSL

Transfer Danych GNSS przez Operatora do SPOE KAS musi zapewniać:

- Przesyłanie danych lokalizacyjnych do SPOE KAS zgodnie ze specyfikacją opisaną w niniejszym dokumencie;
- Kolejkowanie (zdarzeń, danych lokalizacyjnych);
- Zdalna aktualizacja oprogramowania OBU/ZSL;
- Autodiagnostyka.

System Operatora, na żądanie administratora SPOE KAS, musi umożliwiać administratorowi Operatora parametryzację co najmniej następujących parametrów:

- częstotliwości zbierania danych lokalizacyjnych **podstawowe ustawienie wyjściowe to 5 sekund**;
- częstotliwości wysyłania danych lokalizacyjnych **podstawowe ustawienie wyjściowe to 1 minuta (60 sekund)**;
- zalecana wielkości bufora danych minimum 250MB (wymaganie to nie jest obowiązkowe);

  Wielkość bufora danych musi umożliwiać przechowywanie danych geolokalizacyjnych zawierających atrybuty wskazane w rozdziale 3.10.1 zbieranych z powyżej wskazaną częstotliwością i przechowywanych po stronie lokalizatora nie krócej niż 10 dni (o ile wcześniej nie zostały przesłane do SPOE KAS) oraz zdarzeń wskazanych w rozdziale 3.4 STRUKTURA JSON

- częstości retransmisji danych w przypadku problemów z komunikacją w zakresie od 30 sek do 60 sek; **podstawowe ustawienie wyjściowe 60 sekund**;

OBU/ZSL musi spełniać następujące wymagania w zakresie GNSS:

- posiada czuły odbiornik GNSS razem z anteną;
- dokładność odczytu lokalizacji musi zapewniać, że odczytane współrzędne będą znajdować się w odległości nie większej niż 4 metry od skraju pasa jezdni, po którym porusza się pojazd;
- obsługuje sieci: GPS, GLONASS, Galileo;
- obsługuje system EGNOS;
- odbiornik GNSS wspiera A-GPS, aby skrócić czas do pierwszego odebrania lokalizacji;
- antena GNSS i jej połączenie z odbiornikiem GNSS jest osłonięta przed zakłóceniami (ekranowanie);
- odbiornik GNSS powinien odświeżać pozycję z częstotliwością przynajmniej raz na sekundę;
- odbiornik GNSS wspiera zawansowaną detekcję zagłuszania i fałszowania;
- wszystkie czujniki kalibrują się automatycznie.

Opcjonalne: Aktualizowanie oprogramowania odbiornika GNSS jest możliwe zdalnie przez sieć komórkową;

OBU/ZSL: musi spełniać następujące wymagania w zakresie komunikacji z siecią:

- posiada moduł komunikacji z siecią komórkową razem z anteną;

- zapewnia zdalny dostęp i możliwość dwukierunkowej wymiany danych z systemem centralnym przez sieć komórkową;

Opcjonalne: OBU/ZSL może posiadać możliwość odbierania komunikatów zwrotnych ze SPOE KAS w formie wiadomości tekstowych oraz może umożliwiać ich wyświetlenie użytkownikowi. Przykładowo może być to informacja o stanie konta, sygnalizacja przejazdu przez bramownicę wirtualną, ostrzeżenie o niskim stanie konta.

OBU/ZSL musi spełniać następujące wymagania w zakresie bezpieczeństwa:

- OBE posiada jednostkę zabezpieczającą taką jak „Secure Acces Module (SAM)" odpowiedzialną za wykonywanie algorytmów szyfrujących i przechowywanie danych wrażliwych takich jak klucze, PIN i inne;
- Jednostka zabezpieczająca wspiera algorytmy kryptografii takie jak szyfrowanie/ deszyfrowanie, generację liczb losowych, przechowywanie kluczy;
- Jednostka zabezpieczająca na stałe przechowuje wrażliwe dane w pamięci nieulotnej;
- Komunikacja między jednostką zabezpieczającą a komponentami OBU (takimi jak procesor, moduły, pamięć i inne) używa uwierzytelniania i szyfrowania;
- Oprogramowanie nie jest znacznie spowolnione przez bezpieczną komunikację jednostki zabezpieczającej z zewnętrznymi komponentami;
- Jednostka zabezpieczająca przechowuje bezpiecznie unikalne ID i zapewnia dostęp do oprogramowania;
- Jednostka zabezpieczająca jest odporna na aktywne i pasywne ataki;
- jednostka zabezpieczająca jest odporna na mechaniczne modyfikacje. Otwarcie obudowy OBU lub jednostki zabezpieczającej jest niemożliwe bez zostawiania śladów;
- Każda próba ataku jest wykryta, udokumentowana i kontrolowana.

Krótkie zaniki napięcia nie mają wpływu na działanie OBU/ZSL:

- W razie odłączenia OBU od zasilania, urządzenie przechowuje dane z pamięci nieulotnej i wyłącza się prawidłowo;
- OBU posiada wbudowany akumulator pozwalający na kilkugodzinną pracę w przypadku braku napięcia zasilającego.

Wraz z urządzeniami musi zostać dostarczony system pozwalający na zarządzanie urządzeniami OBU. System w szczególności musi umożliwiać:

- Zdalne aktualizacje oprogramowania;
- Zdalne ustawianie parametrów pracy OBU;
- Monitorowanie stanu OBU.

Niespełnienie wymogów technicznych dla urządzenia może skutkować dezaktywacją urządzenia.

5 Wymagania prawne i normatywne

Rozdział ten zawiera wymagania prawne i normatywne dotyczące poboru opłat.

Dokument	Wersja	Zawartość
Decyzja 2004/52/EC1	6 października 2009	Decyzja Komisji Europejskiej w sprawie definicji europejskiej usługi opłaty elektronicznej oraz jej elementów technicznych
Dyrektywa 77/649/EEC	27 września 1977	Dyrektywa w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do pola widzenia kierowców pojazdów silnikowych
Dyrektywa 2002/95/EC	27 stycznia 2003	Dyrektywa w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym
Dyrektywa 2012/19/EC	4 lipca 2012	Dyrektywa w sprawie zużytego sprzętu elektrycznego i elektronicznego
Dyrektywa 2004/108/EC	15 grudnia 2004	Dyrektywa w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej
Dyrektywa 2004/53/EC	16 kwietnia 2014	Dyrektywa w sprawie harmonizacji ustawodawstw Państw Członkowskich dotyczących udostępniania na rynku urządzeń radiowych
Dyrektywa 2014/30/EC	26 lutego 2014	Dyrektywa w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej
Dyrektywa 2011/65/EC	8 czerwca 2011	Dyrektywa w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym
Dyrektywa 2006/66/EC	6 września 2006	Dyrektywa w sprawie baterii i akumulatorów oraz zużytych baterii i akumulatorów
Dyrektywa 2013/56/EC	20 listopada 2013	Dyrektywa w sprawie baterii i akumulatorów oraz zużytych baterii i akumulatorów w odniesieniu do wprowadzania do obrotu baterii i akumulatorów przenośnych zawierających kadm przeznaczonych do użytku w elektronarzędziach bezprzewodowych i ogniwach guzikowych o niskiej zawartości rtęci
ISO DIS 12813	28 września 2018	Elektroniczny pobór opłat - Kontrola zgodności w systemach autonomicznych
ISO 13141	1 czerwca 2017	Elektroniczny pobór opłat - Komunikacja mająca na celu usprawnienie lokalizacji w systemach autonomicznych