Ministerstwo Finansów

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

Warszawa 12.10.2020 r.

Spis treści

1 Wstęp 4

2 Interfejsy rejestracji 5

2.1 Rejestracja usług przesyłania danych lokalizacyjnych przez Operatorów 5

2.2 Rejestracja przez Operatora urządzeń lokalizacyjnych 5

3 Komunikacja Proxy Serwer <-> SPOE KAS 6

3.1 Przekazywanie przez Operatora ZSL lub Operatora OBU danych lokalizacyjnych z urządzeń wskazanych przez Użytkownika końcowego do SPOE KAS 6

3.2 Przekazywane dane lokalizacyjne 6

3.3 Częstotliwość przesyłania danych 6

3.4 Struktura JSON 7

3.5 Metoda przekazywania danych 9

3.6 Bezpieczeństwo przesyłanych danych 9

3.7 Walidacja danych - obowiązki po stronie Operatora ZSL i Operatora OBU 10

3.8 Lista komunikatów dla Operatora ZSL i Operatora OBU 10

3.9 Informacje konieczne do podłączenia Operatora ZSL lub Operatora OBU do NSKPO 11

3.10 Sprzężenie zwrotne pomiędzy SPOE KAS a Operatorami ZSL i Operatorami OBU 11

3.10.1 Interfejs zwrotny dla Operatora ZSL lub Operatora OBU 12

3.10.2 Komunikaty zwrotne na OBE 13

3.11 Zastosowanie certyfikatów 14

4 Zalecenia ogólne 19

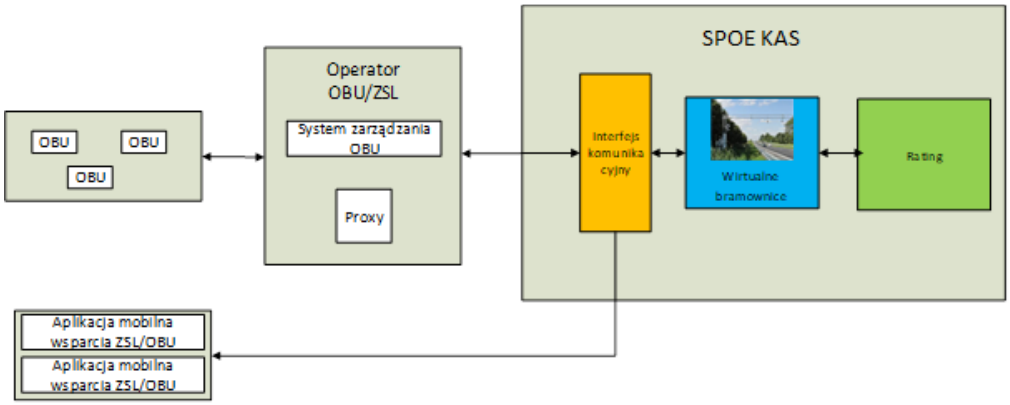
5 Wymagania prawne i normatywne 21

Słownik pojęć

Pojęcie	Opis
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 OBU	Firma zarządzająca usługami OBU.
Operator ZSL	Firma zarządzająca usługami ZSL.
Operator	Operator ZSL i/lub Operator OBU.
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.
JSON	(ang. JavaScript Object Notation) – format wymiany danych.
JSON Schema	Definiuje strukturę danych w JSON.
MCC	(ang. Mobile Coutry 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 (oeratora) telefonii bezprzewodowej.
Jamming	Zagłuszanie sygnału GNSS przez urządzenia elektroniczne.
Spoofing	Ataki na system teleinformatyczny poprzez podszywanie się pod inny element systemu informatycznego.
EGNOS	(ang. European Geostationary Navigation Overlay Service) – europejski system wspomagający systemy GPS i GLONASS, a w przyszłości Galileo.
PEM	(ang. Privace Enhanced Mail) – format pliku służący do zapamiętywania i wysyłania kluczy kryptograficznych, certyfikatów i innych danych zdefiniowane w RFC 7468.
Base64	Służy do kodowania ciągu bajtów. Zdefiniowane w RFC 4648.
TLS	(ang. Transport Layer Secuirty) – protokół kryptograficzny będący standardem w Internecie, zapewnia poufność i integralność transmisji danych, uwierzytelnianie serwera, czasami klienta. Jest rozwinięciem protokołu SSL.
SSL	(ang. Secure Socket Layer) – standardowy protokół kryptograficzny wykorzystywany do bezpiecznej transmisji dokumentów przez sieci komputerowe.
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.
GPS	(ang. Global Positioning System) – amerykański radiowy system nawigacyjny oparty na satelitach.
GNSS	(ang. Global Navigation Satetellite System) – globalny system nawigacyjny obejmujący swoim zasięgiem całą Ziemię. Przykładem jest system GPS.
SPOE KAS	System Poboru Opłaty Elektronicznej Krajowej Administracji Skarbowej

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 ta 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.



Rysunek 1 Główne komponenty systemu omawiane w dokumencie

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 Specyfikacji Technicznej 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 opisane szczegółowo w wyżej wymienionym dokumencie.

2.1 Rejestracja usług przesyłania danych lokalizacyjnych przez Operatorów

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

a. Operator przesyła do SPOE KAS:
   i. wykaz numerów IP serwerów, z których będzie w przyszłości przesyłał dane,
   ii. żądanie wydania certyfikatu SSL/TLS klienta,
   iii. adres interfejsu zwrotnego oraz dane uwierzytelniające (login name, password) (metody dla interfejsu zwrotnego: asynchroniczny odbiór komunikatów potwierdzających przyjęcie przekazywanych danych, metoda umożliwiająca uzyskanie aktywnego klucza uwierzytelniającego- standard OAuth2.0, metoda odbierająca komunikaty dla odpowiednich urządzeń – w przypadku OBU bez wyświetlacza),
   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-GEO 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

Rejestracja przez Operatora urządzeń lokalizacyjnych ZSL lub OBU w SPOE KAS obejmuje następujące kroki:

a. Operator przesyła do SPOE KAS między innymi:
   i. identyfikatory techniczne urządzeń lokalizacyjnych GNSS użytkownika końcowego powiązane z usługą Operatora
b. Operator otrzymuje zwrotnie między innymi:
   i. numer biznesowy urządzenia GNSS Użytkownika końcowego powiązany z identyfikatorem technicznym urządzenia GNSS (powiązanie 1 identyfikator techniczny = 1 numer biznesowy urządzenia OBE) oraz hasło umożliwiające połączenie urządzenia z aplikacją SPOE KAS.

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.

3.2 Przekazywane dane lokalizacyjne

Rekord danych lokalizacyjnych powinien posiadać następujące informacje:

- numer rekordu danych lokalizacyjnych,
- szerokość geograficzna*,
- długość geograficzna*,
- azymut*,
- prędkość*,
- stempel czasu zebrania danych lokalizacyjnych*,
- błąd przekazania danych lokalizacyjnych*,
- liczba widocznych satelitów**,
- liczba satelitów użytych do ustalenia pozycji,
- identyfikator urządzenia OBU,
- CID - Cell id (identyfikator komórki),**
- LAC - Location Area Code (identyfikator obszaru, w ramach którego Cell id jest unikalne),**
- MCC – Mobile Country Code,
- MNC – Mobile Network Code,
- klasa zdarzenia**:
    - włączenie urządzenia (turnon),
    - wyłączenie urządzenia (turnoff),
    - początek trasy (startjourney),
    - zakończenie trasy (endjourney),
    - odłączenie od zasilania (plugout),
    - podłączenie do zasilania (plugon),
    - GSM online (gsmonline),
    - GSM offline (gsmoffline),
    - GNSS online (gpsonline),
    - GNSS offline (gpsoffline),
    - Jamming,
    - Spoofing;

* są zaznaczone dane wymienione w ustawie o drogach publicznych (pkt 3, art. 13))
** to są niewymagane (danych nie może zbierać iOS- system operacyjny Apple)

3.3 Częstotliwość przesyłania danych

Operator ZSL, Operator OBU przekazuje dane do SPOE KAS z częstotliwością 1 pakiet danych na jedną minutę. Pakiet danych zawiera dane lokalizacyjne oraz wygenerowane na poziomie OBE zdarzenia

(takie jak włączenie zapłonu, rozpoczęcie jazdy, zatrzymanie, wyłączenie itp.). Dane lokalizacyjne muszą być zbierane z częstotliwością 1 lokalizacja na 5 sekund.

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 1.

Tabela 1. Schema_SPOE_v_1_0

Nazwa	Opis	Reguła walidacji	Wymagane
dataId	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.	"type": "string", minLength": 1,"maxLength": 32, "examples": ["1", "1960472"]	Tak
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

Nazwa	Opis	Reguła walidacji	Wymagane
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
gpsSpeed	Prędkość przemieszczania się pobrana z nadajnika GNSS - jednostka [m/s], dozwolona maksymalna liczba miejsc po przecinku: 2. Dozwolona maksymalna prędkość: 56.00 [m/s].	"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}$"	Tak
Mcc	identyfikator kraju operatora GNSS	„type”: „string” „pattern”: "^[0-9]{3}$"	Tak
Mnc	identyfikator sieci operatora GNSS	„type”: „string” „pattern”: "^[0-9]{2,3}$"	Tak
mobileCellId	identyfikator komórki sieci GNSS	„type”: „string” „pattern”: "^[A-Fa-f0-9]{4,9}$"	Tak
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	Tak

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 2**.

Tabela 2. 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 mniejsza 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 1 (słowniej jednej) do 500 (słownie pięciuset) obiektów JSON.
Maksymalna dopuszczalna wielkość pojedynczego pakietu wyrażona w bajtach wynosi 1 MB (słownie jeden megabajt).

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 dostępnie dla wskazanych IP,
- 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 2** i odrzucać dane niespełniające kryteriów zawartych w **Tabela 2**. Tym samym Operator powinien separować zbędne dane i wysyłać do systemu SPOE KAS **tylko** dane z Polski.

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 3 zawiera najczęściej występujące komunikaty w procesie walidacji danych.

Tabela 3. 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	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
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".

Reguły drop występują w przypadku:
1) niezarejestrowanych urządzeń,
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 systemu.

3.9 Informacje konieczne do podłączenia Operatora ZSL lub Operatora OBU do NSKPO

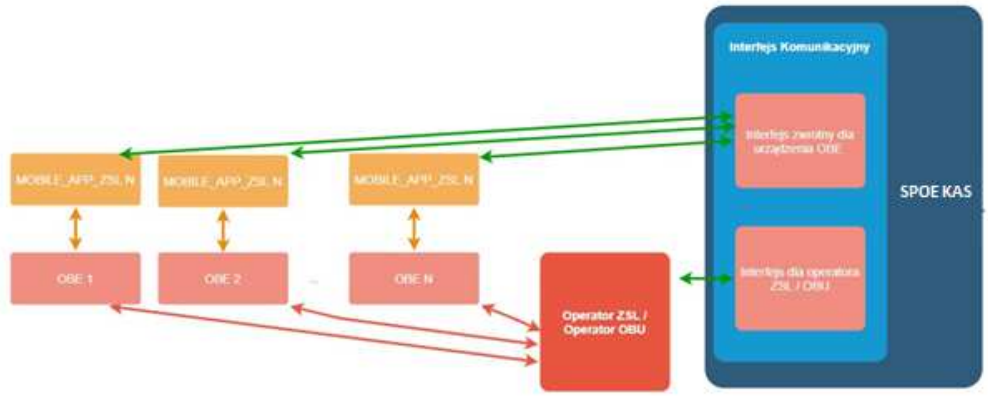
Podłączenie Operatora ZSL lub Operatora OBU do SPOE KAS wykorzystuje certyfikaty i oparte jest o formularze dedykowanego portalu SPOE KAS.

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

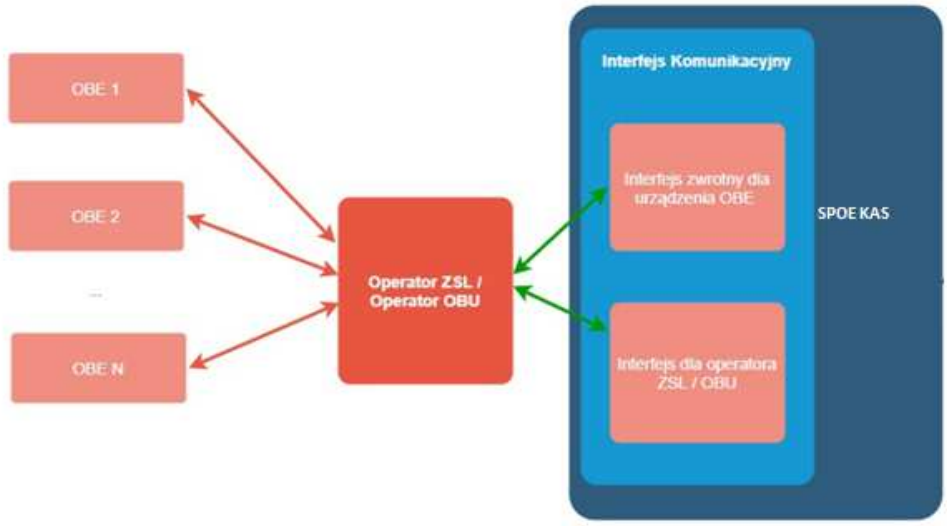
A. interfejsy danych SPOE KAS akceptują dane geolokalizacyjne dostarczane przez mechanizm REST-JSON oparty na protokole HTTPS z metodą HTTP POST;
B. dostarczone dane muszą być wyposażone w struktury danych JSON, które są kompatybilne z aktualnym schematem JSON – SPOE KAS. Interfejs danych SPOE KAS sprawdza 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 500 pozycji geolokalizacyjnych dla różnych urządzeń geolokalizacyjnych lub dla tego samego urządzenia geolokalizacyjnego.

3.10 Sprzężenie zwrotne 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 z użytkownikiem końcowym. Urządzenia OBU wykorzystywane u Operatora ZSL lub Operatora OBU, które nie posiadają możliwości komunikacji z użytkownikiem mogą być powiązane z aplikacją mobilną SPOE KAS. 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.



Rysunek 2a Komunikacja zwrotna – OBE bez wyświetlacza



Rysunek 3b Komunikacja zwrotna – OBE z wyświetlaczem

3.10.1 Interfejs zwrotny dla Operatora ZSL lub Operatora OBU

W Systemie przewidziano wdrożenie kanału niewizualnego pozwalającego na weryfikację stanu zarejestrowanych urządzeń w ramach systemu Operatora ZSL lub Operatora OBU. 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. 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”). Proponowana zawartość komunikatu zwrotnego jest następująca:

```
{
	"serialnumber": {
		"type": "integer",
		"format": "int64",
		"description": "identyfikator OBE unikalny w ramach SPOE KAS "
	},
	"code": {
		"type": "integer",
		"format": "int64",
		"description": "biznesowy kod błędu"
	},
	"description": {
		"type": "string",
		"description": "opis błędu"
	},
	"action": {
		"type": "string",
		"description": "akcja podjęta w wyniku wykrycia błędu"
	},
	"reason": {
		"type": "string",
		"description": "powód wygenerowania błędu"
	},
	"errorTimestamp": {
		"type": "string",
		"format": "date-time",
		"description": "czas wygenerowania błędu"
	}
	„dataId”:{
		 „type”: „string”,
		„description”: „unikalny identyfikator rekordu danych w systemie źródłowym”
	}
}
```

3.10.2 Komunikaty zwrotne na OBE

OBE, które nie posiada możliwości wyświetlania komunikatów, do prawidłowego działania może być powiązane z aplikacją mobilną SPOE KAS umożliwiającą odbiór komunikatów. 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 w 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}$"
        }
}
```


3.11 Zastosowanie certyfikatów

Operator ZSL, Operator OBU łączy się z dedykowanym portalem SPOE KAS. Zakłada na nim konto lub już je ma. Wyświetla się główne okno portalu. Użytkownik wybiera w menu Formularze → Formularze SPOE KAS.
Potem klika w zakładkę Rejestracja usług dla Operatora ZSL lub Operatora OBU i urządzeń GPS w ramach usług i wybiera formularz: REJESTRACJA USŁUG ZEWNĘTRZNYCH SYSTEMÓW LOKALIZACYJNYCH (ZSL) OPERATORA.

Użytkownik wypełnia pola formularza. Między innymi w polu **Żądanie podpisania i wystawienia certyfikatu dla domeny wskazanej przez operatora usługi 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+TQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBADjODu1l
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.

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 PUT --cert ./certyfikat.pem --key ./fd1.key -H 'Content-Type: application/json' -H 'cache-control: no-cache' -d '[{"id": "1960472", "dev": "ALBS8_74718", "lat": 52.17264488, "lon": 21.1956136, "alt": 140.0, "tsp": 1505893301000000, "spd": 0.0, "acc": 15.17, "brg": 0.0},{"id": "1960473", "dev": "ALBS8_74718", "lat": 52.17264546, "lon": 21.195608, "alt": 138.0, "tsp": 1505896249000000, "spd": 10.0, "acc": 15.17, "brg": 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 ZSL lub Operatora OBU

Do obowiązków Operatora usługi 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 dedykowane 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 SPOE KAS 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.

4 Zalecenia ogólne

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;
- wielkości bufora danych w zakresie od 250mb do 300mb; podstawowe ustawienie wyjściowe to 300mb;
  Wielkość bufora danych musi umożliwiać przechowywanie danych globalizacyjnych o zawierających atrybuty wskazane w rozdziale 3.10.01 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 3.4JSON
- częstości retransmisji danych w przypadku problemów z komunikacją w zakresie od 30 sek do 60 sek; podstawowe ustawienie wyjściowe 1 minuta;

OBU/ZSL musi spełniać następujące wymagania w zakresie GNSS:

- posiada czuły odbiornik GNSS razem z anteną;
- 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 (opcjonalnie);

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;
- zapewnia możliwość pobrania i instalacji oprogramowania i parametrów konfiguracji przez sieć komórkową;
- Oprogramowanie wszystkich modułów sprzętowych można zaktualizować zdalnie przez sieć komórkową lub interfejs serwisowy;

Opcjonalne: OBU/ZSL może posiadać możliwość odbierania komunikatów z 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, urządzenia przechowuje dane z pamięci nieulotnej i wyłącza się prawidłowo.
  - OBU posiada wbudowany akumulator pozwalający na kilkugodzinną pracę w przypadku braku napięcia zasilającego.
  - OBU posiada baterię pozwalająca na działanie pamięci trwałej co najmniej 7 lat,
  - OBU może być zasilane napięciem od 9V do 32 V.

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

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

5 Wymagania prawne i normatywne

Rozdział ten zawiera wymagania prawnie i normatywne dotyczące poboru opłat.

Dokument	Wersja	Zawartość
Decyzja 2004/52/EC1	6 października 2009	Decyzja komisji europejskiej w sprawie definicja europejskiej usługi opłaty elektronicznej i jej elementy techniczne
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 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 stosowania w elektronarzędziach bezprzewodowych i ogniwach guzikowych o niskiej zawartości rtęci
ISO DIS 12813	28 września 2018	Elektroniczne pobieranie opłat-autonomiczne systemy kontroli zgodności
ISO 13141	1 czerwca 2017	Elektroniczne pobieranie opłat-komunikacja powiększenia lokalizacji dla autonomicznych systemów