Ministerstwo Finansów

Technical requirements for the transfer of geolocation data necessary for the electronic toll collection for OBU and ZSL Operators

Warsaw 29/04/2021

Contents

Dictionary of terms

Term	Description
OBE	(Eng. On Board Equipment) - a toll system component located in a moving vehicle. For example: mobile devices (equipped with free software provided by KAS), a device providing information for an external locating system (ZSL), and on-board units (OBU) using satellite positioning and data transmission technologies.
OBU	(Eng. On Board Unit - a device installed in a vehicle to collect the Electronic Toll, providing information for the OBU operator's system.
OBU operator	The OBU service management company.
ZSL operator	The ZSL service management company.
Operator	ZSL operator and/or OBU operator
ZSL	- a system independent of the SPOE KAS that provides information on vehicle location. They are solutions by commercial companies for tracking the location and movement of vehicle fleets.
JSON	(Eng. JavaScript Object Notation) - a data exchange format.
JSON Schema	Defines the data structure in JSON.
MCC	(Eng. Mobile Country Code) - a unique wireless network country of operation identification number.
MNC	(Eng. Mobile Network Code) - a wireless network (operator) identification number unique within a given country.
Jamming	GNSS signal jamming by electronic devices.
Spoofing	Attacks on an ICT system by impersonating another element of the IT system.
EGNOS	(Eng. European Geostationary Navigation Overlay Service - the European GPS and GLONASS systems and, in the future, the Galileo system.
PEM	(Eng. Privacy Enhanced Mail) - a file format for storing and sending cryptographic keys, certificates, and other data defined in RFC 7468.
Base64	Used to encode a sequence of bytes. Defined in RFC 4648.
TLS	(Eng. Transport Layer Security, a standard Internet cryptographic protocol that ensures data transmission confidentiality and integrity, server (sometimes client) authentication. This is a SSL protocol extension.
SSL	(Eng. Secure Socket Layer) - a standard cryptographic protocol used for secure transmission of documents over computer networks.
CSR	(Eng. Certificate Signing Request - a request to sign a certificate; an encrypted message sent to the issuer in the process of applying for an SSL Certificate. During CSR generation, there is also a private key created.
GPS	(Eng. Global Positioning System - an American radio navigation system based on satellites.
GNSS	(Eng. Global Navigation Satellite System - a global navigation system covering the whole Earth. For example: GPS.
SPOE KAS	The Electronic Toll Collection System of the National Revenue Administration

1 Introduction

The SPOE KAS is used for toll collection based on GNSS techniques. The Act of 6 May 2020 amending the Act on Public Roads and some other acts defines the principles of toll collection by means of mobile devices, external location systems (ZSL) and on-board units (OBU). There must be OBE (On-Board Equipment) installed in the vehicle. Data from OBE devices are transferred to the SPOE KAS via the

OBU Operator or ZSL Operator. It is also possible to transfer location data by means of a mobile application (**this application is not discussed in this document**). Fig.1 shows a supporting mobile application that may be used to display the SPOE KAS feedback, e.g. balance status, to the driver. For an OBU with a display, it is possible to send feedback to the OBU via the Operator's system. The messages are sent to the OBU Operator who sends them to the appropriate OBU devices to which they are addressed. Data from the locating devices is sent to the Operator's Proxy Server and then transferred to the input interface of the SPOE KAS.

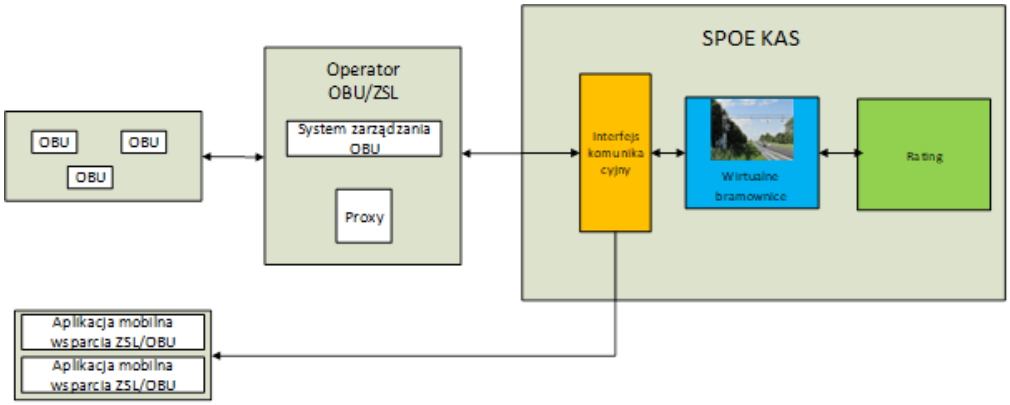


Figure 1 1 Main system components discussed in the document

This document describes the technical requirements for transmitting geolocation data necessary for electronic fee collection, in particular the technical specification of the interface, communication and encryption protocols and the method of communication authentication by the OBU or ZSL Operator.

2 Registration interfaces

The process of registration of services and devices will be carried out in accordance with the rules described in detail in the Technical Specification of Communications and Communication Interfaces of the ZSL/OBU Operator. The Specification allows the registration and updating of data through a visual HTML interface (dedicated forms) or through a non-visual web service (SOAP). Communication with the use of non-visual services is based on structured xml messages, compliant with the specification of data exchange with the PUESC portal.

2.1 Registration of location data transmission services by the Operators

The Operator may choose the scope of the service provided for two systems: SENT-GEO and SPOE KAS. The service may be provided to SENT-GEO, SENT-GEO, and SPOE KAS or only SPOE KAS. Registration of ZSL Operators or OBU Operators consists of the following steps:

a. The Operator sends to the SPOE KAS
   i. a list of IP numbers of the servers from which it will be transferring data in the future;
   ii. a request for an SSL/TLS client certificate;
   iii. a complete address of the feedback interface (main and dedicated to obtain a token authorizing feedback communication according to the OAuth2.0 standard) and authentication data: client id (login), client secret (password)), scope (scope of rights), grant type (type of rights),
   iv. contact details of the service administrator on the Operator's side,

b. As feedback, the Operator receives
   i. the Operator's service number registered in the SPOE KAS,
   ii. the URL of the SPOE KAS service dedicated to communication with the Operator's service (this is the address of the individual interface used to exchange data with the SPOE KAS); In the case of SENT-GEO registration, a second independent interface is transferred to the geolocation data port according to the adaptation in the specification of the data connector for this system
   iii. SSL/TLS certificate of the customer issued by SPOE KAS certification center

2.2 Registration of locating devices by the Operator

Registration by the Operator of ZSL or OBU locating devices in the SPOE KAS includes the following steps:

a. The Operator sends to the SPOE KAS i.a.:
   i. technical identifiers of the end user's GNSS location devices associated with the Operator's service

b. As feedback, the Operator receives i.a.:
   i. the end user's GPS device number linked to the technical identifier of the GPS device (link 1 technical identifier = 1 GPS device number) and a password (PIN) enabling connection of the device with the SPOE KAS application.

When transmitting, the operator provides the technical number for which the business identifier was received in the "serialnumber" field. Do not send the values of the business IDs received in the "serialnumber" field.

3 Proxy Server <-> SPOE KAS communication

3.1 Transmission by the ZSL Operator or the OBU Operator location data from devices indicated by the End User to SPOE KAS

The ZSL Operator or OBU Operator provides the SPOE KAS with location data from devices indicated by the end user:

a. to the service available at the address provided during the registration of the Operator's localization service,
b. using the HTTPS protocol to authorize itself with an issued client certificate,
c. Using the REST mechanism and HTTP POST method in JSON format, as per the current scheme hereinafter referred to as JSON Schema.

The data transmission costs remain with the user and depend on the selected operator.

3.2 Location data transmitted

The location data record must have the following information, with the exceptions described in * and **:

- location data record number,
- technical identifier of the device
- latitude
- longitude
- altitude above sea level*,
- time stamp of the location data collection time
- speed
- location data transfer error*;
- azimuth,
- class of the event**:
    - location,
    - turning on the device (turnon) - usually involves pressing a button; if there is no such button, it is often connected to the power supply; sometimes the device is always turned on, then it is recommended to generate a "startjourney" event after changing the position of the vehicle after a long period of inactivity,
    - turning off the device (turnoff) - similar to turning on the device,
    - beginning the route (startjourney) - detection of a change in position after a period of inactivity, usually it is half an hour,
    - ending the route (endjourney) - reaching the destination point, it can also be synonymous with turning off the ignition,
    - disconnecting from the power supply (plugout),
    - connection to the power supply (plugin),
    - GSM online (gsmonline) - GSM range greater than 0,
    - GSM offline (gsmoffline) - GSM range 0,
    - GNSS online (gpsonline) - the number of visible satellites at least 3,
    - GNSS offline (gpsoffline),
    - jamming,
    - spoofing - an attempt to impersonate another device and sending false data; due to the fact that not every device is able to detect such intrusion, this functionality is recommended and not required;
- lac – Location Area Code (area identifier where Cell ID is unique)*,
- mcc – Mobile Country Code*,
- mnc – Mobile Network Code*,

- cid – GSM cell area identifier (Cell ID)*,
- number of satellites used to establish the position,
- number of visible satellites*.

The exact specification of the fields is presented in chapter 3.4.
*- in accordance with point 3.4 is not required, but these fields shall be included in the data record if available.
- not required **except for the location (location), which is mandatory to provide as part of the event classes.

3.3 Frequency of data transmission

The ZSL Operator, OBU Operator **MUST** transmit data to the SPOE KAS at a frequency of **1 data packet per minute (60 seconds)**. The data packet contains location data and events generated at the OBE level (such as switching on the ignition, starting, stopping, switching off, etc.). in accordance with point 3.2). Location data **MUST** be collected at a frequency of **1 location per 5 seconds**. In one packet, the operator can send data from many devices (the packet size limit is 5 MB).
The frequency of data collection and transmission is a necessary condition and is not subject to change.

3.4 JSON structure

The data will be transmitted in the form of a JSON array, in which individual elements are JSON objects containing single route recording points. The description of individual fields, validation rules and information on field maturity in Schema_nkspo_v_1_0 are shown in Table 1.

Table 1. Schema_SPOE_v_1_0

Name	Description	Validation rule	Required
dataId	A unique and incremented (at the OBE level) identifier of the record in the source system, a variable used for verification purposes during the test period and useful for sorting - completing data when packages are not be shipped in sequence.	"type": "string", minLength": 1,"maxLength": 32, "examples": ["1", "1960472"]	Yes
serialNumber	A unique locator identifier, a maximum length of 50 characters allowed, lowercase and uppercase Latin letters from ranges (a-z) and (A-Z), digits (0-9) and hyphen-minus (-) and underscore (_), which are a subset of the ASCI (eng. American Standard Code for Information Interchange) are allowed. Not case sensitive.	"type": "string", "minLength": 1, "maxLength": 50, "pattern": "^[a-zA-Z0-9\-_]{1,50}$", "examples": ["00000000000B1", "35A058060495422C7934"]	Yes
latitude	A latitude downloaded from the GNSS transmitter, WGS 84 reference system, recommended minimum number of decimal places: 6, maximum number of decimals allowed: 10.	"type": "number","minimum": -90.0, "maximum": 90.0, "multipleOf": 0.0000000001, "examples": [52.0375868826, 52.172644]	Yes
longitude		type": "number","minimum": -180.0,	Yes

Name	Description	Validation rule	Required
	A longitude downloaded from the GNSS transmitter, WGS 84 reference system, recommended minimum number of decimal places: 6, maximum number of decimals allowed: 10.	"maximum": 180.0, "multipleOf": 0.0000000001, "examples": [21.1956136, 20.026094]	
altitude	An ellipsoidal altitude downloaded from the GPS transmitter, unit [m], maximum number of decimals allowed: 2.	"type": ["number", "null"], "minimum": -1000.0, "maximum": 4000.0, "multipleOf": 0.01, "examples": [10.0, 200.02]	No
fixTimeEpoch	A time stamp with the date and time downloaded from the GNSS transmitter, associated with the geographical position from a given record, UTC time zone, the SPOE KAS time stamp has a format similar to Epoch / Unix Timestamp, but given with microsecond accuracy (16 digits), so it is the number of microseconds that elapsed from '00:00:00 Coordinated Universal Time (UTC), Thursday, 1 January 1970', the minimum value indicates 2017. 09.20 00:00:00 UTC, integer.	type": "integer", "minimum": 1505865600000000, "examples": [1506086623000000, 1511273867317000]	Yes
gpsSpeed	A speed of movement downloaded from the GNSS transmitter – unit [m/s], maximum number of decimal places allowed: 2. Maximum speed allowed: 56.00 [m/s].	"type": "number", "minimum": 0.0, "maximum": 56.0, "multipleOf": 0.01, "examples": [3.21, 20.0]	Yes
accuracy	Location accuracy downloaded from GNSS transmitter – circle radius in meters, maximum number of decimal places allowed: 2.	"type": "number", "minimum": 0.0, "multipleOf": 0.01, "examples": [10.14, 30.0]	No
gpsHeading	Azimuth – unit [degree], maximum number of decimals allowed: 2.	"type": "number", "minimum": 0.0, "maximum": 360.0, "multipleOf": 0.01, "examples": [40.14, 230.0]	Yes
eventType	type of event	„type": „string" „enum": ['turnon', 'turnoff', 'startjourney', 'endjourney', 'plugout', 'plugon', 'gsmonline', 'gsmoffline', 'gpsonline', 'gpsoffline', 'jamming', 'spoofing', 'location']	Yes
lac	GNSS base station ID	„type": „string" „pattern": "^[A-Fa-f0-9]{4}$"	No
mcc	GSM operator country identifier	„type": „string"	No

Name	Description	Validation rule	Required
		„pattern”: "^[0-9]{3}$"	
mnc	GSM operator network identifier	„type”: „string” „pattern”: "^[0-9]{2.3}$"	No
mobileCellId	GNSS network cell ID	„type”: „string” „pattern”: "^[A-Fa-f0-9]{ 9}$"	No
satellitesForFix	number of satellites used for position determination	„type”: „integer „maximum”: 90 „minimum”: 0	Yes
satellitesInView	number of satellites visible during position determination	„type”: „integer” „maximum”: 90 „minimum”: 0	No

Location data must be transmitted from on-board units using EGNOS (European Geostationary Navigation Overlay Service). The system significantly increases the accuracy and reliability of the position obtained from the GPS, which is important for SPOE KAS.

Moreover, data whose coordinates are outside Poland are rejected, The rules are presented in **Table 2**.

Table 2. Rules for rejecting data from outside Poland

Rule code	Rule	Notes
B-W06	If lon < 14.116667	Rejection of data when longitude is less than 14.116667. Applies to the western border,
B-S06	If lat < 49.0	Rejection of data when latitude is less than 49.0. Applies to the southern border.
B-E06	If lon>24.15	Rejection of data when longitude is less than 24.15. Applies to the eastern boundary.
B-N06	If lat > 54.835778	Rejection of data when latitude is greater than 54.835778. Applies to the northern border.
L-SSW-CZ	If the geographical coordinates meet the condition: 54.9 - lat - 0.3 * lon > 0	Rejection of data in the southwest. Applies to the border with Czech Republic.
L-ESE-UA	If the geographical coordinates meet the condition: 1.25 * lon + 20.375 - lat > 0	Rejection of data in the southeast. Applies to the border with Ukraine.
S-NE-RU	If the geographical coordinates meet the condition: lon > 19 AND lat > 54.5	Rejection of data in the northeast. Applies to the border with the Russian Federation.

3.5 Data transmission method

The data to the SPOE KAS data interface will be sent using REST mechanism via HTTPS and the HTTP POST method. The transmitted data should be included in a JSON structure according to the JSON schema described in this document. Each data sample collected during a single measurement that contains location data collected at the same time (date and time of acquisition of coordinates – time stamp containing date and time) is transferred as a single JSON object. In order to limit the number of transmitted data packets, data from one vehicle or from different vehicles saved within a JSON object

is transmitted as elements of a JSON array, which creates a single data packet. A single JSON table can contain from 1 (one) to 10000 (ten thousand) JSON objects.
The maximum allowed size of a single packet expressed in bytes is 5 MB (in words, five Mega Bytes).

3.6 Security of transmitted data

Data transfer to the SPOE KAS input interface (first stage of streaming) will be carried out with certificates only. The security set includes:

- a dedicated URL interface,
- a restriction in the access for the indicated IPs,
- TLS 1.2,
- authorizations via a client certificate.

3.7 Data validation – responsibilities of the ZSL Operator and the OBU Operator

The Operator is obliged to validate the data packet using the current JSON schema before passing it to the SPOE KAS data interface. The validation must be carried out using software that supports scheme-based validation according to the version of the JSON Schema specification given in the JSON Scheme of the SPOE KAS data interface. The current JSON Scheme of the SPOE KAS data interface is compliant with the Schema JSON Draft-06 specification (http://json-schema.org/draft-06/schema#).
Moreover, the Operator has to verify the rules from Table 2 on its own and reject the data that does not meet the criteria included in Table 2. Thus, the Operator should separate the redundant data and send **only** data from Poland to the SPOE KAS system.

3.8 List of messages for the ZSL Operator and OBU Operator

As far as data validations are concerned, the basic principle is that any packet that has not been accepted should be resubmitted, unless it conflicts with JSON Schema, and then it should be corrected (if possible) and resubmitted (non-repairable packets should be skipped).

Table 3 contains the most frequent messages in the data validation process.

Table 3. List of most frequent messages

Message	Rule/Warning	Operator's action
HTTP 200 JSON: {"result": "OK"}	confirmation of the correct validation of the submitted JSON packet	Not required.
400 Bad Request	the delivered data packet does not conform to the applicable JSON schema or does not meet any other requirements	The whole packet is rejected, the operator must eliminate the data frames that do not meet the JSON schema and resend the packet
	The package is sent as a single JSON object	The object should be sent as a list
	if any of the individual packets is rejected,	it should be sent after correcting the error or omitted.
401 Unauthorized	data was not delivered due to an authorization error	The Operator must check what has happened.
	Authentication certificate not found	A certificate must be attached
	Incorrect private key used to verify the certificate	You must include the appropriate key used to

		generate the certificate generation request
	Wrong protocol used for communication (http instead of https)	Use the appropriate transmission protocol
415 Unsupported media type	Validation error of the frame	The structure of the incoming data frame should be improved
500 Internal Server Error -		re-try until successful. The SPOE KAS team must be informed about this case.
503 Service Unavailable —	service unavailable	The operator should repeat the attempt to deliver the data until it is done. The SPOE KAS team must be notified in such a situation.
404 Wrong address	Resource unavailable	The destination address of the input interface must be verified

NOTE:
"result": "OK" indicates that the data is syntactically correct (it meets the scheme).
Each of the warnings is an independent result of a business rule. The action field determines what effect a given rule has on the data indicated in a warning. Rules with the "drop" action have higher priority than rules with the "pass" action.

Drop rules occur for:

1) unregistered devices;
2) data from outside Poland.

In the case of the rules, this may be interpreted as the absence of a legal basis for processing the data indicated in the warning. This is tantamount to the lack of transmission of geolocation data to the system.

3.9 Information necessary to connect the ZSL Operator or OBU Operator to the NSKPO

Connection of the ZSL Operator or OBU Operator to the SPOE KAS uses certificates and is based on forms of a dedicated SPOE KAS portal.

Summary of some technical details to be provided to the ZSL Operator or OBU Operator:

A. SPOE KAS data interfaces accept geolocation data provided by REST-JSON mechanism based on HTTPS protocol with the HTTP POST method;
B. the provided data must be provided with JSON data structures that are compatible with the current JSON scheme – SPOE KAS. The SPOE KAS data interface checks the correctness of the provided data against the mandatory JSON schema and rejects any incompatible data;
C. JSON Schema enables the provision of data in data packets, each packet can contain up to 10000 (say ten thousand) geolocation positions for different geolocation devices or for the same geolocation device.

3.10 Feedback between the SPOE KAS and ZSL and OBU Operators

In feedback communication, two basic channels are distinguished. The channel with the ZSL Operator or OBU Operator and with the end user. OBU devices used by the ZSL Operator or OBU Operator

without the possibility of communication with the user may be linked to the SPOE KAS mobile application. If OBE has a display, messages are forwarded to the Operator, who, according to the given identifier, redirects them to the appropriate device. If OBE does not have a display, it is possible to associate it with the SPOE KAS mobile application which receives the messages and displays them to the user.

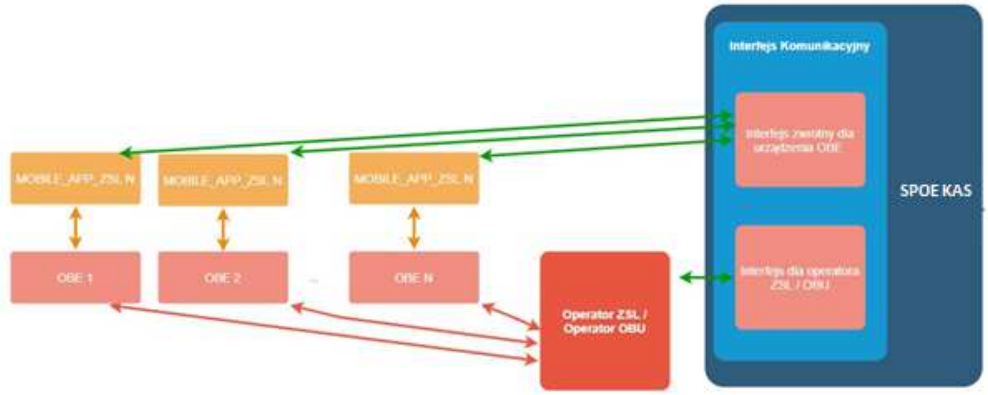


Figure 2a Feedback communication – OBE without a display

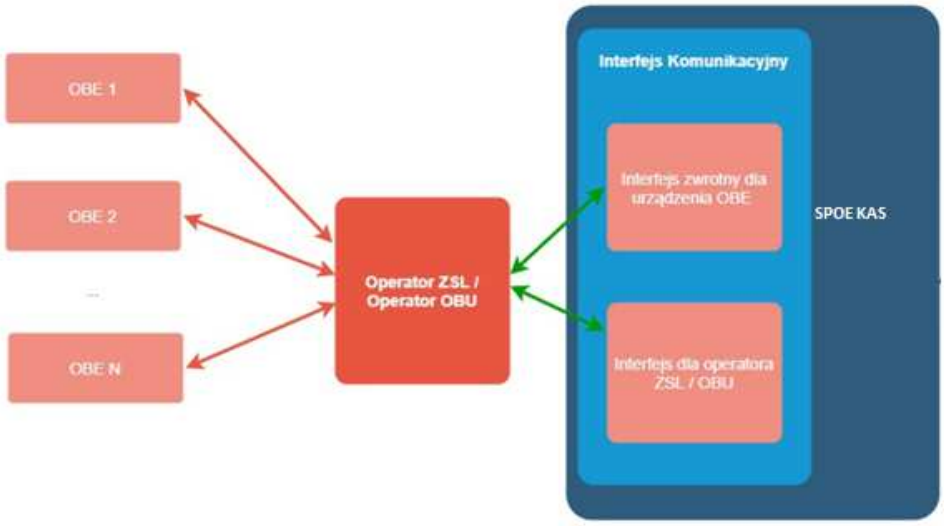


Figure 3b Feedback communication – OBE with a display

3.10.1 Feedback interface for the ZSL Operator or OBU Operator

The System provides for the implementation of a non-visual channel allowing for getting feedback messages. As a transmission protocol, an asynchronous interface based on HTTPS protocol is used for this purpose, which uses OAuth 2.0 standard authentication. Messages are sent to a defined IP address which is dedicated for this purpose on the side of the ZSL Operator / OBU Operator. Each time a data frame is received, the data is validated. If each location data passes the validation correctly, a general message of class 200 is returned. If the selected record generates an error code, an additional error information is returned for each incorrect record. The error may cause the data to be rejected ("action": "drop"), or a warning that allows further processing of the data ("action": "pass"). The

purpose of the feedback communication is to provide information about the balance and warning messages detected during system stream processing. The proposed content of the return message is as follows:

```
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: the type of event
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 Feedback messages on OBE - balance information

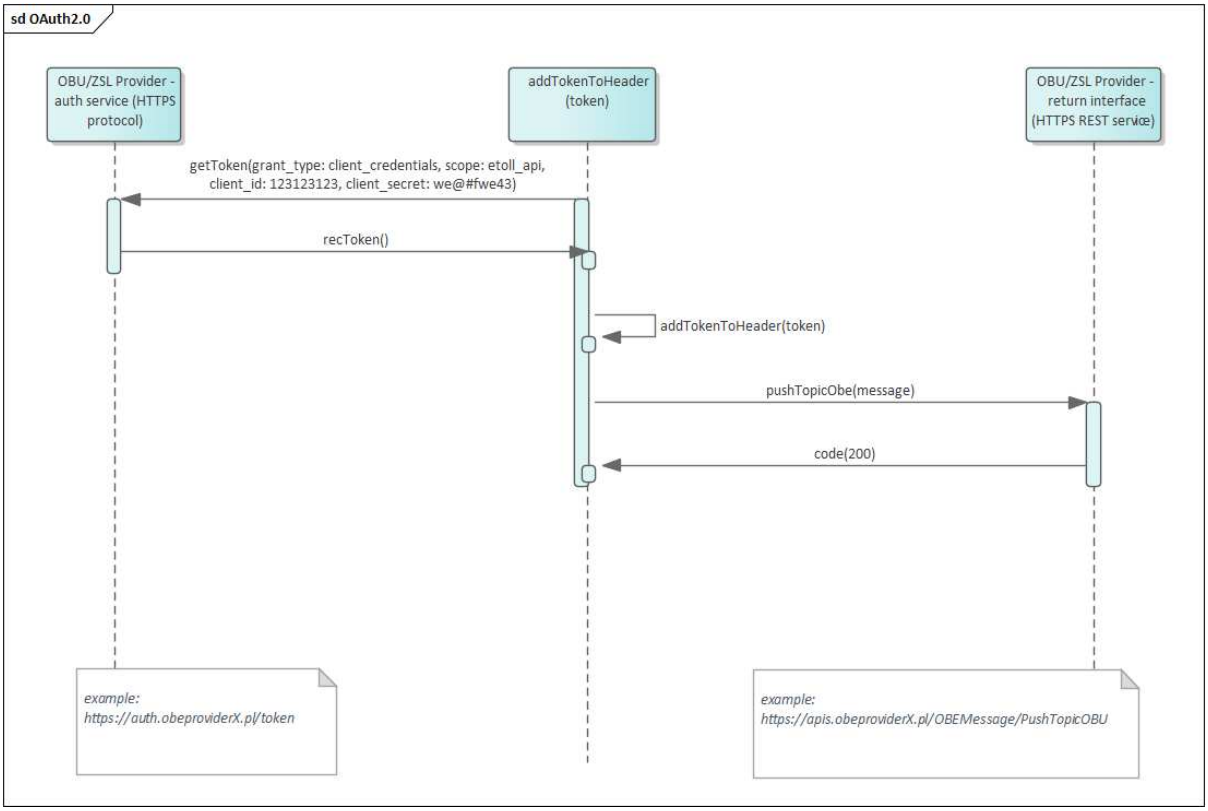
OBE that does not have the ability to display messages may be linked to the SPOE KAS mobile application that allows for message reception. The messages concern the current balance status, information on the toll section driven or the device registration status. The link is made at the level of services related to the customer service module where through the Internet portal the user logging into his account makes a link between OBE and the SPOE KAS mobile application which has its unique business identifier. If the transmitting device features a display according to the appropriate specification, then information containing a message for the appropriate OBE is sent to the ZSL Operator or OBU Operator, from where the message is transmitted to the target device. The content of the feedback message is described according to the following scheme:

```
{
    "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 OBE feedback - OAuth2.0 specification

In order to facilitate reverse communication, the Operator should configure communication security in accordance with OAuth2.0 standards. The sequence diagram for communication is shown below:



In order to establish a connection for return communication, please provide the URL for:
- the target endpoint for the return communication

- the endpoint to generate a token

Values for parameters for the token generating service:
- grant_type (client_credentials the best)
- scope
- client_id
- client_secret
Example:
request.json: {‘grant_type’:’client_credentials’, ‘client_secret’:’we#er!2e’, ‘client_id’:11111, ‘scope’:’etoll_api’}

Attributes that should be returned in the json structure:
- access_token
- expires_in (constant is the best, that is 3600 which is 1h)
- token_type (constant Bearer the best)
- scope (any)

Example:
response.json : {‘acces_token’:’sad3rf34g4g45gf23424rwef42f2f23ewf24f2223234343’, ‘expires_in’:3600, ‘token_type’:’Bearer’, ‘scope’:’etoll_api’}

The data sent from the system to the Operator meets the scheme included in the interface definition below.

```
--- YAML FILE BEGIN ---
openapi: 3.0.1
info:
  version: '3.0'
  title: 'PushTopicOBU'
  description: 'The PushTopicObu interface is used to send information about the balance of the billing account associated with a given OBE and the type of contract in force (pre-paid or post-paid) to be transferred to the OBE device. The information is sent after each toll payment is calculated.  Along with the information on the balance, a marker is provided whether the balance is below the minimum threshold and should be topped up soon. The fact that the balance is low or zero should be presented on the OBE with an appropriate message and an audible signal. Initialization module: MPDS (communication interface), receiving module:

endpoint of the OBU opearator.
paths:

  /PushTopicOBU:
    post:
      tags:
      - PushTopicObu
      summary: Transmission of a message to an OBE operating within the respective system
      description: The message is in text form. The message includes information about the toll section traveled and the fee calculation, as well as, in the case of a pre-paid agreement, information on the current balance
      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 Use of certificates

The ZSL Operator, OBU Operator connects to a dedicated SPOE KAS portal. He creates an account on it or already has one. The main portal window is displayed. The user chooses Formularze → Formularze SPOE KAS from the menu.
Then the user click on the Rejestracja usług dla Operatora ZSL lub Operatora OBU i urządzeń GPS w ramach usług tab and select the form: REJESTRACJA USŁUG ZEWNĘTRZNYCH SYSTEMÓW LOKALIZACYJNYCH (ZSL) OPERATORA.

The user fills in the form fields. Inter alia, in the field **Żądanie podpisania i wystawienia certyfikatu dla domeny wskazanej przez operatora usługi Operatora ZSL lub Operatora OBU**, the user pastes a CSR (eng. Certificate Signing Request). A CSR is generated on the basis of its private key. Openssl may be used (www.openssl.org). If the user already has a private key (e.g. private.key file), the command has the following structure in Linux environment:

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

If the user does not have a private key, it can be generated for example:

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

(4096 bits length gives better security level than 2048 key)

An example of a file containing a private key is shown in Fig. 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-----
```

Fig. 4. Example of a file with a private key

An example of a file containing CSR is shown in Figure 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-----
```

Fig. 5. Example of a file with a CSR

More details can be found at:
https://tech-itcore.pl/2012/07/04/generowanie-wlasnego-certyfikatu-ssl/
https://uk.godaddy.com/help/apache-generate-csr-certificate-signing-request-5269

The form **must include a possibility** to provide an **e-mail address** to which the user will receive a reply form.

In the form with the answer the ZSL Operator, the OBU Operator receives the Client Certificate encoded in base64 format.
It must be decoded. **Do not add BEGIN/END CERTIFICATE lines** to it, it is only necessary to use a tool that can decode the text encoded in Base64, e.g.:

- Notepad++ > Wtyczki > Mime Tools > Base64 Decode
- openssl base64 -d -in plik_z_zakodowanym_certyfikatem.txt -out certyfikat.pem
- Websitehttps://www.base64decode.org/
- Certutil -decode plik_z_zakodowanym_certyfikatem.txt certyfikat.pem (for Windows using the command line).

An example of a certificate in base64 is shown in Fig. 6.

Fig. 6. Base64 encoded certificate

An example of a certificate decoded in PEM (eng. Privacy-Enhanced Mail) format is shown in Figure 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
rblxdNRBl5QnzvFVBaXvBhzROgB812tArfMCIfVxlYwCTZvajnDyWbm5lQwWcXUv
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
ayBJbmZvcm1hY3lqbnljaCAoWi02KTEdMBsGA1UEAwwUU0VOVCBHRU8gSVRMIEJv
```

Fig. 7. Example of a decoded certificate

After decoding, you receive a file containing up to three certificates in PEM format:

- Client certificate,
- CA (Authorization Center) level 1 certificate, which issued the client certificate,
- CA (Authorization Center) level 0 certificate, which issued the CA level 1 certificate.

Each certificate begins and ends with the following lines:
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

The above lines mark the beginning and the end of individual certificates.

The scope and use of data that are used to secure TLS communication is different and depends on the system / application used by the entity. However, typical requirements of SSL/TLS tools/components include the use of the following elements during SSL authentication:

- a client certificate;
- a private key, which secures the possibility of using the client certificate only by the entity that holds it;
- a certification / certificate chain, which authenticates the client certificate as a certificate issued by the relevant CA and contains:
  a CA (Authorization Center) level 1 certificate, which issued the client certificate,
  a CA (Authorization Center) level 0 certificate, which issued the CA level 1 certificate.

In a Linux environment, the connection to the SPOE KAS may be tested by the curl tool. A sequence of commands is shown below. Certyfikat.pem means a received certificate that has been decoded from base64 to PEM format. Whereas fd1.key means the private (decrypted) key used to generate CSRs.

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

Note 1: The address https://cloud.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001 should be replaced with the address received from the form received by e-mail, it concerns the content of the field **Adres URL usługi SPOE KAS dedykowany do komunikacji z usługą Operatora ZSL lub Operatora OBU**.

Note 2: X.509 SSL/TLS client certificate on the ZSL's or the OBU Operator's side

The responsibilities of the ZSL Service Provider or OBU Operator include:

1. obtaining the above-mentioned certificate:
   a. the first one as a result of service registration;
   b. each subsequent one before the expiration of 365 days after the previous certificate was issued;
2. using the current X.509 SSL/TLS client certificate to authenticate communication with the SPOE KAS data interface.

The first X.509 SSL/TLS client certificate is issued in response to sending to the SPOE KAS via a dedicated request portal for issuing an X.509 client SSL/TLS certificate via one of the two available forms of communication:

1. an XML document;
2. the service registration form filled in on the SPOE KAS service site in the dedicated SPOE KAS portal.

Another certificate may be obtained by sending a X.509 SSL/TLS client certificate request to the SPOE KAS via the dedicated portal via one of the two available forms of communication:

1. an XML document;
2. the service data update form filled in on the SPOE KAS service site in the dedicated portal.

The X.509 SSL/TLS client certificate used to authenticate the ZSL Operator or OBU Operator during communication with the SPOE KAS data interface is the first of the certificates returned by the SPOE KAS in response to sending an XML form/document. Each of the returned certificates starts with the line "-----BEGIN CERTIFICATE-----" and ends with the line "-----END CERTIFICATE-----".

The expiration date of an X.509 SSL/TLS client certificate is available for viewing with the free OpenSSL toolkit using the following command:

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

where:

- plik_z_certyfikatem_klienta_x509.pem is an example name of a file containing an X.509 SSL/TLS client certificate issued by the SPOE KAS.

Below is a sample response to the above command:

notAfter=Sep 30 08:30:58 2020 GMT

where:

- notAfter – the label of the field "not after" from the X.509 certificate, which contains the final date of validity of the certificate, after which, you should neither use it nor trust it;
- Sep – a three-letter abbreviation of the month's name, in this case it is the abbreviation for September;
- 30 – day;
- 08:30:58 – hour, minute and second;
- 2020 - year;
- GMT – a three-letter abbreviation of the time zone name, in this case it is an abbreviation of Greenwich Mean Time, meaning that in order to get an hour for the Europe/Warsaw time zone you have to add 2 hours for summer time and one hour for winter time to the given hour.

4 General recommendations

The transfer of GNSS data by the Operator to the SPOE KAS must ensure:

- Transmission of location data to SOPOE KAS according to the specifications described in this document;
- Queuing (events, location data);
- Remote updating of OBU/ZSL software;
- Self-diagnosis.

Upon request of the SPOE KAS administrator, the Operator's system must allow the Operator's administrator to parameterize at least the following parameters:

  - with the frequency of location data collection, the **basic output setting is 5 seconds**;
  - with the frequency of sending the location data, the **basic output setting is 1 minute (60 seconds)**;

- recommended data buffer size minimum 250MB (that requirement is not mandatory);

  The size of the data buffer must enable the storage of globalization data containing the attributes indicated in chapter 3.10.1 collected at the above indicated frequency and stored on the locator side not less than 10 days (unless previously sent to the SPOE KAS) and events indicated in chapter 3.4 JSON structure

- in case of communication problems, with a retransmission frequency in the range of 30 sec to 60 sec; the **basic output setting 60 seconds**;

OBU/ZSL must meet the following GNSS requirements:

- it has a sensitive GNSS receiver together with an antenna;
- it supports the following networks: GPS, GLONASS, Galileo;
- it supports the EGNOS system;
- The GNSS receiver supports A-GPS to reduce the time before the first location reception;
- The GNSS antenna and its connection to the GNSS receiver is shielded from interference (shielding);
- The GNSS receiver should refresh the position at least once per second;
- The GNSS receiver supports advanced jamming and falsification detection;
- All sensors calibrate automatically.

Optional: Software update of the GNSS Receiver is possible remotely via the cellular network;

The OBU/ZSL must meet the following network communication requirements:

- it has a module for communication with the cellular network together with the antenna;
- it provides remote access and a possibility of bidirectional data exchange with the central system via cellular network;

Optional: OBU/ZSL can receive messages from the SPOE KAS as text messages and can help displaying them to the user. For example, it can be information about the account balance, signaling the passage through the virtual gateway, warning about low account balance.

The OBU/ZSL must meet the following security requirements:

- OBE has a security unit such as the "Secure Access Module (SAM)" responsible for performing encryption algorithms and storing sensitive data such as keys, PIN and others;
- The security unit supports cryptographic algorithms such as encryption/decryption, random number generation, key storage;
- The security unit permanently stores sensitive data in non-volatile memory;
- Communication between the Security Unit and OBU components (such as CPU, modules, memory and others) uses authentication and encryption;
- Software is not significantly slowed down by secure communication between the Security Unit and external components;
- The security unit safely stores a unique ID and provides access to the software;
- The security unit is resistant to active and passive attacks;
- The security unit is resistant to mechanical modifications. Opening the OBU housing or security unit is impossible without leaving traces;
- Every attack attempt is detected, documented and controlled.

Short power outages do not affect the operation of the OBU/ZSL:

- If the OBU is disconnected from the power supply, the device stores data from non-volatile memory and switches off correctly.
- The OBU has a built-in battery for several hours of operation in the absence of the supply voltage.

A system for managing OBU devices must be provided with the said devices The system must in particular make it possible

- To perform remote software updates;
- To perform remote setting of OBU operating parameters;
- To perform OBU status monitoring.

5 Legal and normative requirements

This chapter contains legal and normative requirements for toll collection.

Document	Revision	Content
Decision 2004/52/EC1	06 October 2009	Commission Decision on the definition of the European Electronic Toll Service and its technical elements
Directive 77/649/EEC	27 September 1977	Directive on the approximation of the laws of the Member States relating to the field of vision of motor vehicle drivers
Directive 2002/95/EC	27 January 2003	Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment
Directive 2012/19/EC	04 July 2012	Directive on waste electrical and electronic equipment
Directive 2004/108/EC	15 December 2004	Directive on the approximation of the laws of the Member States relating to electromagnetic compatibility
Directive 2004/53/EC	16 April 2014	Directive on the harmonisation of the laws of the Member States relating to market access to radio equipment
Directive 2014/30/EC	26 February 2014	Directive on the approximation of the laws of the Member States relating to electromagnetic compatibility
Directive 2011/65/EC	08 June 2011	Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment
Directive 2006/66/EC	06 September 2006	Directive on batteries and accumulators and waste batteries and accumulators
Directive 2013/56/EC	20 November 2013	Directive on batteries and accumulators and waste batteries and accumulators as regards placing on the market of portable batteries and accumulators containing cadmium intended for use in cordless power tools and button cells with low mercury content
ISO DIS 12813	28 September 2018	Electronic fee collection – autonomous compliance control systems
ISO 13141	01 June 2017	Electronic fee collection and location enhancement communication for standalone systems