Ministerstwo Finansów

Krajowa Administracja Skarbowa

Technical requirements and rules of transferring geo-location data necessary to collect the electronic amount for the OBU and ELS Operators

Warszawa 22.10.2024

Table of contents

Dictionary of terms

Definition	Description
Base64	Is used for coding a sequence of bites. Defined in RFC 4648.
CSR	(Eng. Certificate Signing Request) – a request for signing the certificate, encoded message is sent to the issuer in the process of applying for the SSL Certificate. During generating CSR also a private key is created.
EGNOS	(Eng. European Geostationary Navigation Overlay Service) – European system supporting the GPS and GLONASS systems, and in the future Galileo.
GNSS	(Eng. Global Navigation Satellite System) – global navigation system covering with its range all the Earth. The example is GPS system.
GPS	(Eng. Global Positioning System) – American radio navigation system based on satellites.
Jamming	Drowning the GNSS signal by the electronic devices.
JSON	(Eng. JavaScript Object Notation) – format of data exchange.
JSON Schema	Defines the data structure in JSON.
MCC	(Eng. Mobile Country Code) – unique identification number of the country, in which a given network of wireless telephone operates.
MNC	(Eng. Mobile Network Code) – unique number in the area of a given country, identifying the network (of the operator) of the wireless telephone.
OBE	(Eng. On Board Equipment) – component of the system of the fee collection system located in the moving vehicle. It can be, for example: mobile devices (equipped with the software free of charge made available by KAS), a device suitable for the external location system (ELS) and onboard devices (OBU), using technology of satellite positioning and data transmission.
OBU	(Eng. On Board Unit) – a device installed in the vehicle in order to collect Electronic Amount, suitable for the system of the OBU Operator.
Operator	Operator ELS and / or Operator OBU.
Operator OBU	Company managing the OBU service.
Operator ELS	Company managing the ELS service.
PEM	(Eng. Privace Enhanced Mail) – format of the file used for memorizing and sending the cryptographic keys, certificates and other data defined in RFC 7468.
PUESC	Platform of Electronic Fiscal-Customs Services
SENT	Transport Electronic Supervision System
SENT GEO	Application intended for drivers and carriers servicing the registered transports registered in SENT
SPOE KAS	System of Collection of the Electronic Fee of the National Fiscal Administration; e-TOLL
Spoofing	Attacks on the data information system by means of impersonating another element of the IT system.
SSL	(Eng. Secure Socket Layer) – standard cryptographic protocol used for safe transmission of documents by means of computer networks.
TLS	(Eng. Transport Layer Security) – cryptographic protocol being a standard on the Internet, assures confidentiality and integrity of data transmission, certification of server, sometimes the client. It is a development of the SSL protocol.
ELS	External Location System – system independent on SPOE KAS which provides information on the location of vehicles. These are the solutions to trace the location and movement of the fleets of the vehicles.

1 Introduction

SPOE KAS is used for collecting amounts on the basis of the GNSS techniques. The act of 6 May 2020 on changing the act on public road and some other acts defines the principle of collecting fees with the use of the mobile devices, external location systems (ELS) and onboard devices (OBU). In the vehicle there must be onboard devices OBE (On-Board Equipment) installed. The data from the OBE devices is transferred to SPOE KAS by means of the OBU Operator or ELS Operator. It is possible also to transfer location data by means of mobile application **(application is not discussed in the document)**. In the Fig. 1 supporting application is indicated, which may be used for displaying feedback from SPOE KAS to the driver, e.g. balance status. In case of OBU with the displayer, it is possible to send feedback to OBU by means of the Operator system. The messages are sent to the OBU Operator, which sends them to the proper OBU deices to which they are addressed. The data from the location devices is sent to the Server of the Proxy Operator and then transferred to the input interface SPOE KAS.

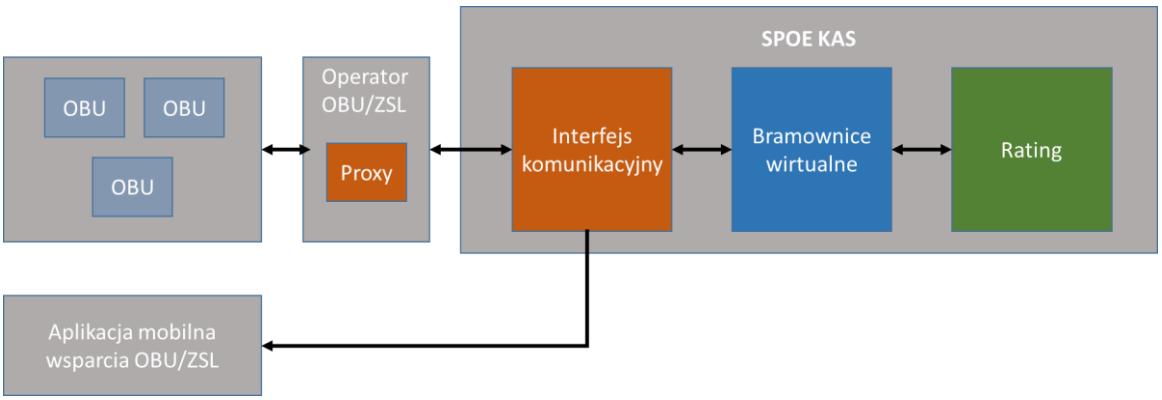

Fig. 1 Main components of the system connected with transferring geo-location data

The document describes technical requirements of transferring geo-location data necessary for collecting electronic amount in particular technical specification of the interface, communication and encoding protocols and the method of communication certification by the OBU Operator or the ELS Operator.

2 Interfaces of the registration

The process of registration of the services and devices will be realized in accordance with the principles described in detail in the Technical Specifications of Messages and Communication Interfaces of the ELS/OBU Operator. The specification allows registration and updating the data by means of the visual interface HTML (dedicated forms) or by means of the non-visual service web service (SOAP). Communication with the use of the non-visual services based on structurised xml messages, consistent with the specification of data exchange with the PUESC portal.

2.1 Registration of the services of sending location data by the Operators

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

a) Operator sends to SPOE KAS (by means of interface):
   i. List of IP numbers of servers from which he shall send data in the future,
   ii. Demand to issue the SSL/TLS certificate of the client,
   iii. optionally complete address of feedback interface (main and allocated for obtaining JWT token authorizing the feedback communication by the OAuth2.0 standard) and certifying data: client id (login), client secret (password)), scope (range of rights), grant type (type of rights). Details of the feedback communication were discussed in point 3.10.
   iv. contact data to the administrator of the service on the side of the Operator,

b) The Operator obtains in return:
   i. number of the Operator service registered in SPOE KAS,
   ii. URL address of the SPOE KAS service dedicated to the communication with the service of the Operator (this is an address of individual interface used for data exchange with SPOE KAS). In case of SENT-GEO registration, the other independent interface is transferred to convey the geo-location data by the rules described in the technical specification to connect the devices to the system
   iii. SSL/TLS certificate of the client issued by the certification center of SPOE KAS service;

2.2 Registration by the Operator of the location devices

The Operator makes registration of the location devices ELS or OBU in SPOE KAS using their technical ID devices. For this purpose, the Operator OBU/ELS:

a) sends to SPOE KAS technical IDs of the location devices connected with the service of the Operator, whereas the IDs may not start nor end with a space or other white marks,
b) obtains in return the business numbers of the location devices connected with the technical IDs of the devices (affiliation 1 technical ID = 1 business number of the device) and a password (PIN) allowing for connecting the device with the SPOE KAS application.

The Operator, during transmitting in the field „serialnumber" provides a technical number for which the business ID was obtained. **One should** send in the field „serialnumber" the values of the business IDs obtained. The value of the ID may not contain spaces nor white marks. Registering a device allows for effective transferring data to SPOE KAS (these devices are active in the system and data is correctly processed by SPOE KAS). Each newly generated business ID (if the service was registered also as a source of data for the SENT-GEO system) is propagated to the SENT-GEO system. There it awaits the activation which takes place by means of sending (by the carrier) a transport SENT document, in which in the field in which the main or the back-up locator the business number will be placed. Until this moment the data is SENT-GEO will be rejected through the SENT-GEO system with the message „unknown-device".

3 Communication Proxy Serwer <-> SPOE KAS

3.1 Transferring by the ELS Operator or the OBU Operator the location data from the devices indicated by the End user to SPOE KAS

The ELS or OBU Operators transfers to SPOE KAS the location data from the devices indicated by the End user:

a) to the service available at the address transferred in return during registration of the location service of the Operator,
b) by means of the HTTPS protocol being authorised with the client certificate issued,
c) with the use of the REST mechanism and the HTTP POST method in the JSON format, consistent with the current diagram hereinafter referred to as JSON Schema.

The costs of data transmission remain on the side of the user and depend on a selected Operator.
The ELS or the OBU Operators undertake to transfer data consistently with the technical requirements, at the same time he acknowledges that failing to fulfill these requirements may result in stating the infringement of the provisions by the users of the devices made available by the Operator, and as a consequence regression of fees for the above infringement.

3.2 Location data transferred

Record of the location data consists of parameters contains in the table (Table 1).

Table 1 List of parameters included in the location – detailed information on permitted values of parameters are located in Table 2

Parameter	Description	Status of the parameter
dataID	ID of the record of the location data (unique for the device)	Obligatory
serialNumber	Technical ID of the device	Obligatory
latitude	Latitude	Obligatory
longitude	Longitude	Obligatory
altitude	Height above seat level	optional (note 1)
fixTimeEpoch	Time stamp of collecting locating data (absolute time UTC)	Obligatory
gpsSpeed	Speed	Obligatory
accuracy	Error in transferring location data	optional (note 1)
gpsHeading	Azymuth	Obligatory

eventType	Class of the event, (one of the values below): ○ location, ○ turnon – usually connected with pressing a button; if there is no such a button, frequently, supply of power is turning on; sometimes a device is always turned on, the nit is recommended to generate the event „*startjourney*" after changing the position of the vehicle after a longer immobility, ○ turnoff – analogically to the turnon, ○ startjourney – detecting a change of the position after immobility, most often it is half an hour, ○ endjourney – reaching a target point, it may also mean turnoff of the start, ○ plugout, ○ plugon, ○ GSM online (gsmonline) –GSM range larger than 0, ○ GSM offline (gsmoffline) – GSM tange equal to 0, ○ GNSS online (gpsonline) – number of visible satellites at least 3, ○ GNSS offline (gpsoffline) – number of visible satellites below 3, ○ jamming, ○ spoofing – the event meaning an attempt to impersonate and sending untrue data; due to the fact that not every device is able to detect such break-in	optional (note 2)
Lac	lac - Location Area Code (ID of the area in which the Cell id is unique)	optional (note 1)
Mcc	mcc – Mobile Country Code	optional (note 1)
mnc	mnc – Mobile Network Code	optional (note 1)
mobileCellId	cid – ID of the area of the GSM mobile (Cell id)	optional (note 1)
satellitesForFix	Number of satellites used for establishing a position	obligatory
satellitesInView	Number of visible satellites	optional (note 1)

Note 1: in accordance with point 3.4 the field is not obligatory, however it should be contained in the data record if possible.
Note 2: parameter is not required if it has another value than **location, which is obligatory to be provided within a class of events** or the **spoofing** value which is optional, but recommended to be placed in the record.

Exact specification of the fields was presented in chapter 3.4.
Charging the amount for the passage with the paid section is generated exclusively on the basis of the trace of single locations collected from the interface (events of „**location** type). The data must possess time stamp UTC corresponding to the moment of collecting coordinates of location. The location data should be transferred immediately after its collection. In case of a failure, which results in a break in sending geo-location data, it is necessary to send it after removing the failure. It requires a prior sending the information on such an event to the box operatorzyOBUZSL@mf.gov.pl.
Location data provided to SPOE KAS by the ELS/OBU Operator within **more than 10 days after their collection WILL NOT BE ACCEPTED** for the calculation of tolls for travel on toll road sections. Operator ZSL/OBU, w miejsce odpowiedzi: „LogsKibanaMessage.getMapperWarnLog("wrong fixTimeEpoch before 10 days", zsl, uuid)" na przesłanie danych przesłanych w czasie powyżej 10 dni, otrzyma zmieniony komunikat: „the data will not be used for billing users".

3.3 Frequency of data sending

The ELS Operator, OBU Operator **MUST** transfer data to SPOE KAS with a frequency of **1 package of data per one minute (60 seconds)**. The data package contains location data and events generated on the OBE level (such as turnon, driving start, stop, turnoff, etc. in accordance with point 3.2). The location data **MUST** be collected with a frequency of **1 location per 5 seconds.** The operator in one package may send data from many devices.
Frequency of collecting and data transferring is a condition necessary and is not subject to change.

3.4 JSON Structure

The data will be transferred in the form of the JSON table, in which particular elements are the JSON objects containing single points of route record. A description of particular fields, rules of validation and information of required fields in Schema_SPOE_v_1_0 is presented by Table 2.

Table 2. Schema_SPOE_v_1_0

Name	Description	Rule of validation	Required
dataId	Unique and incremental (on the OBE level) ID of the record in the source system, variable used for the purposes of the review in the period of tests and suitable for sorting – completing data when the parcels are not sent in a sequence.	"type": "string", minLength": 1,"maxLength": 32, "examples": ["1", "1960472"]	Yes
serialNumber	Unique ID of the localizer, permitted maximum length 50 marks small and capital Latin letters are allowed from the ranges (a-z) and (A-Z), digits (0-9) and marks like hyphen-minus (-) and emphasizing underscore) (_), which constitute a set of ASCII (American Standard Code for	"type": "string", "minLength": 1, "maxLength": 50, "pattern": "^[a-zA-Z0-9\-_]{1,50}$", "examples": ["00000000000B1", "35A058060495422C7934"]	Yes

Name	Description	Rule of validation	Required
	Information Interchange). Size of letters is not differentiated.		
latitude	Latitude collected from the GNSS transmitter, reference system WGS 84, recommended minimum number of places after coma: 6, permitted maximum number of places after coma: 10.	"type": "number","minimum": -90.0, "maximum": 90.0, "multipleOf": 0.0000000001, "examples": [52.0375868826, 52.172644]	Yes
longitude	Longitude collected from GNSS transmitter, reference system WGS 84, recommended minimum number of places after com: 6, permitted maximum number after coma: 10.	type": "number","minimum": -180.0, "maximum": 180.0, "multipleOf": 0.0000000001, "examples": [21.1956136, 20.026094]	Yes
altitude	Elipsoid height collected from the GNSS transmitter, unit [m], permitted maximum number after coma: 2.	"type": ["number", "null"], "minimum": -1000.0, "maximum": 4000.0, "multipleOf": 0.01, "examples": [10.0, 200.02]	No
fixTimeEpoch	Time stamp containing date and time from the GNSS transmitter, associated with the geographic position from a given record, time zone UTC, time stamp SPOE KAS possesses a format approximate to Epoch / Unix Timestamp, but provided to the exactness to micro-second (16 digits), this is therefore a number of which lapsed from '00:00:00 Coordinated Universal Time (UTC), Thursday, 1 January 1970', minimum value shows for 2017.09.20 00:00:00 UTC, total number.	type": "integer", "minimum": 1505865600000000, "examples": [1506086623000000, 1511273867317000]	Yes
gpsSpeed	Speed of moving collected from the GNSS transmitter - unit [m/s], permitted maximum number after coma: 2.	"type": "number", "minimum": 0.0, "maximum": 56.0, "multipleOf": 0.01, "examples": [3.21, 20.0]	Yes
accuracy	Exactness of location collected from the GNSS transmitter – radius of the circle in meters, permitted maximum number after coma: 2.	"type": "number", "minimum": 0.0, "multipleOf": 0.01, "examples": [10.14, 30.0]	No
gpsHeading	Azymuth - unit [degree], permitted maximum number after coma: 2.	"type": "number", "minimum": 0.0, "maximum": 360.0,	Yes

Name	Description	Rule of validation	Required
		"multipleOf": 0.01, "examples": [40.14, 230.0]	
eventType	Type of the event	„type”: „string” „enum”: ['turnon', 'turnoff', 'startjourney', 'endjourney', 'plugout', 'plugon', 'gsmonline', 'gsmoffline', 'gpsonline', 'gpsoffline', 'jamming', 'spoofing', 'location']	Yes
lac	ID of the area of the GNSS base station	„type”: „string” „pattern”: "^[A-Fa-f0-9]{4}$"	No
mcc	ID of the country of the GSM operator	„type”: „string” „pattern”: "^[0-9]{3}$"	No
mnc	ID of the network of the GSM operator	„type”: „string” „pattern”: "^[0-9]{2,3}$"	No
mobileCellId	ID of the mobile phone of the GNSS network	„type”: „string” „pattern”: "^[A-Fa-f0-9]{ 9}$"	No
satellitesForFix	Number of satellites used for establishing the position	„type”: „integer „maximum”: 90 „minimum”: 0	Yes
satellitesInView	Number of the satellites visible during establishing position	„type”: „integer” „maximum”: 90 „minimum”: 0	No

Location data must be sent from the onboard devices using EGNOS (European Geostationary Navigation Overlay Service). The system significantly reduces exactness and reliability of the position obtained from GPS, which has a particular meaning for SPOE KAS.
In addition the data is rejected, the coordinates of which are outside Poland. The rules were presented in **Table 3**.

Table 3. Rule of rejecting data from outside Poland

Rule code	Rule	Notes
B-W06	If lon < 14.116667	Rejection of data when the longitude is smaller than 14.116667. It refers to the western border.
B-S06	If years <49.0	Rejection of data when the longitude is smaller than 49.0. It refers to the southern border.
B-E06	If lon>24.15	Rejection of data when the longitude is smaller than 24.15 It refers to the eastern border
B-N06	If years > 54.835778	Rejection of data when the longitude is smaller than 54.835778. It refers to the Northern border.
L-SSW-CZ	If geographic coordinates fulfill the condition: 54.9 - years - 0.3 * lon > 0	Rejection of data in the Southern-West. It refers to the border with Czech Republic.
L-ESE-UA	If geographic coordinates fulfill the condition: 1.25 * lon + 20.375 - years > 0	Rejection data in the Southern-. It refers to the border with Ukraine.
S-NE-RU	If geographic coordinates fulfill the condition:	Rejection of data in the Northern-East. It refers to the border with the Russian Federation.

	lon > 19 AND years > 54.5	

3.5 Method of data transferring

The data for the data interface SPOE KAS will be sent with the use of the REST mechanism with the use of the HTTPS and the HTTP POST methods. The data sent should be returned in the JSON structure consistent with the JSON diagram described in the document. Each sample of data collected during a single measurement, which contains location data collected at the same time (date and time of gaining coordinates – time stamp containing date and time) is transferred as a single JSON object. In order to limit the number of the transferred package of data, data from one single vehicle or from different vehicles recorded within the JSON object is sent as the elements of the JSON table, which makes up a single package of data. A single JSON table may contain from one to 10.000 JSON objects.

Maximum permitted size of a single package expressed in bites amounts to 5 MB (in words: five megabites). Whereas, after obtaining the package, the size of which exceeds 2 MB, the warning is sent to the ELS/OBU Operator (placed in the confirmation of the obtained data package). The warning informs the Operator that he should prepare for the optimisation of the mechanism of the sending of the location data to SPOE KAS in order to avoid exceeding the maximum size of the amount of the single package if the number of the location data sent grows.

3.6 Security of the data sent

Sending the data to the starting interface (first stage of stream processing) SPOE KAS will be realized only with the use of the certificates. A set of security means covers:

- dedicated URL interface,
- limitation in the access for the indicated IP,
- TLS 1.2 and TLS 1.3 (feedback is realized with the use of TLS 1.2),
- authorisation with the use of the client's certificate.

3.7 Data validation – obligations on the side of the ELS Operator and OBU Operator

The Operator shall be obliged to validate the data package with the use of the currently applicable JSON package before starting it being transferred to the data interface SPOE KAS. The validation should be conducted with the use of the software servicing the validation based on the diagrams consistent with the specification version of JSON Schema provided in the JSON Diagram of the data interface SPOE KAS. A currently applicable diagram JSON of the data interface SPOE KAS is consistent with the specification Schema JSON Draft-06 (http://json-schema.org/draft-06/schema#).

In addition, the Operator must review independently the rules from the Table Table 3 and reject the data not fulfilling the criteria contained in the Table Table 3. As a result, the Operator should separate necessary data and sent to the SPOE KAS system **only** data from Poland.

The repeated sending location data by the Operator is not allowed in the event when earlier the reception of the data was not confirmed from SPOE KAS. The exception to the rule are the failures reported by the Operator to the address operatorzyOBUZSL@mf.gov.pl.

Location data should be sent to SPOE KAS in the sequence of their generation. Repeated sending data is connected with a possibility to charge the amount for passing.

3.8 List of messages for the ELS Operator and the OBU Operator

As far as data validation is concerned, the basic principle is that any package which was not accepted should be sent again, unless it is contrary to JSON Schema, and then it should be corrected (if possible) and sent again (irreparable packages should be omitted).

Table 4 contains most frequent messages in the validation process of data. The full list of possible messages exchanged between systems is in accordance with the IETF standard "RFC 9110: HTTP Semantics" (https://www.rfc-editor.org/rfc/rfc9110.html).

Table 4. List of most frequent messages

Message	Rule/ Warning	Operator's activity
HTTP 200 JSON: {"result": "OK"}	Confirmation of correct validation of the JSON package sent	Not required.
400 Bad Request	Delivered package of data is inconsistent with the applicable JSON scheme or does not fulfill any other requirements	The whole package is rejected, the Operator must eliminate the frames of data not fulfilling the JSON diagram and send the package again
	Package is sent as a single JSON subject	The subject should be sent as a list
	If any single package is rejected,	It should be sent after adjusting an error or omitted.
401 Unauthorized	Data was not delivered due to authorisation error	Operator must check what happened
	No certificate for authorisation was found	One should attach the certificate
	Wrong private error used for the review of the certificate	One should attach the proper key to generate the demand to generate the certificate
	Wrong protocol used for communication (http instead https)	One should use the proper transmission protocol
404 Błędny adres	Resources unavailable	One should review the target address of the input address
408 Request Timeout	End of request timeout – the client has not sent the request to the server within the set time limit.	The stability of the internet connection must be verified and the server's waiting time must be checked.
415 Unsupported media type	Frame validation error	One should correct the structure of the frame of the incoming data
500 Internal Server Error -		One should repeat the attempt all the way. The SPOE KAS team must be informed about such a case.
503 Service Unavailable —	The service is unavailable	Operator should repeat the attempt to provide the data until the effect is achieved. The SPOE KAS team should be notified in such a situation
504 Gateway Timeout	Time exceeded, the server acting as gateway did not receive a response from the designated server within the set time limit.	The operator should try to deliver the data until it succeeds. It is also advisable to verify response times.

NOTE:
"result": "OK" informs that the data is correct in the syntax terms (fulfill the scheme).
Each warning is an independent result of the business rule. The field „action" defines which effect has a given rule on a given warning. The rules with the „drop" action have the higher priority than those

with the „pass” action. Obtaining the feedback „result”: „OK” is equal to the effective sending data to SPOE KAS.

Data rejection occurs in the case of:

1) unregistered devices (the lack of the ascribed business ID),
2) data from outside Poland.

In case of failing to fulfill one of the said rules, the data should be treated as not fulfilling the processing requirements. This is equal to the lack of transferring the geo-location data to SPOE KAS.

3.9 Information necessary to connect the ELS Operator or the OBU Operator to SPOKE KAS

The connection of the ELS Operator or the OBU Operator to SPOE KAS uses certificates and is based on the form of the dedicated portal SPOE KAS.

Summary of some technical details which should be transferred to the ELS Operator or the OBU Operator:

A. data interfaces SPOE KAS accept the geo-location data delivered by the REST-JSON mechanism based on the HTTPS protocol with the HTTP POST method;
B. the data delivered must be equipped with the structures of the JSON data, which is compatible with the current JSON – SPOE KAS diagram. SPOE KAS data interface checks the correctness of the data delivered towards obligatory JSON scheme and rejects all inconsistent data;
C. JSON Schema allows to provide the data in the data package each package mat contain up to 10.000 (in words ten thousand) of the geo-location data for different geo-location devices or for the same geo-location device.

3.10 Feedback between SPOE KAS and the ELS Operators and OBU Operators

In feedback two basic channels are differentiated: channel with the ELS Operator or the OBU Operator and the channel with the end user. In case when OBE is equipped with the displayer, the messages are transferred to the Operator, by the provided ID, reroutes the messages to the proper device. When OBE does not have a displayer, it is possible to affiliate OBE with mobile application SPOE KAS receiving the messages and displaying them to the user, especially in case of the ELS devices. This affiliation is realized on the side of the backend of the mobile application. In this case the messages are transferred to the mobile application. -

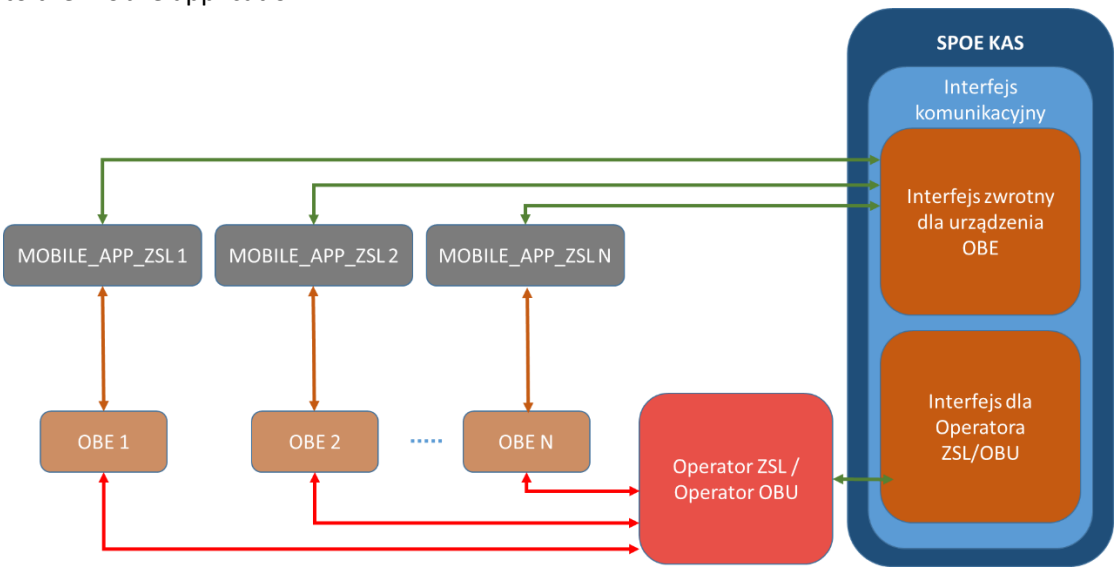

Fig. 2a Feedback– OBE without displayer

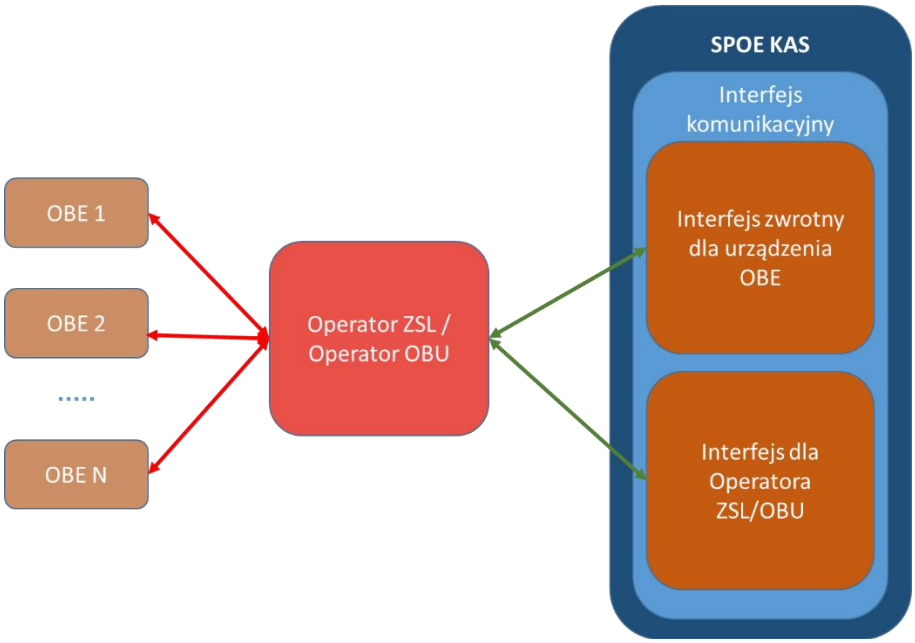

Fig. 2b Feedback– OBE with displayer

In SPOE KAS the implementation of the non-visual channel was foreseen allowing for collection of feedback. As the protocol of transmission, in this purpose the asynchronic interface is used based on the HTTPS protocol, which uses certification with the use of the OAuth 2.0.standard. The messages are sent to the defined IP address, which on the side of the ELS Operator / OBU Operator is dedicated for this purpose.

3.10.1 Feedback for OBE – structure of messages on warning

Each time after obtaining a frame with data, the data is validated. In the event when a given location data passes correctly the validation, the general message is returned of the class 200. In the event when the selected record generates the code of error, additionally the information on error is returned each time for each wrong record. The error may cause rejection of a data („action": „drop"), or the warning which allows for processing of a given data („action": „pass"). The feedback aims at transferring the information on the balance and messages of warnings detected during the stream processing of the system. The message on detected warning possesses a structure presented below (format YAML OpenAPI 3.0).

```
WarningResponse:
    type: object
    additionalProperties: true
    required:
    - subcode
    - message
    properties:
      subcode:
        type: string
        format: string20
      message:
        type: string
        format: string4096
      objectExample:
        type: object
```

```
required:
- eventType
- fixTimeEpoch
- gpsHeading
- gpsSpeed
- latitude
- longitude
- mcc
- mnc
- satellitesForFix
- serialNumber
- dataId
- altitude
properties:
  eventType:
    type: string
    format: enumEventType
    enum: [
      location,
      turnon,
      turnoff,
      startjourney,
      endjourney,
      plugout,
      plugon,
      gsmonline,
      gsmoffline,
      gpsonline,
      gpsoffline,
      jamming,
      soofing
    ]
    description: type of event
  fixTimeEpoch:
    type: integer
    format: int64
    example: [1506086623000000, 1511273867317000]
    description: time stamp of collecting a location data in the form of Epoch
    minimum: 1500000000
  gpsHeading:
    type: number
    format: numberP5S2
    minimum: 0
    maximum: 360
    description: astronomic azymuth
  gpsSpeed:
    type: number
    format: numberP5S2
    minimum: 0
    maximum: 56
    description: velocity
  latitude:
```

```
  type: number
  format: numberP13S10
  description: latitude
  example: 58.0123456789
longitude:
  type: number
  format: numberP13S10
  description: longitude
  example: 21.0123456789
lac:
  type: string
  format: string20
  description: ID of GSM base station
mcc:
  type: string
  format: string3
  pattern: "^[0-9]{3}$"
  description: ID of the country of GSM operator
mnc:
  type: string
  format: string3
  pattern: "^[0-9]{2,3}$"
  description: ID of the GSM operator
 mobileCellId:
  type: string
  format: string11
  pattern: "^[A-Fa-f0-9]{9}$"
  description: ID of mobile network GSM
satellitesForFix:
  type: integer
  format: int64
  description: number of satellites used to establish the position
satellitesInView:
  type: integer
  format: int64
  description: number of visible satellites dring establishing position
serialNumber:
  type: string
  format: string50
  maxLength: 50
  description: OBE unique ID within NKSPO
dataId:
  type: string
  format: string50
  maxLength: 50
  description: ID of a single location unique on the OBE level
accuracy:
  type: number
  format: numberP13S8
  minimum: 0
  example: [10.14, 30.0]
  description: exactness of the measuremnt calculated on the level of the device
```

altitude:
type: number
format: numberP13S8
minimum: -1000
maximum: 4000
example: [10.0, 200.0]
description: exactness of the measurement calculated on the level of the device

3.10.2 Return message to OBE – structure of the information on the balance

An OBE device which does not have the possibility to display the messages, may be connected with the mobile application SPOE KAS allowing for the collection and displaying the messages directed to the device. The messages refer to the current balance, information on the passed section paid or the status of the device registration. The affiliation is realized on the level of the services connected with the service module of the client, where by means of the Internet portal the user logging on onto this account makes an affiliation of OBE with the mobile application SPOE KAS, which has a unique business ID. In the event when the device transmitting is equipped with the displayer, by the proper specification, the message containing the message for the proper OBE is sent to the ELS Operator or the OBU Operator, from where the message is transferred to the target device. The contents of the feedback is described by the following diagram:

```
{
        "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 Feedback to OBE – specification and configuration OAuth2.0

In order to make the feedback flowing, on the side of the Operator there is a need to configurate the security for the communication consistent with the standards OAuth2.0. A diagram of the sequence for the communication was presented below:

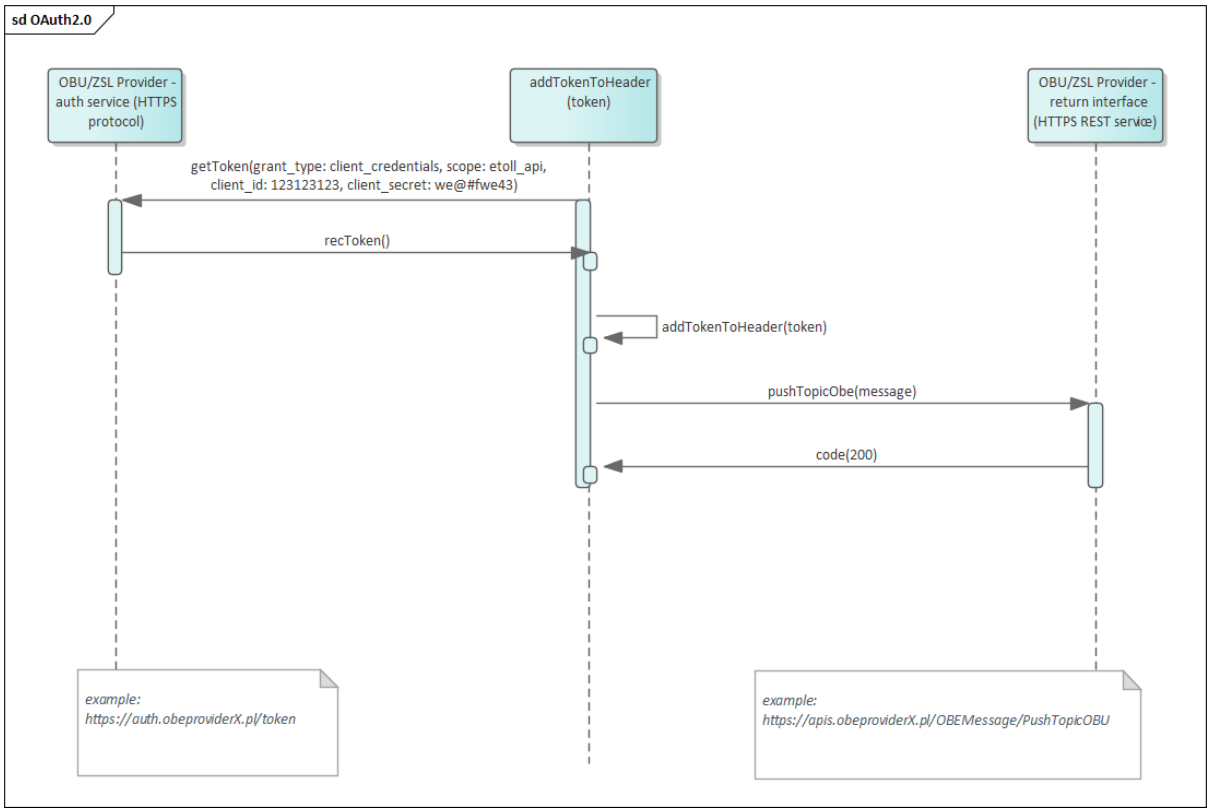

Fig. 3 Diagram of sequence of exchange of message with the use of the standard OAuth 2.0

On the stage of the service registration, the Operator declares whether he will use the feedback communication and completes the necessary data as it was described in the point 2.1. In order to list the communication for the feedback communication, one should provide URL addresses for:

- target endpoint for the feedback
- endpoint for the generated token

The values for the parameters for the service generating token:

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

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

Attributes which should be returned in the json structure:

- - access_token (in standard JWT (header and in payload the attribute 'exp' is required in the format Epoch in the future for the example 1634639693))
- - expires_in (best constant namely 3600 which corresponds 1h)
- - token_type (best constant Bearer)
- - scope (any)

Example (json):
response.json : {'access_token':' eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJPbmxpbmUgSldUIEJ1aWxkZXIiLCJpYXQiOjE2MzgxOTAwMDEsImV4cCI6MTY2OTcyNjAwMSwiYXVkIjoid3d3LmV4YW1wbGUuY29tIiwic3ViIjoianJvY2tldEBleGFtcGxlLmNvbSJ9.w36F0KPrHoM76_MaQLAPzkDiHb_FyxZ9dvGz09h6F3Y', 'expires_in':3600, 'token_type':'Bearer', 'scope':'etoll_api'}

{"access_token":"xxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxxtokentokenxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxtokenxxxxxxxxxxxxxxxxxxxxxxxxtokenxxxxxxxxxxtokenxxxxxxxxxxxx","expires_in":86400,"token_type":"Bearer","scope":"etoll_api"}

Exemplary correct token :
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJPbmxpbmUgSldUIEJ1aWxkZXIiLCJpYXQiOjE2MzgxOTAwMDEsImV4cCI6MTY2OTcyNjAwMSwiYXVkIjoid3d3LmV4YW1wbGUuY29tIiwic3ViIjoianJvY2tldEBleGFtcGxlLmNvbSJ9.w36F0KPrHoM76_MaQLAPzkDiHb_FyxZ9dvGz09h6F3Y

Its decoded structure is as follows:

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

Data sent from the system to the Operator fulfill the diagram contained in the definitione of the interface below.

```
--- YAML FILE BEGIN ---
openapi: 3.0.1
info:
  version: '3.0'
  title: 'PushTopicOBU'
  description: 'Interfejs PushTopicObu is used for sending the information on the status of the billing balance account affiliated with a given OBE and a type of the applicable agreement (pre-paid or post-paid) in order to transfer it to the OBE device. The information is selected after each charging the amount for each time passing the paid road. With the information on the balance status, the marker is transferred  whether the balance is below minimum threshold and should be charged soon. The fact of low or zero balance should be presented on the OBE device with the proper message and sound signal. Initiating module: MPDS (communication module), receiving module: endpoint operator of OBU.'
paths:

  /PushTopicOBU:
    post:
      tags:
      - PushTopicObu
      summary: Passing the message to the OBE device operating within a proper system
      description: Message is prepared in text form. Within the message there is a piece of information on passing a paid section and charging the amount as well as in case of the pre-paid agreement the information on current balance of the account
      operationId: PushTopicOBU

      requestBody:
        description: message is transferred in the form of a complete subject
        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: message is transferred in the form of a complete subject
        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: attribute defining weight/significance of the message
      serialNumber:
        type: string
        format: string50
        description: ID OBE unique, within the system, in transmits
        example: '000410001858840'
        maxLength: 50
      systemBusinessId:
        type: string
        format: string10
        description: business of the OBU/ELS service to which the business ID of the device is ascribed
        example: 'ELS-AZEA-7'
        maxLength: 10
      message:
        type: string
        format: string50
        maxLength: 50
```

```
      description: text of the message for the device containing the information on the event for
charging the amount and the balance for the pre-paid agreements
      billingAccountId:
        type: integer
        format: int64
        example: 1
        multipleOf: 1
        description: ID of the billing account
      billingAccountBalance:
        type: string
        format: money
        description: cash amount of the balance after charging the amount
        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 Certificate management

In order to obtain a certificate for the domain used by the OBU Operator or the ELS Operator for sending location data to SPOE KAS within the e-TOLL service, authorized representative of the Operator should use the account in the service https://puesc.gov.pl/. After logging and displaying the main window of the portal, a representative of the Operator selects in the menu Formularze → Formularze SPOE KAS.
Then, in the folder Registration of services for the ELS or OBU Operator and the GPS device within the services selects the form: REGISTRATION OF THE EXTERNAL SERVICES OF THE LOCATION SYSTEMS (ELS) OF THE OPERATOR.

The user fills in the fields of the form. In the field **Demand to sign and issue the certificate for the domain indicated by the ELS or OBU Operator** pastes CSR (Certificate Signing Request). CSR is generated on the basis of a separate private key. openssl (www.openssl.org) may be used for that. If the user has already a private key (e.g. file private.key), in the Linux environment the order has the following construction:

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

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

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

(length 4096 bites gives a better level of security than the key 2048)

The example of the file containing a private key is presented by the 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+fV4uFHzGqPpMKMXZHUK1pLTVWNvswe0SBfZ5U5
-----END RSA PRIVATE KEY-----
```

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

In turn, the example of the file containing CSR is presented by Fig. 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 the file containing CSR

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

In the form **there must be a possibility to provide the e-mail address**, to which the user will obtain a form with the reply.

In the form with the reply the ELS Operator, OBU Operator obtains the client certificate encoded in the base64 form.
It should be decoded. **The line BEGIN/END CERTIFICATE should not be added**, only the tool which can decode the encoded text should be used in Base64, e.g.:

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

Example of the certificate in base64 is presented by Fig. 6.

Fig. 6. Certificate encoded in Base64

Whereas, the example of the certificate decoded in the format PEM (Privacy-Enhaced Mail) was showed in the Fig. 7.

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

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

Fig. 7. Example of the decoded of the certificate

After decoding, the file is obtained containing maximum three certificates in the PEM format:

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

Each certificate starts with and ends with lines:
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
The above lines shall mean the beginning and the end of the particular certificates.

The scope and method of using data which is used to secure the TLS communication is different and depends on the system/application used by the entity. Nonetheless, the typical requirements of the tools / components SSL/TLS cover the usage of the following elements during SSL certification:

- client certificate;
- private key – which secures a possibility to use the client certiifcate exclusively by the entity being its deponent;
- ang. certificate chain which certifies the client certificate as the certificate issued by the proper CA and contains:
  - CA certificate (Authorisation center) level 1 which issued the client certificate,
  - CA certificate (Authorisation center) level 0, which isued the CA certificate of level 1.

In the Linux environment, the connection with SPOE KAS one may test with the use of the curl tool. A sequence of the commands was presented below. Certyfikat.pem shall mean the certificate obtained which was decoded from the format base64 to format PEM. Whereas, fd1.key shall mean the private key (decoded) used for generating CSR.

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

Note 1: Address https://cloud.spoe-dev.il-pib.pl:8443/ELS/ssl/10000000-0001-1001-0001-0000000000001 should be replaced with the address obtained from the form obtained by email, it is about the contents of the field **Address URL of the service SPOE KAS dedicated to the communication with the service of the ELS Operator or the OBU Operator**.

Note 2: Certificate X.509 of the client SSL/TLS on the side of the ELS Operator or the OBU Operator

The obligations of the ELS Operator or the OBU Operator include:

1. obtaining the above certificate:
   a. first – as a result of the service registration,
   b. each next before the lapse of 365 days from the issue of the previous certificate;
2. using the valid X.509 certificate of the client SSL/TLS to certify the communication with the data interface SPOE KAS.

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

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

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

1. document XML;

2. update form of the data of the service filling in on the site the e-TOLL service in the dedicated portal.

Certificate X.509 of the client SSL/TLS used for certifying the ELS Operator or the OBU Operator during the communication with the data interface SPOE KAS is the first of the certificate returned by SPOE KAS in response to sending the form/document XML. Each certificate returned starts from the line „-----BEGIN CERTIFICATE-----" and ends with the line „-----END CERTIFICATE-----".

The validity date of the certificate X.509 of the client SSL/TLS may be viewed by means of OpenSSL tool package free of charge with the use of the following order:

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

where:

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

Below the exemplary response was provided to the above order:

notAfter=Sep 30 08:30:58 2020 GMT

where:

- notAfter – label of the field „no later" from the X.509 certificate, which contains the final validity date of the certificate after which it should not be used nor trusted;
- Sep – three letter abbreviation of the name of the month, in this case the abbreviation from September ;
- 30 – day;
- 08:30:58 – time, minute and second;
- 2020 – year;
- GMT – three letter abbreviation of the name o the time zone, marking the time zone, in this case this is abbreviation from Greenwich Mean Time, meaning that in order to obtain time for the time zone Europe/Warsaw to the provided hour one should add 2 hours in case of summer time and one hour in winter time.

Note 3: Configuration „mutual TLS"
In case of configuration mutual TLS the attention should be paid that the change of the certificate of the serer will prevent from proper authentification of the communication. The information on changing the certificate of the server will be propagated to Operators, whereas in case of any problems with the review of the server certificate one may use the orders allowing for review of the certificate, i.e..:

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

4 General requirements for the System of the Operator and OBU/ELS devices

Transfer of GNSS Data by the Operator to SPOE KAS must assure:

- Sending location data to SPOE KAS in accordance with the specification described in the document;
- Queuing (of events, location data);
- Remote update of the OBU/ELS software;
- Autodiagnostics.

System of the Operator, upon the demand of the SPOE KAS administrator must allow for the administrator of the Operator parametrization of at least the following parameters:

- frequency of collecting location data **basic starting setting is 5 seconds**;
- frequency of sending location data **basic starting setting is 1 minute (60 seconds)**;
- recommended size of the data buffer minimum 250MB (this requirement is not obligatory);

  The size of the data buffer must allow for storing geo-location data containing attributes indicated in the chapter 3.10.1 collected with the above indicated frequency and stored on the side of the localizer not shorter than 10 days (unless it was sent earlier SPOE KAS) and the events indicated in chapter 3.4 JSON STRUCTURE

- frequency of the data retransmission in case of problems with communication in the range from 30 sec to 60 sec; **basic starting setting is 60 seconds**;

OBU/ELS must fulfil the following requirements in the scope of GNSS:

- possesses sensitive GNSS receiver with antennae;
- exactness of the location readout must assure that the coordinates read out will be placed in the distance not larger than 4 meters from the edge of the lane on which the vehicle is driving;
- services the networks: GPS, GLONASS, Galileo;
- services the system EGNOS;
- GNSS receiver supports A-GPS to shorten the time from the first collecting location;
- GNSS antennae and its connection with the GNSS receiver is covered against the interruptions (screening);
- GNSS receiver should refresh the position with the frequency of at least once per second;
- GNSS receiver supports the advanced detection of drowning out and distorting;
- All sensors calibrate automatically.

Optionally: Updating the software of the GNSS receiver is possible on a remote basis through mobile network;

OBU/ELS: must fulfill the following requirements in the scope of the communication with the network:

- possesses the module of communication with the mobile network with the antennae;

- assures remote access and a possibility of two-direction data exchange with the central system by means of mobile network;

Optionally: OBU/ELS may possess a possibility to receive the feedback from SPOE KAS in the form of text messages and may allow for their displaying. As an example, this can be the information on the account balance, signaling the passage through the virtual gate, warning on the low account balance.

OBU/ELS must fulfill the following requirements in the scope of safety:

- OBE possesses the security unit such as „Secure Access Module (SAM)" responsible for performing encoding algorithms and storing sensitive data such as keys, PIN and others;
- Securing unit supports algorithms of the cryptography such as encoding/decoding, generation of chance number, storing keys;
- Securing unit permanently stores sensitive data in the non-transitory memory;
- Communication between the securing unit and OBU components (such as processor, modules, memory and others) uses certification and encoding;
- Software is not significantly slowed down by safe communication of the securing unit with external components;
- Securing unit stores safely unique ID and assures access to software;
- Securing unit is immune to active and passive attacks;
- Securing unit is immune to mechanic modifications. The opening of the OBU housing or the securing unit is impossible without leaving traces;
- Each attempt of attack is detected, documented and controlled.

Short deficiency of voltage have no influence on OBU/ELS:

- In case of disconnecting OBU from the supply, the device stores data from the non-transitory memory and turns off properly;
- OBU possesses in-built accumulator allowing for a few-hour work in case of no supply voltage.

With the devices, the system must be supplied allowing for managing the OBU devices. The System in particular must allow for:

- Remote software update;
- Remote setting the work parameters of OBU;
- Monitoring OBU status.

Failing to fulfill technical requirements for the device may result in deactivation of the device.

5 Legal and normative requirements

The chapter contains legal and normative requirements concerning fee collection.

Document	Version	Contents
Decision 2004/52/EC1	6 October 2009	Decision of the European Commission on definition of the European service of electronic fee 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 January2003	Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment
Directive 2012/19/EC	4 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 and repealing
Directive 2004/53/EC	16 April 2014	Directive on the harmonisation of the laws of the Member States concerning making available radio devices
Directive 2014/30/EC	26 February 2014	Directive on the harmonization of the laws of the Member States relating to electromagnetic compatibility
Directive 2011/65/EC	8 June 2011	Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment
Directive 2006/66/EC	6 September 2006	Directive on batteries and accumulators and waste batteries and accumulators
Directive 2013/56/EC	20 November 2013	Directive on batteries and waste batteries and accumulators as regards the placing on the market of portable batteries and accumulators containing cadmium intended for use in cordless power tools and of button cells with low mercury content
ISO DIS 12813	28 September 2018	Electronic fee collection – Control of conformity in autonomic systems
ISO 13141	1 June 2017	Electronic fee collection – Communication aiming at improving location in autonomic systems