

## MANUALS OF OPERATION FOR THE Operators of OBU/ZSL in the scope of the SSL certificate update

The validity of the SSL certificate is maintained for 1 year counting from the day of its issue and is one of the conditions for proper functioning of the data information infrastructure communication of the operator with the e-TOLL system. The SSL certificate is network protocol, used for safe Internet connections in the scope of coding on the WWW sites, protecting transactions and securing the information sent by the post and the WWW site such as passwords, logins, personal data, etc. The lack of the SSL certificate updated by the OBU/ZSL operator exposes the users of the e-TOLL system to the lack of possibility to use the functionality of the system, including the one concerning transferring geo-location data to charge the due amount.

(example)

### Step 1

- enter <https://puesc.gov.pl>
- log onto the account in the company context
- choose folder „Forms” in the menu
- unfold „Forms alphabetically” and enter „ZSL105”
- open the link searched for

The screenshot displays the PUESC website's 'Forms' section. At the top, there is a navigation menu with items: MY DESKTOP, SERVICES, NETWORK SERVICES, FORMS, HELP, SINGLE WINDOW, and NEWS. Below the menu, a breadcrumb trail reads 'PUESC > Services > Forms >'. On the left, a sidebar menu lists various categories, with 'FORMS' highlighted. The main content area is titled 'Forms catalog' and includes instructions to search for forms and follow on-screen instructions. A search bar contains the text 'ZSL105' and a 'Q SEARCH' button. Below the search bar, a list of forms is shown, starting with 'S' and 'SENT ZSL105 - Aktualizacja danych rejestracyjnych usługi ZSL/OBU (SENT)'. A green dot indicates the form is 'Available'. The description for this form is 'Formularz do zarządzania zarejestrowanymi usługami ZSL/OBU oraz urządzeniami przez operatorów ZSL/OBU'. Other sections visible include 'Mapping PUESC forms to PUESC2', 'Forms alphabetically', and 'Forms in groups'.

### Step 2

- approve the NIP of the company showed

Back

DATA OF THE SERVICE OPERATOR

IDENTIFICATION TYPE \* ⓘ

NIP

IDENTIFICATION NUMBER \* ⓘ

5970551996

Confirm

3.22.36, Host: 152  
Main portal version: 3.22.36

Step 3  
- choose „List of services”

Edit List of services List of devices Print Back

ZSL101 - INFORMATION ABOUT REGISTERED ZSL/OBU OPERATOR

Service operator type: **ZSL**  
Service operator status: **registered**

**INFORMATION ABOUT THE NOTIFICATION**  
Checksum: 0e32d0ca908ff9b74cab3b14fec9a1e28e4a2203

**INFORMATION ABOUT REGISTRATION OF THE ZSL/OBU SERVICE OPERATOR**  
Creation date: 2020-09-15 godz.18:10:27  
Creator: **Marek Tomczyk**  
Modification date: 2022-09-22 godz.10:28:48  
Modifier: **Marek Tomczyk**

**INFORMATION ABOUT THE THE ZSL/OBU SERVICE OPERATOR**  
idSISC identification number: PL597055199600000  
Full name: **GEO INFO 1.3**  
Identification type: **NIP**  
Identification number: **5970551996**  
**Address information**  
**Świętokrzyska1 12 / 21261**  
**00-916 Warszawa123, PL**

**CONTACT INFORMATION TO THE ADMINISTRATOR OF THE ZSL/OBU SERVICE OPERATOR**  
Phone number: 226663322  
E-mail: **marek.tomczyk.puesc@gmail.pl**

3.22.36, Host: 152  
Main portal version: 3.22.36

Step 4  
- in the column „Akcja” choose icon at the service which you want to update (symbol of the document with the magnifying glass in green)

Add new service List of devices Print Back

ZSL114 - LIST OF REGISTERED ZSL/OBU OPERATOR SERVICES

INFORMATION ABOUT THE NOTIFICATION

Checksum: 3ba6478878cc1d6013ec3cf1a0181a6f85521263

INFORMATION ABOUT THE ZSL/OBU SERVICE OPERATOR

Identification type: NIP
Identification number: 5970551996

LIST OF ZSL/OBU OPERATOR SERVICES

Table with 10 columns: Service number, Service own name, eTOLL, SENT- GEO, Device status, Creation date, Creator, Modification date, Modifier, Akcja. Row 1: ZSL-CSFF-8, Test123455 1, checked, unchecked, registered, 2022-04-28 godz.05:54:34, Marek Tomczyk, 2022-09-22 godz.10:33:40, Marek Tomczyk, icon.

Step 5
- choose button „Edit service”

Edit service Cancel service Add device Delete device List of devices Print Back

ZSL111 - CONFIRMATION REGISTRATION OF THE ZSL/OBU SERVICE

Service number: ZSL-CSFF-8
Service status: registered

SERVICE OWN NAME

Test123455 1

SERVICE TYPE

[checked] eTOLL
[unchecked] SENT- GEO

INFORMATION ABOUT THE NOTIFICATION

Checksum: bb0ca86c255d790b8cf18d820d85b0aa624331f2

INFORMATION ABOUT REGISTRATION OF THE ZSL/OBU SERVICE

Creation date: 2022-04-28 godz.05:54:34
Creator: Marek Tomczyk
Modification date: 2022-09-22 godz.10:33:40
Modifier: Marek Tomczyk

INFORMATION ABOUT THE ZSL/OBU SERVICE OPERATOR

Identification type: NIP
Identification number: 5970551996

URL ADDRESS OF THE ETOLL SERVICE DEDICATED TO COMMUNICATION WITH THE ZSL/OBU SERVICE

https://spoe-dev.il-pib.pl:8443/zsl/ssl/68c9435b-3288-470a-9882-1e2493fd6876

IPv4 ADDRESSES FROM WHICH THE ZSL/OBU SERVICE WILL TRANSFER DATA TO ETOLL / SENT- GEO SERVICE

IP: 222.111.111.222

CLIENT CERTIFICATE ISSUED BY THE ETOLL / SENT- GEO CERTIFICATION CENTER (ENCODED IN BASE64 FORMAT)

LS0tL\$1CRUdJTIBDRVJU\$UzJQ8FUR\$0L\$0hcK1J\$UISVENDQkMyZ0F3\$UJ\$BZ0IDQTNz0RRWUjP\$LpJaH2jTKFRURx\$CUUF3Z2U0eEN6QUpCZ05WQkFZVEf+Qk0KTVJrd0VnWURWUVJREF0dFYcHZkMmxsWtJ0cFURPURTNRHhH
QTfVRUNndzBTvzV6ZehsMGRYUWd4WUhfFadONgpiB\$9GbtJ\$OcEIDMGdVR0hGaEhOMGQyOTNIU0JKYm50MGMVYUjFKQJ\$DWWdSaGQyTjZIVEU4TURvR0EXVUVd3d6CldRnJ4WUpoWkNCYIXRjNZvzV6YJnKaGJubGphQJVVld
Ob2JhHJRRWx1Wm05eWJXRmpjV3B1ZvOb0IDaGekTFRzE1Ta3RkdIEVIFRFRERDQIR\$VTV\$UVKRRIR50kpWRXdnVz0TUIGUmxM1FvVEWmJpXtd2dNU0JEUVRfAaPnQjHq1Nxr1N1JYJNEUJVKVQJZU2MyVnVkr2R2sYJBCcGR
Hd3VMkYzTGSco01CNfHEVEI8TUReU1qQTRNek0wCk1G1bHEVEI8TUReU1qQTRNek0wTuZvd11URUxNQWHQTFVRUJoTUNVRX4dRgpBTUJnTIZCQU1NQIVwaFkyVnlkTVJF0R3WURWUVFIREF0WfYnplbUyZVWVRFTE1Ba0dB
MNVzQ2d3Q1RWXhGREFQmdOVKJBZ0IDMjFczW05MmepH1ZqYTTsB1Rd3dDZIEVIFRFRERBTkVvEzF322dFau1BMEdDU3FHU0iMORRRUJBUUVBQTRJQkR3QXdnZ0VLckFv\$UIJBUURwZkozU2J0NThNC9WUkxpVHR5SmMwVz
JTTWJctnNkH0xVn9acc3B5WnFkNk5sXIIPOEJYNlpyT\$EKZ2VGUUVkxamZJRjkwXJnQ0VNMIBZINNV2N2NkdzMEF0Zk0dVHZXaW9leE1kQ0FLKx1\$UUVX3dkbXhFay95ZAp6E8BV2I2dGH50TVvO5SvC9yaDByYh0ZTRJa3FDTRUY
kN\$K2IKTjHYZCtulZvKWHZINDRhaUISRFJ0VW01CkdNMG5j3hThI5MvkvTmJrMW9qd1VPQWKNjYdXnzhR2d3N5QXVzSh0vEh2SWp\$WJZleW5JKzhxQjVUUEKROFRIR25IOHg1UkVqY1UxkIlnVBBvNobW3K2hmZ013RHn4R
3c23F45G8VUZZaWx1c0GvK1ZURGlvdE92agpFNH0rL2bVHlmZtd3QXFYIMxYzIldGMrWEFjQWdNkQFBR2pnZ0YzTUIJQmN6QUpCZ05W\$FJNRUFQqUNQjBHCkExVWREZ1FXQkJRnZnQMndnSVFZ3m5DZkwrL3BfVZUyIh5bXNU
Q93C205W\$FE4QkFmOEVCQU1DQmVb0d9V3WUqKvllwEjBd3dDZ1J\$3dZQkJRvUhb0j3Z2dFZ0JnTIZU01FZ2dFWE1J\$UJFNEFVTEJyaUNwUzizNTIpb1Y5MqPmECwWENZMUxXbWhnZmFrZ2Zn2d2dmQXhDekFKQmdOVKJBWV
RbEJNTVJRd0VnWURWUVJREF0dFYcHZkMmxsCikydhBaVEV\$TUE4R0EXVUVd3dJdVjJGvWmZcGhkMkV4UFRBN0JnTIZCQW8NTkvsdWmZUjVfSkFwSU1XQnhJvmoKZW01dnhdpGhU0F\$SUZCaHhZUnpkSGRZ2DnZINXNpk
S9wwZfRz21FIRmZWG8RqZw5reFBEQTZC205WQkFzTQpNMXBoYThXQ1XIUWdXbUz0ZDZGdWMyOTNZVzU1WTJnZ1ZHvmpHrZvWYXCSmJtWnZjbF0WtNscWJubGphQ0FvClidpMDJLVEVktUJzR0EXVUVd3dVBTW1ZDQkH5
VtnhUz2STUIG\$Nz2M1FhUTBFeE8EOWF\$CZ2tXaG1pRzIMEIKQ1FFV0RYbzJRR2wwYkM1M1Y1Y3VJR3IDQWbBRE1BMEdDU3FHU0iMORRRUJd1VBQTRJURFRQmZxXhLeDnhWaoxVfDqeGU1R2xQalNoRGITbGNKYXJ1TDh6SzJ4T
FVEVDV1QkZsMndvVo1KE4T0NEK2FKMllS256fNaaXRRPcIiIzE5NTU5E5K08vQ25qa3F5eGUzNdh3R3qUgVkr8q5UtbJksrenBENjErcHJXM3c9vCfUzJuN24KL0Y5VGd0VmUrcEwrV2Y3cJjJNHM0T31sTtSbTn4WW

## Step 6

- in point 4 (A request to sign and issue a certificate for the domain indicated by the ZSL/OBU services operator) of the vision showed (ZSL112 – UPDATE DATA OF A ZSL/OBU OPERATOR SERVICE) paste the new CSR (CERTIFICATE SIGNING REQUEST)
- choose button „Save” on the form ZSL112

MY DESKTOP SERVICES NETWORK SERVICES FORMS HELP SINGLE WINDOW NEWS

My cases and documents To send and drafts My services My Data Entity data e-Documents e-Płatności

PUESC > Services > Excise duties, gambling games, transfers and transport > SENT - Road carriage monitoring > ZSL - 105 >

### ZSL112 - UPDATE DATA OF A ZSL/OBU OPERATOR SERVICE

**Save** **Back**

Service number: ZSL-CSFF-8

#### 1. Service type

ETOLL SERVICE ⓘ

SENT-GEO SERVICE ⓘ

At least one service must be checked

#### 2. Service own name or description

SERVICE OWN NAME OR DESCRIPTION \*

Test123455 1

#### 3. IPv4 addresses from which ZSL/OBU service will transfer data to the eTOLL / SENT-GEO

IP ADDRESS

000.000.000.000 **Add**

1.	222.111.111.222	
----	-----------------	--

#### 4. A request to sign and issue a certificate for the domain indicated by the ZSL/OBU service operator

CSR (CERTIFICATE SIGNING REQUEST) ⓘ

(please paste CSR including -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----)

## Step 7

- obtaining confirmation of the updated service





```

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAua
SvEsSeMUYYdw4fCOWeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB
lmKuux1XP0tCsHXgPJ0ezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMR1D4G3cPBD
dOOZqSmX7tHp97q+PbVbWwvUg6eISxsgQ16SZTbAoilaG8HgIO+5i2RRdZOFj++7
KGFjwEl+UxDgsNaSp7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyf
kW4k8gvltwueKScsc9/Ordlr6YopGg5xwQr+TQIDAQABAoIBAQDePSF9cqTf9X4I
TVqk16cqkQQqSU5sokTQSiDbkRQmK1S/JCrcqQ5VZ6Ldz+1260DCYiia2g1pdcy7a
zCz01ldhtHsWfVBI5HdTLieu2iJO/8Igt2DGOqG8chQbpQ8HQ1WqVIBaF+ha3W64d
VJlH7f4ctfxoGi8S5XH8Jtgg3JoLdeH9YqaNzQ2LKSx91/PxO6J7sLya82KKUBrp
M3AOumtEt0YRy57JkV7j1YeYUFLpWT7cR5rh2cZs5r1fQTGQjQorWBU/e4Po7PMn
Vbp/qDBqni femd/dxDWydtXtJukp1mLdUSK15jAXApr2ZSXZ56espTnuIxxkvuzZ
mny15mItAoGBAP34wh8DZwvUeKiN408osSgzHETMnefIMBOu0yoj94RQZuv8VwAR
eoTeFIEPOqgqdB7MSgkqZpNuyYxw+OrQI4mMl9Wh9DyHwnWTxNO7pDJEB6BCukQb
/+bdjLSytmDyVhkGMLMQ1E0l7MdncrQRSURvByNRXbDzZoP7w1L2bASTAoGBAPGb
HIDDLxcHZkdOWNof2RDE+Ubgau86aI3dtGSsoTo6bmPkXxFe6PJPu8pLwhzVOafZ
EXH4jQ9C1OE4r6PelyA944KDwx8mlBsU7E6fEchJaR6xykW8u25Nr5P304szxCTI
987eJmQq+BGUUp7LgC/Qlcpir7yyP+h5CnNkAp2fAoGAECsaiCLrzacSvX1+6KXX
Jsowm5ADqBiYTSJegZ88jNq3LyFbUNToNml3D8Rp4DVzikiGoke7jXkms9JWNGphv
NATAA4xkR6Kw0F4Trvc8+tXx+WDNIqk75jmZCnwmn25ykx1ruwJf1A97YFuq+zF
rHT8Edt6a4vTEebGJm62uMcGyA06NMfH9AmqgrFW0/1lmh4oD01JB7WT8sUjD/
Gw7zwXgLScfLanXhGrT1SEIoRAGsUE0RUHK07c0sBU3xhPlzghogqtpAKCKn530
WcF7KxhqMGUrgH1LXpFkv5EEGwIJD14hA3EQeSxdNnjDI216ufiukMbf62fK2JT
aMnp4QKBGdxQkHSX8E7Fh1Uijf3C8IMZsZ7frzCbdIfNX6/PcVrex3UKSVWmB9/v
auOMEHZmoo/FRZXdcZPI0wzcGb4oz4few2Dp2savew5QEGg4v3DZDehGK5X7Yc+m
skL3MCgqGqVN1+fV4uFHzGqPpMKMXZHUKlpLTVWNVswe0SBfZ5U5
-----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-----
MIIC1zCCAb8CAQAwZEXxCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAtNQVpPV01FQ0tJ
RTERMA8GA1UEBwwIV0FSU1pBV0ExDDAKBgNVBAoMAA05JVDELMAkGA1UECwwWjYx
FzAVBgNVBAMMDnd3dy5pdGwud2F3LnBsMSUwIwYJKoZIhvcNAQkBFhZlLmtsaW1h
c2FyYUBpdGwud2F3LnBsMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAuaSvEsSeMUYYdw4fCOWe
HUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB1mKuux1XP0tCsHXg
PJ0ezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMR1D4G3cPBDdOOZqSmX7tHp97q+
PbVbWwvUg6eISxsgQ16SZTbAoilaG8HgIO+5i2RRdZOFj++7KGFjwEl+UxDgsNaS
p7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyfkW4k8gvltwueKScs
c9/Ordlr6YopGg5xwQr+TQIDAQABAAwDQYJKoZIhvcNAQELBQADggEBADj0Du1l
Wqp2GJ/8nam/bjnh2WNSczQ0FjQ6iK/+rh1Bforeky0J9cz+hRsZt5m9D8UVWkC
u4a/iJicrMZHPHtbc9tKuAk2c29ErxKJeSxR/anRKg9EbD7AB4RFmEjsJo/yRauL
oHetcTqxNPDbspkCmo2eRrKb2LdhCGFQRG4Wx/Gg6iuzd7zZKnOVkMuELpOP/vTz
Gu6QUdi2kpg/cr5A1rwq4d5uIEag1vi9G8YXNa/wkqOrNsuP660Wj8u9QgIWPwdV
ikYJShahrHFxk3Qr//3P3lg0vge4AuDes/r4aO1ET7dzuIt0qZymoQKPuOWXpfgY
gxjEmtwLRv5Bgm8=
-----END CERTIFICATE REQUEST-----

```

Fig. 5. Example of the file containing CSR

More details to 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 **e-mail address**, to which the user will receive a form with the reply.

In the form with the reply Operator ZSL, Operator OBU shall obtain the Certificate of the client encoded in the base64 form.

It should be decoded. **One should not add to it the line BEGIN/END CERTIFICATE**, one should only use the tool which can decode the encoded text in Base64, e.g.:







1. client certificate;
2. private key – which secures the possibility to use the client certificate exclusively through the entity being its deponent;
3. chain of certification / chain of certificates (ang. certificate chain), which certifies the client as the certificate issued by the CA and contains:
  1. CA Certificate (Authorisation Center) level 1, which issued the certificate of the client,
  2. CA Certificate (Authorisation Center) level 0, which issued the certificate CA of level 1.

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

```
curl -X POST --cert ./certyfikat.pem --key ./fd1.key -H 'Content-Type: application/json' -H 'cache-control: no-cache' -d '{"dataid": "1960472", "serialNumber": "ALBS8_74718", "latitude": 52.17264488, "lonitude": 21.1956136, "altitude": 140.0, "fixTimeEpoch": 1505893301000000, "gpsSpeed": 0.0, "accuracy": 15.17, "gpsHeading": 0.0}, {"dataid": "1960473", "serialNumber": "ALBS8_74718", "latitude": 52.17264546, "longitude": 21.195608, "altitude": 138.0, "fixTimeEpoch": 1505896249000000, "gpsSpeed": 10.0, "accuracy": 15.17, "gpsHeading": 0.0}]' https://cloud.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-000000000001
```

**Note 1:** Address <https://cloud.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-000000000001> should be replaced with the address obtained from the form by email, namely the contents of the field **Address URL of the e-TOLL dedicated after communication with the service Operator ZSL or Operator OBU**.

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

The obligations of the ZSL Operator or OBU Operators include:

1. obtaining the above certificate:
  - a. first – as a result of the service registration,
  - b. for each next before the lapse of 365 days from the issue of the previous certificate;
2. using the valid certificate X.509 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 the response to sending to SPOE KAS via dedicated portal, the demand to issue the X.509 certificate of the client SSL/TLS by means of one of two available forms of communication:

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

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

1. document XML;
2. form of data updating the service filled on the side of the service e-TOLL in dedicated portal.

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

Validity date of the certificate X.509 of the client SSL/TLS may be seen by means of the package of tools OpenSSL free of charge with the use of the following order:

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

where:

1. plik\_z\_certyfikatem\_klienta\_x509.pem – constitutes an example name of the file containing the certificate X.509 of the client SSL/TLS issued by SPOE KAS.

Below the example answer was given to the above order:

```
notAfter=Sep 30 08:30:58 2020 GMT
```

where:

1. notAfter – label of the field „nie później” from the certificate X.509, which contains the final validity date of the certificate, after which it should not be used nor trusted;
2. Sep – three letter abbreviation of the name of the month, in this case the abbreviation from September, namely September;
3. 30 – day;
4. 08:30:58 – time, minute and second;
5. 2020 – year;
6. GMT – three letter abbreviation of the name of the time zone, marking of the time zone, in this case this is abbreviation from Greenwich Mean Time, marking that in order to obtain the time of the time zone Europe/Warsaw, one should add to the time provided 2 hours in case of summer time and 1 hour in winter time.

### **Note 3: Configuration „mutual TLS”**

In case of configuration of mutual TLS one should pay attention to the fact that the change of the certificate of the server will prevent from correct authentication of the communication. The information on the change of the certificate of the server will be distributed to Operators, whereas in case of Operators, whereas in case of any problems with the review of the certificate one may use the order allowing for the view 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
```