

ИНСТРУКЦИЯ для операторов OBU/ZSL по обновлению SSL-сертификата

Актуальность SSL-сертификата действительна в течение 1 года, считая со дня его выдачи, и является одним из условий правильного функционирования связи ИКТ-инфраструктуры оператора с системой e-TOLL. SSL-сертификат - это сетевой протокол, используемый для безопасных Интернет-соединений с точки зрения шифрования на веб-страницах, защиты транзакций и информации, передаваемой почтой и веб-страницами, такой как пароли, логины, персональные данные и т. д.

Отсутствие SSL-сертификата, обновленного оператором OBU/ZSL, угрожает пользователям системы e-TOLL невозможностью пользования функционалом системы, в том числе в отношении передачи данных геолокации для начисления причитающейся платы.

(пример)

Шаг 1

- перейдите на страницу <https://puesc.gov.pl>
- войдите в учетную запись в поле компании
- выберите в меню вкладку „Forms”
- разверните панель „Forms alphabetically” и введите „ZSL105”
- откройте поисковую ссылку

The screenshot shows 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, NEWS. Below the menu, the breadcrumb path is 'PUESC > Services > Forms >'. On the left, there is a sidebar menu with categories: DUTY, BORDER, STATISTICS; EXCISE DUTIES, GAMBLING GAMES, TRANSFERS AND TRANSPORT; REQUESTS AND GUARANTEE HANDLING; KAS CUSTOMER AREA; FORMS (highlighted); NETWORK SERVICES - INFORMATION AND SPECIFICATIONS. The main content area is titled 'Forms catalog' and includes instructions: 'Search for the interactive form you are interested in in the catalog below. Follow the on-screen instructions when completing the selected form.' Below this, there are two expandable sections: 'Mapping PUESC forms to PUESC2' and 'Forms alphabetically'. The 'Forms alphabetically' section is expanded, showing a search input field with 'ZSL105' and a 'SEARCH' button. Below the search field, there is a horizontal list of letters: A D G I K L O P R S T V W Z. Under the letter 'S', the form 'SENT ZSL105 - Aktualizacja danych rejestracyjnych usługi ZSL/OBU [SENT]' is listed with a green dot and the word 'Available'. Below this, there is a section titled 'Forms in groups'.

Шаг 2

- подтвердите отображаемый NIP компании

Back

DATA OF THE SERVICE OPERATOR

IDENTIFICATION TYPE * ⓘ

NIP

IDENTIFICATION NUMBER * ⓘ

5970551996

Confirm

3.22.36, Host: 152
Main portal version: 3.22.36

Шаг 3
- выберите поле „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

Шаг 4
- в столбце „Акція” выберите значок рядом с услугой, которую вы хотите обновить (символ документа с лупой зеленого цвета)

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.

Шаг 5

- выберите кнопку „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)

LS0tLS1CRUdJTBDRVJUSUJzQ0FUR50L50hcK1J5UISVENDQkMyZ0F3SUJBZ0IDQTNZd0RRWUJpLpJaH2jTKFRURxCUUF3Z2U0eEN6QUpCZ05WQkFZVEF+Qk0KTVJrd0VnWURWUVVJREF0dFVYcHZkMmxsWTJ0cFURTRIRNHh... (base64 encoded text)

Шаг 6

- в п. 4 (A request to sign and issue a certificate for the domain indicated by the ZSL/OBU services operator) отображаемого на экране контента (ZSL112 – UPDATE DATA OF A ZSL/OBU OPERATOR SERVICE) вставьте новый CSR (CERTIFICATE SIGNING REQUEST)

- выберите кнопку „Save” в форме 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 **Add**

000.000.000.000	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-----)

Шаг 7

- получение подтверждения обновления услуги

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
[e] eTOLL
[] SENT-GEO

INFORMATION ABOUT THE NOTIFICATION
Checksum: fc67a652778374529d6618ab663f6349e1048111
Document own number: 234

INFORMATION ABOUT REGISTRATION OF THE ZSL/OBU SERVICE
Creation date: 2022-04-28 godz.05:54:34
Creator: Marek Tomczyk
Modification date: 2022-10-06 godz.11:55:40
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)
LS0tLS1CRUdJTBmZGVzV6ZEsMGRYUWd4WUhfFdONGpibSSGbtJ0cEIDMGdVr0hGaEhOMGQyOTNIUJKYm5OMGVYUJfKQ0JDVWdSaGQyTjZVEU4TURvR0EXVUDd3d6CldRnJ4WUpoWkNcYVIXRjNZVzV6YjNkaGJubGphQ0JjVWld...

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Пользователь заполняет поля формы. В поле A request to sign and issue a certificate for domain indicated by the ZSL/OBU service operator вводит CSR (ang. Certificate Signing Request). CSR генерируется на основе своего закрытого ключа. Для этого можно использовать openssl (www.openssl.org). Если у пользователя уже есть закрытый ключ (например, файл private.key), то в среде Linux команда имеет следующую конструкцию:

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

Если у пользователя нет закрытого ключа, его можно сгенерировать, например:

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

(длина 4096 бит дает лучший уровень безопасности, чем ключ 2048)

Пример файла, содержащего закрытый ключ, показан на Рис. 4.

```

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQE77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAua
SvEsSeMUYYdw4fCOWeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB
lmKuuxlXP0tCsHXgPJ0ezrcbMTiSpM0QU9Fc4KKOpqIV65pjJ4IinMRlD4G3cPBD
dOOZqSmX7tHp97q+PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7
KGFjwEl+UxDgsNaSp7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VT2jyf
kW4k8gvltwueKScsc9/Ordlr6YopGg5xwQr+TQIDAQABAoIBAQDePSF9cqtF9X4I
TVqk16cqqQQqSU5sokTQSiDbkRQmK1S/JCrgQ5VZ6Ldz+I260DCYiia2g1pdcy7a
zCz01ldhtHsWfVBI5HdTleu2iJO/8Igd2GQOgC8chQbpQ8HQ1WqVIBaF+ha3W64d
VJlR7f4ctfxoGi8S5XH8Jtggq3JoLdeH9YgaNzQ2LKSx91/PxO6J7sLya82KKUBrp
M3AOumtEt0YRy57JkV7j1YeYUFLpWT7eR5rh2cZs5r1fQTGQjQorWBU/e4Po7PMn
Vbp/qDBqniFemd/dxDWydtXtJukp1mLdUSK15jAXApr2ZSXZ56espTnuIxxkvuzZ
mny15mItAoGBAP34wh8DZwvUeKiN408osSzcHETMnefIMB0u0yoj94RQZuv8VwAR
eoTeFIEPOqgdB7MSgkgZpNuyYxw+OrQI4mMl9Wh9DyHwnWTxNO7pDJEB6BCukQb
/+bdjLSytmDyVhkGMLMQ1E0l7MdnrcQRSURvByNRXbDzZoP7w1L2bASTAoGBAPGb
HIDDLxchZkdOWNof2RDE+Ubgau86aI3dtGSsoTo6bmPkXxFe6PJPu8pLwzhVOafZ
EXH4jQ9CIE4r6PelyA944KDwx8mlBsU7E6fEchJaR6xykW8u25Nr5P304szxCTI
987eJmQq+BGUUp7LgC/QlcpIR7yyP+h5CNNAp2fAoGAecSaiCLrzacSvX1+6KXX
Jsowm5ADqBiYTSJegZ88jNQ3LyFbUNToNm13D8Rp4DVzikgOke7jXkMs9JWNGphv
NATAA4xkR6Kw0F4Trvc8+tXx+WDNIqk75jmZCnwmm25yxlruwJf1A97YFuq+zF
rHT8Edt6a4vTEebGJjM62uMCGYA06NMfH9AmqgrFW0/1lmh4oD01JB7WT8sUjD/
Gw7zwXqLSCfLanXhGrT1SEIoRAGSUE0RUHK07c0sBU3xhPlzghogqtPACkKnc530
Wef7KxhqMGUrgH1LXpfkv5EEGwIJD14hA3EQeSxdNnjDI216ufiukMbf62fK2JT
aMnp4QKBGdxQkHSX8E7Fh1Uijf3C8IMZsZ7frzCbdfINX6/PcVrcx3UKSVWmB9/v
auOMEHZmoo/FRZXdcZPI0wzcGb4oz4few2Dp2savew5QEGg4v3DZDEhGK5X7Yc+m
skL3MCgqGqVN1+fV4uFHzGqPpMKMXZHUklpLTVWNvswes0SBfZ5U5
-----END RSA PRIVATE KEY-----

```

Рис. 4. Пример файла с закрытым ключом

В свою очередь, пример файла, содержащего CSR, показан на Рис. 5.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC1zCCAB8CAQAwgZExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAtNQVpPV01FQ0tJ
RTERMA8GA1UEBwwIV0FSU1pBV0ExDDAKBgNVBAoMAA05JVDElMAkGA1UECwwWjYx
FzAVBgNVBAMMDnd3dy5pdGwud2F3LnBsMSUwIiwJKoZIhvcNAQkBFhZlLmtsaW1h
c2FyYUBpdGwud2F3LnBsMIIBIjANBgkqhkiG9w0BAQsFAAOCAQ8AMIIBCgKCAQE77
EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAuaSvEsSeMUYYdw4fCOW
eHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB1mKuuxlXP0tCsHXg
PJ0ezrcbMTiSpM0QU9Fc4KKOpqIV65pjJ4IinMRlD4G3cPBDdOOZqSmX7tHp97q+
PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7KGFjwEl+UxDgsNaS
p7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VT2jyfkW4k8gvltwueKScs
c9/Ordlr6YopGg5xwQr+TQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBADj0Du1l
Wqp2GJ/8nam/bjnh2WNSczQ0FjQ6iK/+rh1Bforeky0J9cz+hRsZt5m9D8UVWkC
u4a/iJicrMZHPbTbC9tKuAk2c29ErXKJeSXR/anRKg9EbD7AB4RFmEjsJo/yRauL
oHetcTqxNPDBspkCmo2eRrKb2LdhCGFQRG4Wx/Gg6iuzd7zZKnOVKMuELpOP/vTz
Gu6QUDi2kpg/cr5A1rwq4d5uIEaglvi9G8YXNa/wkqOrNsuP660Wj8u9QgIWPwdV
ikYJShaHRHFxk3Qr//3P3lg0vgc4AuDcs/r4a0LET7dzuIt0qZymoQKPuOwXpfgY
gxjEmtwLRv5BgM8=
-----END CERTIFICATE REQUEST-----

```

Рис. 5. Пример файла, содержащего CSR

Более подробную информацию можно найти по адресу:

<https://tech-itcore.pl/2012/07/04/generowanie-wlasnego-certyfikatu-ssl/>

<https://uk.godaddy.com/help/apache-generate-csr-certificate-signing-request-5269>

В форме должна быть возможность указать адрес электронной почты, на который пользователь получит форму с ответом.

В форме с ответом оператор ZSL, оператор OBU получает сертификат клиента, закодированный в формате base64.

Его нужно расшифровать. **Не следует добавлять к нему строку BEGIN/END CERTIFICATE**, нужно только использовать инструмент, способный декодировать текст, закодированный в Base64, напр.:

3. Notepad++ > Плагины > Mime Tools > Base64 Decode
4. openssl base64 -d -in файл_с_закодированным_сертификатом.txt -out certyfi.kat.pem
5. Страница <https://www.base64decode.org/>
6. Certutil -decode файл_с_закодированным_сертификатом.txt certyfi.kat.pem (для Windows с помощью командной строки).

Пример сертификата в base64 показан на Рис. 6.

```
LS0tLS1CRUdJTTI8DRVJUSUZJQ0FURSB0LS0tck13SUVqekNOQW5jQ0FnRlhNQTBlHQ1NkRINjYjNEUUVVC3dVQ
U1DQXhIakFjQmdOVK7BTU1GVU5sY255cFptbGokWWhSbE1FRjFkR2h2Y21sMGVUQWVWZzB4T0RBNNU1USXhNRE
V3TwpkYUz3MhhPVEE1TVRJeE1ERXdaaRhtU1HRgpUukF3RGdZRFZRUURFd2RvYjIxbExuQnNNU113RkFRZFRZ
RUUUFdZfVYjIxbExuQnNjSE53TG1vdU1Rc3dDUV1EC1ZRUUdF0pRVERFYk1Ca0dBHVVFQ0jNUZVTRmpRz1r
Ym1sdmNHOXRlM0p6YTJsbE1SRXEdEd1EV1FRSEV3aHoKZWI0N1pxTnBiaKVjTU3vR0NTcUdTSWlzfRFFSkFSW
USZV1J0YVc1QWFOXRaUzV3YkRQ0FTSxdEUV1KS29aSQpedmHOQVFFQk3RQRnZ0VQURDQ0FRb0NnZ0VCQU
1RMVpSY1NnZ1HMRzRwSC9TWExvYwJZTjVsa3NCcTFpcXorCmVUcTBPMVko0enRiRkYVZ1ZYWhPc1JwZEfnyWf
ieGNGZudTznZjYkVPMGtEeThjN1cVdmpMcVQwSGFuZEt3QUwKV1BSndGaDawR2RjRHJaTVRNTG1jbE24a09B
Nzhnd1Z5R3VzTTNSNip2V0tvQ204bwVpk2NVDEpOTENpWtdwQgpaRT1vZnN1RnXcd2Z1Mj10QWFMVZOT1FVS
1QyQj1hukIwMeJQVhZwQX11dwe5VhpFK2h2ZjIyQ290Sm9FMXh6CkE0W10REFEM0dmS1VDMnZmZ31UMHBkbn
c0e13pa1U5TGRpR05ja1VGH8FTUJQM1o3amZrHngvW1JkRzg3dWIKZWIW110MEFRbj1vcURLc59LW15d3p
jaH9WbHE1NW1QVz20QnFRTDNNAH8iQmNjcz2VQ0F3RUFBYU5StUH8dwpDUV1EV1IwVEJBSXdBREfKQmdOVkhr
NEVGZ1FVNGFqcFRmekVtmet1Zz31ckRxejvSS1Nr0WVd0RnMURWUjBQCkFRSC9CQVFEQWdPSU1CtUdBMVvKS
IFRTU18b0edDQ3NHQVFRK73TUNNQjhHQTFVZE13dV1NQwFRk11bD3aQUkKbk81NER1OTQzd1dJNDUrc1Z3ck
NNQTBHQ1NkRINjYjNEUUVVC3dVQ0E0SUNBUUJvYmZRUUkV0HHZ0h1M1dDMQpIUdu2QXY2Wkk3b2sZaVA1bXp
xUmXzRHN3SU5uNHJWkhvcmppQVFDdHcyan1NeU1obU1kOFJ1bm1hUUNSVuk4Cn8XcXdhL1J0Q11idEdEL0pH
bE3zdnR5bzV3d3A2Tm9tVFB5TE55WVhLMUJUWmo3RwZXR1g3aH10SGRmNH8aZCBKMTk0V2hucnR3SV1UbW1NV
HkV13VubHhW09ieG95MeRyZXkyOT1nVVR0eThNbnVYNGNuNm03dmVsURMRTVjKwptRGN4VUE5MjNlcX1jMe
V1M1F0VpNdk5FanVES3d0eGhYnZmYrWdsE68yYkSIwMvPQVNBkVBBEFqZw11JdfQzCktUeXRkMct1amo1df1
hS2tRnkRSNGZSVUUFUjErb2xTYj1TUTU3dkQ5Rwcz2UXabXhCQ3Vd0Hhwz2JuZvdTWfUKU1K1L0h2uVhVnQ0
aDc2RwD0c01V0WdVn1dCRWgzZ0thNjFDZTUybtRzY1h1YmpjMvBuTUE3eXRXaUNEeGtoNqpsMh5WVRkeF1oM
FdTcWNeUy8zS11mVkJZe1Y0eHhZUWhUvH1VcndxNEt1M3p2bXN1V2k5bmZweXcvUeVpTNRc1ZANURtUVpuYn
Byd1h1aU5M2FvNhDVk3VRzZzeehhemNvVhd4YnZBeT1B21JGaEJ1S0g1TTE1Q0FrQp3MNgkKb1Cv3pXb3B
UY29EN1NXNuthVme84RVQyM29rZUpqMGYSk9EN1pOV2wrVzBSbk1ak8DYtk0Z0FWS0J1M3B1bgphdWYV1Vk
T1NemW50bU9aUudMhtpsU0rR2IwdXpJdHdraEN1OSTwME4T2xv0FBPN2NTWHS0UF0FJ353HDcndYbGuxV
1Ayk3hhhbZsUnhudejhsVHZxc2VRPT0KLS0tLS1FtkQgQ0VSVE1GSUNBVEUtlS0tLQo=
```

Рис. 6. Сертификат, закодированный в Base64

В свою очередь, пример сертификата, декодированного в формате PEM (ang. Privacy-Enhaced Mail), показан на Рис. 7.

к инструментам/компонентам SSL/TLS включают использование в процессе аутентификации SSL следующих элементов:

1. сертификата клиента;
2. закрытого ключа, который обеспечивает возможность использования сертификата клиента только субъектом, который является его владельцем;
3. цепочки сертификации / цепочки сертификатов (ang. certificate chain), которая аутентифицирует сертификат клиента как сертификат, выданный компетентным CA, и содержит:
 1. Сертификат CA (Centrum Autoryzacji) уровня 1, выдавший сертификат клиента,
 2. Сертификат CA (Centrum Autoryzacji) уровня 0, выдавший сертификат CA уровня 1.

В среде Linux соединение с SPOE KAS можно протестировать с помощью инструмента curl. Последовательность команд представлена ниже. Certyfikat.pem означает полученный сертификат, который был декодирован из формата base64 в формат PEM. С другой стороны, fd1.key означает закрытый ключ (расшифрованный), используемый для генерации 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.spoev-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001
```

Примечание 1: Адрес <https://cloud.spoev-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001> следует заменить адресом из формы, полученной по электронной почте, речь идет о содержимом поля **URL-адрес услуги e-TOLL, предназначенный для связи с услугой оператора ZSL или оператора OBU.**

Примечание 2: Сертификат X.509 клиента SSL/TLS со стороны оператора ZSL или оператора OBU

К обязанностям оператора ZSL или оператора OBU относятся:

1. получение вышеуказанного сертификата:
 - a. первого - в результате регистрации услуги,
 - b. каждого последующего - до истечения 365 дней с момента выдачи предыдущего сертификата;
2. использование текущего сертификата X. 509 клиента SSL/TLS для аутентификации связи с интерфейсом данных SPOE KAS.

Первый сертификат X. 509 клиента SSL/TLS выдается в ответ на отправку в SPOE KAS через выделенный портал запроса на выдачу сертификата X. 509 клиента SSL/TLS через одну из двух доступных форм связи:

1. документ XML;
2. форму регистрации услуги, заполняемую на странице услуги SPOE KAS на специальном портале SPOE KAS.

Последующий сертификат может быть получен путем отправки в SPOE KAS через специальный портал запроса на выдачу сертификата X. 509 клиента SSL/TLS через одну из двух доступных форм связи:

1. документ XML;
2. форму обновления данных услуги, заполняемую на странице услуги e-TOLL на специальном портале.

Сертификат X. 509 клиента SSL/TLS, используемый для аутентификации оператора ZSL или оператора OBU при взаимодействии с интерфейсом данных SPOE KAS, является первым из сертификатов, возвращаемых SPOE KAS в ответ на отправку формы/документа XML. Каждый из возвращенных сертификатов начинается со строки „-----BEGIN CERTIFICATE-----”, а заканчивается строкой „-----END CERTIFICATE-----”.

Срок действия сертификата X. 509 клиента SSL/TLS можно посмотреть, используя бесплатный пакет инструментов OpenSSL с помощью следующей команды:

```
openssl x509 -inform PEM -enddate -noout -in файл_с_сертификатом_клиента_x509.pem,
```

где:

1. файл_с_сертификатом_клиента_x509.pem - является примерным именем файла, содержащего сертификат X. 509 клиента SSL/TLS, выданный SPOE KAS.

Ниже приведен пример ответа на в/у команду:

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

где:

1. notAfter - метка поля "не позднее" из сертификата X. 509, содержащего срок действия сертификата, после которого его нельзя использовать или доверять ему;
2. Sep – трехбуквенное сокращение названия месяца, в данном случае это сокращение от September, то есть сентябрь;
3. 30 – день;
4. 08:30:58 – час, минута и секунда;
5. 2020 – год;
6. GMT – трехбуквенное сокращение названия часового пояса, обозначение часового пояса, в данном случае это сокращение от Greenwich Mean Time, означающее, что для получения времени для часового пояса Европа/Варшава необходимо к указанному времени добавить два часа для летнего времени и один час для зимнего времени.

Примечание 3: Конфигурация „mutual TLS”

При конфигурации mutual TLS обратите внимание, что изменение сертификата сервера делает невозможным правильную аутентификацию связи. Информация об изменении сертификата сервера будет распространяться до операторов, в то время как в случае каких-либо проблем с проверкой сертификата сервера можно использовать команды для предварительного просмотра сертификата, т. е.:

```
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
```