

ANLEITUNG für die Anbieter der OBU/ZSL zur Aktualisierung des SSL-Zertifikats

Das SSL-Zertifikat gilt für 1 Jahr ab Ausstellung und ist eine der Voraussetzungen korrekten Ablaufs der Kommunikation der IT-Infrastruktur des Anbieters mit dem e-TOLL-System. Das SSL-Zertifikat ist ein Netzprotokoll, das für sichere Internet-Verbindungen bei der Verschlüsselung auf den WWW-Sites verwendet wird, das die Transaktionen schützt und die von der Post und die WWW-Site versendeten Informationen, wie Passwörter, Logins, persönliche Daten usw. sichert.

Vom Anbieter der OBU/ZSL nicht aktualisiertes SSL-Zertifikat gefährdet die Nutzer des e-TOLL-Systems, die Funktionalitäten des Systems, darunter im Bereich des Transfers der Geolokalisierungsdaten zwecks Berechnung der Gebühr, nicht nutzen zu können.

(Beispiel)

Schritt 1

- gehen Sie zur Seite <https://puesc.gov.pl>
- loggen Sie sich in das Konto im Firmenkontext ein
- wählen Sie im Menü das Bookmark „Forms“ (Formulare)
- öffnen Sie die Leiste „Forms alphabetically“ (Formulare alphabetisch) und tragen Sie „ZSL105“ ein
- öffnen Sie den gefundenen Link

The screenshot shows the PUESC website's 'Forms catalog' page. At the top, there is a navigation menu with items: MY DESKTOP, SERVICES, NETWORK SERVICES, FORMS, HELP, SINGLE WINDOW, NEWS. Below the menu, a breadcrumb trail reads 'PUESC > Services > Forms >'. On the left, a sidebar menu lists various categories, with 'FORMS' highlighted in red. The main content area is titled 'Forms catalog' and includes instructions to search for forms and follow on-screen instructions. Below this, there are sections for 'Mapping PUESC forms to PUESC2' and 'Forms alphabetically'. A search bar contains the text 'ZSL105' and a red 'SEARCH' button. Below the search bar, a list of letters 'A D G I K L O P R S T V W Z' is displayed, with the letter 'S' highlighted in red. Under 'S', a search result is shown: 'SENT ZSL105 - Aktualizacja danych rejestracyjnych usługi ZSL/OBU (SENTI)' with a green dot indicating it is 'Available'. Below the search results, there is a section for 'Forms in groups'.

Schritt 2

- bestätigen Sie die angezeigte NIP-Nummer der Firma

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 >

[Back](#)

DATA OF THE SERVICE OPERATOR

IDENTIFICATION TYPE * ⓘ

NIP

IDENTIFICATION NUMBER * ⓘ

5970551996

[Confirm](#)

3.22.36, Host: 152
Main portal version: 3.22.36

Schritt 3

- wählen Sie das Feld „List of services ” (Verzeichnis der Dienste) aus

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 >

[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

Schritt 4

- in der Spalte „Akcja” (Tätigkeit) wählen Sie die Ikone, die bei der Dienstleistung, die Sie aktualisieren möchten, steht (Dokumentensymbol mit dem grünen Vergrößerungsglas)

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

Service number	Service own name	eTOLL	SENT- GEO	Device status	Creation date	Creator	Modification date	Modifier	Akcja
ZSL-CSFF-8	Test123455 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	registered	2022-04-28 godz.05:54:34	Marek Tomczyk	2022-09-22 godz.10:33:40	Marek Tomczyk	

Schritt 5

- wählen Sie die Taste „Edit service“(Dienstleistung bearbeiten)

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

eTOLL
 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)

LS0L5ICRUDjTBDRLVJU SUZJQ6FUR S0L S0cK1J SUJ SVEINDQKMyZ0F3 SUJBJZ0IDQTNZ0RRWUjpl b1pJaH2TfFRRUxCIUUF3ZU0eEN6QUpCZ05W0kFZVEfQk0KTVJrd0VnWURUUVFJREF0dFFYcHZXmmsWTJ0cPjURtNRHhH Q7FVRU0NdzBTVzV6ZEhsMGRYUW4dWUhfAdONgpb S9GbtJ0cEIDMGdVr0hGaEhOMGQyOTNIIU0JKYm50MGVYUJFQ0J0WVdSaG0yTjZVFEUATURvR0EXVUVDd3d6CldRnJ4WUpoWkNcYVIXRjNzVzV6YJkwaGJubGphQ0JVVWd 0BzJtbHJJRWx1Wm05eWJXRmpIV3B1ZV0d0b0IDaGEKTRZcE1Ta3dKd1IEVIFRRERDQIRSVTVVUVKRR9GkpWRXdnV2x0TUIUGmXjMfNvEdWMLpXd2dNU0JEUVRFApNqjHq1Nxr1N1YJNEUUVKQJZU2MyVnVkrZRrsYjBCcGR Hd3VMkYzTg5C01CNFHEVEISTURreU1qQTRNek0wCk1Gb1hEVEI6TURreU1qQTRNek0wTUZvd11UURxNQWHQTFVRUJoTUNVRX4dRgPBTUJnTIZCQU1NQIVwaFkyVnlkTVJf0R3WURUUVFIREF0WfYI SnpIbUYzVWRFTE1Ba0dB MVVQ2d3QIRVWWhGREFTQmdOVKJBZ01DMJF0zW05MwphV1ZqYtYjsE1Rd3dZ1IEVIFRTERBTKvXbEF32dF4U1BMEdDU3FHU0iMORRRUJBUVBQTRJqkR3QXdnZ0VLCKFvSUJBUURwZkozU2JONTIRNC9WUkxpVHRSSmMwVz JTTWJ0cnNveHoxVn9ac3B6WfnKk5u5XIP0EJYNIpyTkEKZ2VGUUVkamZJfJkwbXJnQ0VNNIBIZINV2N2kzdMEFOZk0VHZXW91E1kQ0FLKz1SUUVX3dKbXhFay95ZAp6E9BV2ldGh50TVvOStVeC9yaDByYVhoZTRJa3FDTJRUY kN SK21KTjYzCtulZVkhWZINDRhaU15RFJ0VW01CkdNMG5jb3htH15MkvTmJrMw9gd1VPQWNNYj0XNzhr2d3NWF5QXVzSh0vEN2SWpSWjzEw5JKzxQVUUEKR0FR25I0Hg1UkVqY1UxcikIInNbBbVnObW13K2hmZ013RHn4R 3c2S3F4S6dVUZaWx1c0GvK1ZURGlvdE92agpFNHcrL2bVHlmZT03QXfYIMxYzlidGMrWEFiQWdNkQfBR2pnZ0YzTUJQmN6QUpCZ05W5FJNRUFQ0FQFNQjBHCkExVWREZ1FXQkJRNzNQmndnSVF2Sm5DZkLwL3BtVfZUyIh5bXNU Q99CZ05W5F4QkFmOEVcQU1DQmVb0d3WUQKvIwbEJbd3dZ1UJ3dZQkJRvUhbD0j3ZdFZ0JnTIZIU01FZ2dFWE1J SUJFNEFVTEJyaUNwUzizNtPpb1Y5MqpGMEcwWENZMUxXbWhnZmFZZN2d2dmQXhDekFKQmdOVkBJBWW RbbEJNTVJrd0VnWURUUVFJREF0dFFYcHZXmmsCklydHBAEVSTUE4R0ExVUVc3dVjJGeWmZcGhKkX4UFRBN0JnTIZCQW9NTkvsdWmZUjVksFYwSU1XQnHJVmoKZ0W1dhdGhU0F0SUZCaHhZUnpkSGRZ2DNrZ1NXNkXp SGwwZfHRZ1FIRmZtWGRqzW5reFBEQTZCZ05WQKfzTQpNMXB0YThXQ1XUWdXbUz0ZdJGdWMyOTNzVzU1WTJnZ1ZHvmpHrZwYXICSmJWnZjbTf0WNTscwJubGphQ0FvCldpMDJLVEVktUJzR0EXVUVBd3dVVTBT1ZDQkhs VthnS1ZSTUIGSnZM1F0UtbF0EhEQWFCZ2tXaGtpRz0MEIKQ1FFV0RYbzJRR2wwYkM1M1Y3VjR3DQWbRE1BMEdDU3FHU0iMORRRUJd1VBQTRJURFRQmZxXhLeDnHWAoxVfDqeGU1R2zQaIn0RGITbGNKYXJ1TDh5Sz4T FVEVDV1QkZsMndvbVo1K2E4T0NEK2FKMmIS25t6pFNaaXRPCllIzE5NTU5T5K08vQ25qa3F5eGUzDh3R3lqcvlgrkR5UtdBjksdenBENJEr0HJM3cvcVFUczJuN24KL0Y5VGd0VmUroEwrV2Y3jJhNMOT31S1SbTn4WW

Schritt 6

- im Pkt. 4 (A request to sign and issue a certificate for the domain indicated by the ZSL/OBU services operator, Forderung der Unterzeichnung und Ausstellung des Zertifikats für die vom Anbieter der Dienstleistung ZSL/OBU genannte Domain) der angezeigten Ansicht ((ZSL112 – UPDATE DATA OF A ZSL/OBU OPERATOR SERVICE, Aktualisierung der Daten der Dienstleistung ZSL/OBU des Anbieters) fügen Sie eine neue CSR (CERTIFICATE SIGNING REQUEST, Forderung der Unterzeichnung des Zertifikats)
- auf dem Formular ZSL112 wählen Sie die Taste „Save ” (Senden)

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-Platności

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-----)

Schritt 7

Beispielhafte Datei mit einem privaten Schlüssel zeigt die Abb. 4 unten.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAua
SvEsSeMUYYdw4fC0WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB
lmKuux1XP0tCsHXgPJ0ezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMR1D4G3cPBD
d00ZqSmX7tHp97q+PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7
KGFjwEl+UxDgsNaSp7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VT2jyf
kW4k8gvltwueKScsc9/OrdIr6YopGg5xwQr+TQIDAQABoIAAQDePSF9cqtF9X4I
TVqk16cqqQQqSU5sokTQSiDbkRQmK1S/JCrcqQ5VZ6Ldz+I260DCYiIA2g1pdcy7a
zCz01ldhtHsWfVBI5HdT1eu2iJO/8Iq2DGQOgC8chQbpQ8HQ1WqVIBaF+ha3W64d
VJlH7f4ctfxoGi8S5XH8Jtgg3JoLdeH9YgaNzQ2LKSx91/PxO6J7sLya82KKUBrp
M3AoumtEt0YRy57JkV7j1YeYUFLpWT7cR5rh2cZs5r1fQTGQjQorWBU/e4Po7PMn
Vbp/qDBqni femd/dxDwydtXtJukplmLdUSK15jAXApr2ZSXZ56espTnuIxxkvuzZ
mny15mItAoGBAP34wh8DZwvUeKIn408osSQzHETMnefIMB0u0yoj94RQZuv8VwAR
eoTeFIEPOQqdB7MSgkgZpNuyYxw+OrQI4mM19W9DyHwnWTxNO7pDJEb6BCukQb
/+bdjLSytmDyVhkGMLMQ1E017MdnrcQRSURvByNRXbDzZoP7wL2bASTAoGBAPGB
HIDDLxcHZkdOWNof2RDE+UbgaU86aI3dtGSsoTo6bmPkXxfe6PJPu8pLwzhVOafZ
EXH4qJ9CIE4r6PelyA944KDwx8mlBsU7E6fEchJaR6xykW8u25Nr5P304szxCTI
987eJmQq+BGUUp7LgC/QlcpIR7yyP+h5CNNAp2FAoGAECsaiCLrzacSvX1+6KXX
Jsowm5ADqBiYTSJegZ88jNQ3LyFbUNToNm13D8Rp4DVzikiGOkE7jXkMs9JWNGphv
NAtTAA4xkR6KW0F4Trvc8+tXx+WDNIqk75jmZCnwmn25yxxlrwJf1A97YFuQ+zF
rHT8Edt6a4vTEebGJm62uMCGYA06NMFH9AmqugrFW0/1lmh4oD01JB7WT8sUjd/
Gw7zwXbLSCfLAnXhGrT1SEIoRAGsUE0RUHK07c0sBU3xhP1zghogqtPAKCKnC530
WcF7KxhqMGUrgHlLXpFkv5EEGwiJTD14hA3EQeSxdNnjDI216ufiukMbf62fK2JT
aMnp4QA4xkR6KW0F4Trvc8+tXx+WDNIqk75jmZCnwmn25yxxlrwJf1A97YFuQ+zF
uOMEHZmoo/FRZXdcZPI0wzcGb4oz4few2Dp2savew5QEGq4v3DZDEHGK5X7Yc+M
skL3MCgqGqVN1+fV4uFHZGgPpMKMX2HUKlpLTVWNVsawe0SBfZ5U5
-----END RSA PRIVATE KEY-----
```

Abb. 4. Beispiel einer Datei mit privatem Schlüssel

Beispiel einer Datei mit CSR zeigt die Abb. 5.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1zCCAB8CAQAwZEXCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAtNQVpPV01FQ0tJ
RTERMA8GA1UEBwwIV0FSU1pBV0ExDDAKBgNVBAoMAA05JVDELMakGALUECwCWjYx
FzAVBgNVBAMMDnd3dy5pdGwud2F3LnBsMSUwIwYJKoZIhvcNAQkBFhZlLmtsaW1h
c2FyYUJpdGwud2F3LnBsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAuaSvEsSeMUYYdw4fC0
WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB1mKuux1XP0tCsHXg
PJ0ezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMR1D4G3cPBDd00ZqSmX7tHp97q+
PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7KGFjwEl+UxDgsNaS
p7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VT2jyfkW4k8gvltwueKScs
c9/OrdIr6YopGg5xwQr+TQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBADj0Du1l
Wqp2GJ/8nam/bjnh2WNSczQ0fjQ6iIk/+rh1Bforeky0J9cz+hRsZt5m9D8UVWkC
u4a/iJicrMZHPhTbC9tKuAk2c29ErXKJeSxR/anRkG9EbD7AB4RFmEjsJo/yRauL
oHetcTqxNPDBspkCmo2eRrKb2LdhCGFQRG4Wx/Gg6iuzd7zZKnOVKMuELpOP/vTz
Gu6QUdi2kpg/cr5A1rwg4d5uIEag1vi9G8YXNa/wkqOrNsuP660Wj8u9QgIWPdV
ikyJShahrHFxk3Qr//3P3lg0vge4AuDes/r4aO1ET7dzuIt0qZymoQKPUoXwPfgY
gxjEmtwLRv5Bgm8=
-----END CERTIFICATE REQUEST-----
```

Abb. 5. Beispiel einer Datei mit CSR

Mehr finden Sie unter:

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

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

Im Formular **muss die Angabe der E-Mail-Adresse**, auf die der Benutzer das Formular mit der Antwort erhält, möglich sein.

Im Formular mit der Antwort erhält der ZSL-/OBU-Anbieter ein Client-Zertifikat, das im Format base64 verschlüsselt ist.

Es ist zu entschlüsseln. **Man soll keine Linie BEGIN/END CERTIFICATE hinzufügen**, es ist lediglich ein Tool, das in Base64 verschlüsselten Text entschlüsseln kann zu verwenden, z. B.:

3. Notepad++ > Plug-Ins > Mime Tools > Base64 Decode
4. openssl base64 -d -in datei_mit_kodiertem_zertifikat.txt -out certyfikat.pem
5. Seite <https://www.base64decode.org/>
6. Certutil -decode datei_mit_kodiertem_zertifikat.txt certyfikat.pem (für Windows bei Nutzung der Eingabeaufforderung).

Beispiel eines Zertifikats in Base64 zeigt Abb. 6.

```
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSB0LS0tCk1JZSUvZekNOQw5jQ0FnR1hNQTBHQ1NxR1NJYjNEUUVQ3dVQ
U1DQXhIakFjQmdOVkbTU1GVUSsV25ScFptbG0KWWhSbE1FRjFkR2h2Y21sMGVUQWVGd2B4T0RBNUIUSXhNRE
V3TwpkYUZY3MhHPVEE1TVRjeE1ERXdNaerRHTU1HRgpNukF3RGoZRFZRUURF02RvYjIxbEkuQnNU113RkFRZ
RUUUtFdzFvYjIxbEkuQnNU1SE53TG1vdU1Rc3dDUV1EC1ZRUUdF0pRVERFYk1Ca0dBmVVFQ0jNU2VtFmpRz1r
Ym1sdmNHOXR1M0p6YTJsbE1SRXdEd11EV1FRSEV3aHoKZW10N1pxTnBiakVjTU3vR0NtCUdtSWIzRFFFskFSW
USZV1j0YVc1QhFH0XRaUzV3YkRDQ0FTSXdEUV1KS29aSQpdmHQ0VFQkJRQRnZ0VQURQ0FR00Nz0VCQU
1RmVp5Y1NnZ1HMRzRiSC9ThExvYnJZTjVsa3NCcTFpcXorCmVucT8PMVkoenRIRkYvZ1ZYWhPc1jwZEFnyWf
ieGNGZudTznJZYkVPMgtEeThjN1cVdnpMcVQvSGFuZEt3QUwKV1B5bndGaDawR2RjRHJaTVRNTG1jbeZ4aU9B
NzhNd1Z5R3VzTTNSNhpZV0tvQ204bwVpK2NVDEpOTENpWtdwQgpaRT1vZnN1RiNkdZ21Mj10QmFMVTZOT1FVS
1QyQj1IhukIwMjQVhZwQX11dWt5VhpFK2h2ZjIyQ290S9fMXh6CkE8WNI0REFEM8dmS1VDMnZmZ31UMHBkbn
c0e1jpa2U5TGRp805ja1VGM8FTUJJQ1o3amZrHmgvhl3KRzg3dWIKZ1JW110MEFRbj1vcURLc59L9W15d3p
jaW9wbHE1NW1QVz20QnFRDnNahBi0wNjczZVQ0F3RUFBYU55TUhb0wpDUV1EV1IwVEJBSXdbREFkQmdOVkhR
NEVGZ1FVNGFqcFRmekVtNmt1Zz31ckRXejv5S1Nr0wNVd0RnNURWUjBQCkFRSC9CQVFEQwdPSU1CTudBMVWks
1FRtU18b0dQ03NHQVFRk13TUNNQjhHQTfVZE13Uv1NQwFRk11b01aQUkKbk81NER10TQzd1dJNDUrc1Z3ck
NNQTBHQ1NxR1NJYjNEUUVQ3dVQUR0SUNBUUJvYmZrdUNkV0HhZ0h1M1d0M0pIUUDU2QXY2Ikk3b2s2aVA1bXp
xUmxzRHN3SU5wNHJWkHvcmpPQUFDDHcyan1NeU1obU1kOFJ1bm1hUUNSVUk4Cn8XcXdhL1j0Q1j1dEdEL0pH
bE3zdnR5bzVj3A2Tm9tVFB5TE55WVhLMUJUwmo3RwZxR1g3aH10SGRiW8aZC8KMTk0V2hucnR3S1Ubh1NV
HkV13Vubhhw0U9ieG95MeRy2XkyOT1nYVROeThNbnVYNGNuNm03dmVsBURmRTVjKwptRGN4VUE5HjHlcX1jMh
V1M1FR0VpNdk5FanVE3d0eGhYnZMyRwdsE6ByYk5IhmVpQvNBIXVBBEFqZw1jdfQzCktUeXrkMCT1amo1dF1
hS2tRnkRSNGZV5UVFJErB2xTYj1TUTU3dkQ5Rnc3ZUxabXhCQ3Vd0HmWZ2juZvdTWfUkU1K1L0h2UvHvWnQ0
aDc2Rwd0c01VdWdVn1dCRWgzZ0tHnjFDZTuybTRzY1h1YmpjHVBuTUE3eXRXaLNEEgtoNQpSM5WVVRkeF1oM
FdTclWUy8zS11mVjZe1Y0eHhZUwhuVH1VcndxNET1M3p2bXN1v2k5bmZwEXcvUEVpZTRNCLZnUDrtUVpuYn
Byd1h1aUUSM2FvVnhDVk1VRzZzZemhheNvVhd4YnZBeT10Z1JGaE3J50g1TTE1Q0FrQp3MhgKbk1CV3pXb3B
UY29EN1NwUthVm84RVQYm29rZUpqMGY5tk9EN1p0V2wrVz8Sbk1aK8dyTkc0Z0FwS0j1M3B1bgphd4IyY1Vk
T1Nemw5obU9aUudNwtpSU0R21wdXpJdHdraEN105twWE4T2xv0FBPN2NtW85cUFp0F3J53h0CndYbGuxV
1Ayk3hhbWz5UnhudjhsVHZxc2VRPT0KLS0tLS1FtkQgQ0VSVE1GSUNBEUTLS0tLQo=
```

Abb. 6. In Base64 verschlüsseltes Zertifikat

Beispiel eines im Format PEM (eng. Privacy-Enhanced Mail) entschlüsselten Zertifikats zeigt die Abb. 7.

1. Client-Zertifikat;
2. Privater Schlüssel – der die Möglichkeit der Nutzung des Client-Zertifikats nur durch die Einheit, der über ihn verfügt, sichert;
3. Zertifikatskette (eng. certificate chain), die das Client-Zertifikat als durch korrektes Autorisierung-Zentrums authentisiert und Folgendes enthält:
 1. Zertifikat CA (Autorisierungs-Zentrum) Niveau 1, das das Client-Zertifikat ausgestellt hat,
 2. Zertifikat CA (Autorisierungs-Zentrum) Niveau 0, das das Zertifikat Niveau 1 ausgestellt hat.

Im Linux-Milieu kann die Verbindung mit SPOE KAS mit Hilfe des Tools curl testen. Die Befehlssequenz wird unten dargestellt. Certyfiikat.pem bedeutet das erhaltene Zertifikat, das von dem Format Base64 in das Format PEM entschlüsselt wurde. fd1.key bedeutet privaten Schlüssel (entschlüsselt), der zur Generierung der CSR verwendet wurde.

```
curl -X POST --cert ./certyfiikat.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/10000000-0001-1001-0001-0000000000001
```

Hinweis 1: Die Adresse <https://cloud.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001> soll durch die Adresse aus dem elektronisch erhaltenem Formular ersetzen, es handelt sic hum den Inhalt des Felds **Address URL of the e-TOLL dedicated after communication with the service Operator ZSL or Operator OBU** (URL-Adresse der e-TOLL Dienstleistung, zur Kommunikation mit der Dienstleistung des ZSL-Anbieters oder OBU-Anbieters dediziert).

Hinweis 2: Zertifikat X.509 des SSL-/TLS-Clients auf Seite des ZSL-Anbieters oder OBU-Anbieters

Zu Pflichten des ZSL-Anbieters oder OBU-Anbieters gehört:

1. Erhalt des o.g. Zertifikats:
 - a. des ersten – infolge der Registrierung der Dienstleistung,
 - b. jedes weiteren vor Ablauf von 365 Tagen ab Ausstellung des vorherigen Zertifikats;
2. Verwendung des aktuellen Zertifikats X.509 des SSL-/TLS-Clients zur Authentifizierung der Kommunikationen mit der Datenschnittstelle SPOE KAS.

Das erste Zertifikat X.509 des SSL-/TLS-Clients wird in Antwort auf Übersendung an SPOE KAS, über das dedizierte Portal, einer Anforderung der Ausstellung eines Zertifikats X.509 des SSL-/TLS-Clients, über eine der zwei verfügbaren Kommunikationsformen, ausgestellt:

1. XML-Dokument;
2. Registrierungsformular der Dienstleistung, das auf der Seite der Dienstleistung SPOE KAS im dedizierten Portal SPOE KAS ausgefüllt wird.

Das weitere Zertifikat kann durch Übersendung an SPOE KAS über das dedizierte Portal, einer Anforderung der Ausstellung eines Zertifikats X.509 des SSL-/TLS-Clients, über eine der zwei verfügbaren Kommunikationsformen, erhalten werden:

1. XML-Dokument;
2. Aktualisierungsformular der Daten der Dienstleistung, das auf der Seite der Dienstleistung e-TOLL im dedizierten Portal ausgefüllt wird.

Das Zertifikat X.509 des SSL-/TLS-Clients, das zur Authentifizierung des ZSL-Anbieters oder OBU-Anbieters während der Kommunikation mit der Datenschnittstelle SPOE KAS dient, ist das erste Zertifikat, das von SPOE KAS in Antwort auf Übersendung des XML-Formulars/-Dokuments, zurückgegeben wird. Jedes der zurückgegebenen Zertifikate beginnt mit der Linie „-----BEGIN CERTIFICATE-----“ und endet mit der Linie „-----END CERTIFICATE-----“.

Das Gültigkeitsdatum des Zertifikats X.509 des SSL-/TLS-Clients kann mit Hilfe des kostenlosen Toolpakets OpenSSL, bei Verwendung folgenden Befehls, eingesehen werden:

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

wo:

1. plik_z_certyfikatem_klienta_x509.pem – ein beispielhafter Name der Datei, die das von SPOE KAS ausgestellte Zertifikat X.509 des SSL-/TLS-Client enthält, ist.

Unten ist eine beispielhafte Antwort auf dieses Befehl angeführt:

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

wo:

1. notAfter – Label des Feldes „nicht später“ aus dem Zertifikat X.509 ist, das die endgültige Geltungsfrist des Zertifikats bedeutet, nach der es nicht verwendet und nicht vertraut werden sollte;
2. Sep – Monatskürzel aus 3 Buchstaben, in diesem Fall von September;
3. 30 – Tag;
4. 08:30:58 – Stunde, Minute, Sekunde;
5. 2020 – Jahr;
6. GMT – Kürzel des Zeitzone aus 3 Buchstaben, Bezeichnung der Zeitzone, hier Greenwich Mean Time, was bedeutet, dass um die Zeitzone für Europa/Warschau zu erhalten, 2 Stunden für Sommerzeit und 1 Stunde für Winterzeit addiert werden müssen/muss.

Hinweis 3: Konfiguration „mutual TLS“

Bei der Konfiguration mutual TLS muss man beachten, dass eine Änderung des Server-Zertifikats korrekte Authentifizierung des Kommunikation unmöglich machen wird. Die Information über Änderung des Server-Zertifikats wird an die Anbieter weitergeleitet, wobei man bei irgendwelchen Problemen mit der Verifizierung des Server-Zertifikats Befehle, die Ansicht des Zertifikats ermöglichen, nutzen kann, d. h.:

```
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
```