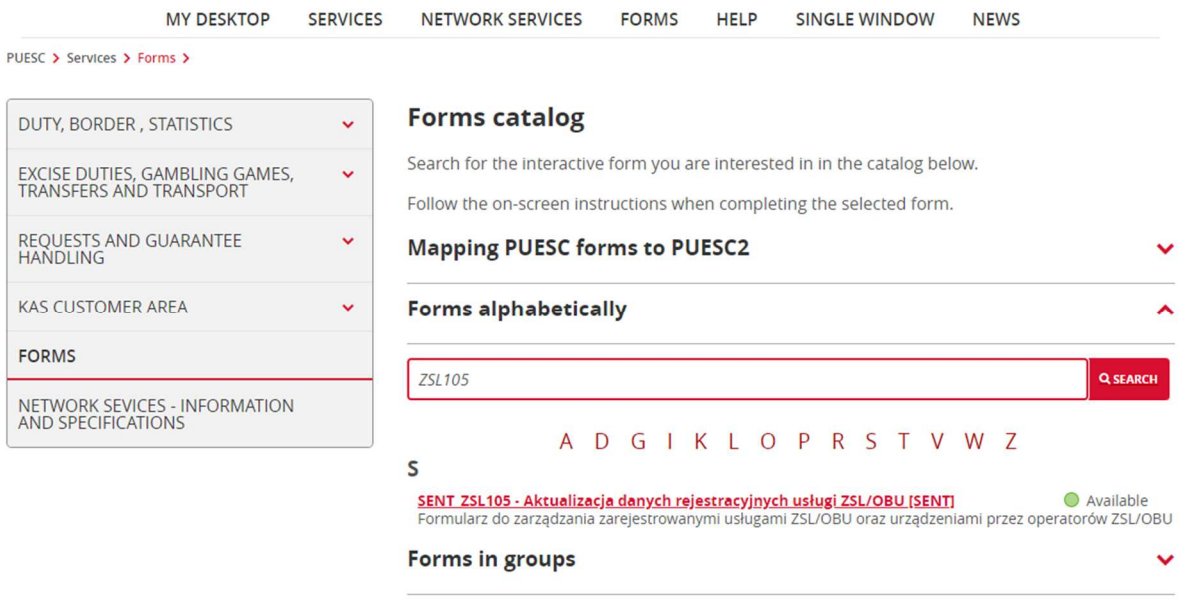
ANLEITUNG für die Anbieter der OBU/ZSL zur Aktualisierung des SSL-Zertifikats

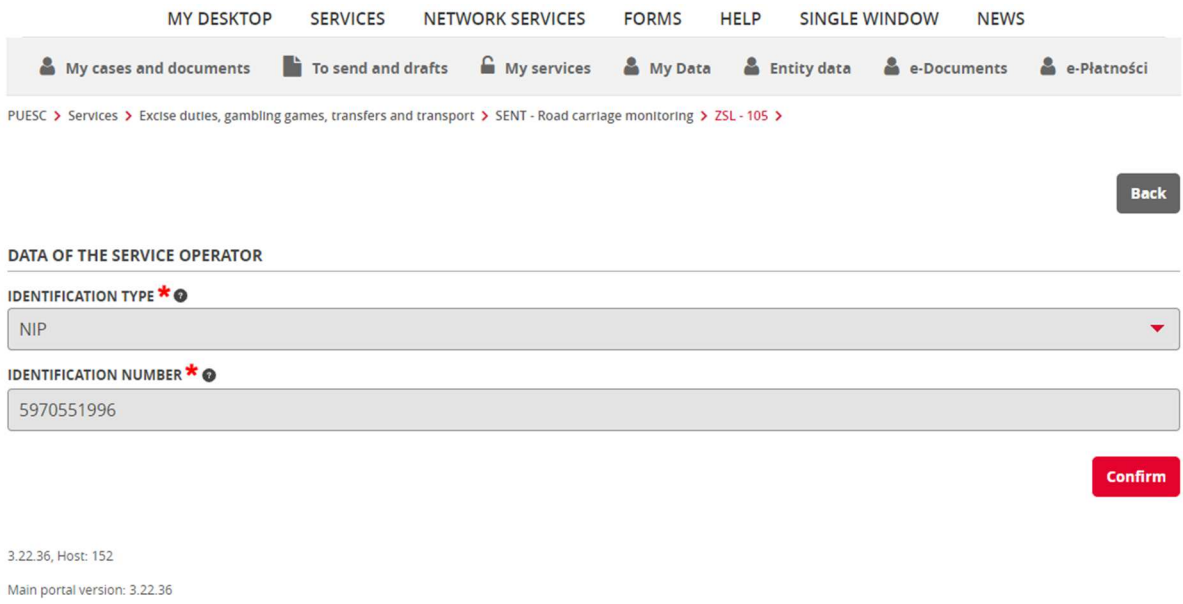
Das SSL-Zertifikat gilt für 1 Jahr ab Ausstellung und ist eine der Voraussetzungen korrekten Ablaufs der Kommunikation der IT-Infrastruktur des Anbieters mit dem e-TOLL-System. Das SSL-Zertifikat ist ein Netzprotokoll, das für sichere Internet-Verbindungen bei der Verschlüsselung auf den WWW-Sites verwendet 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*)

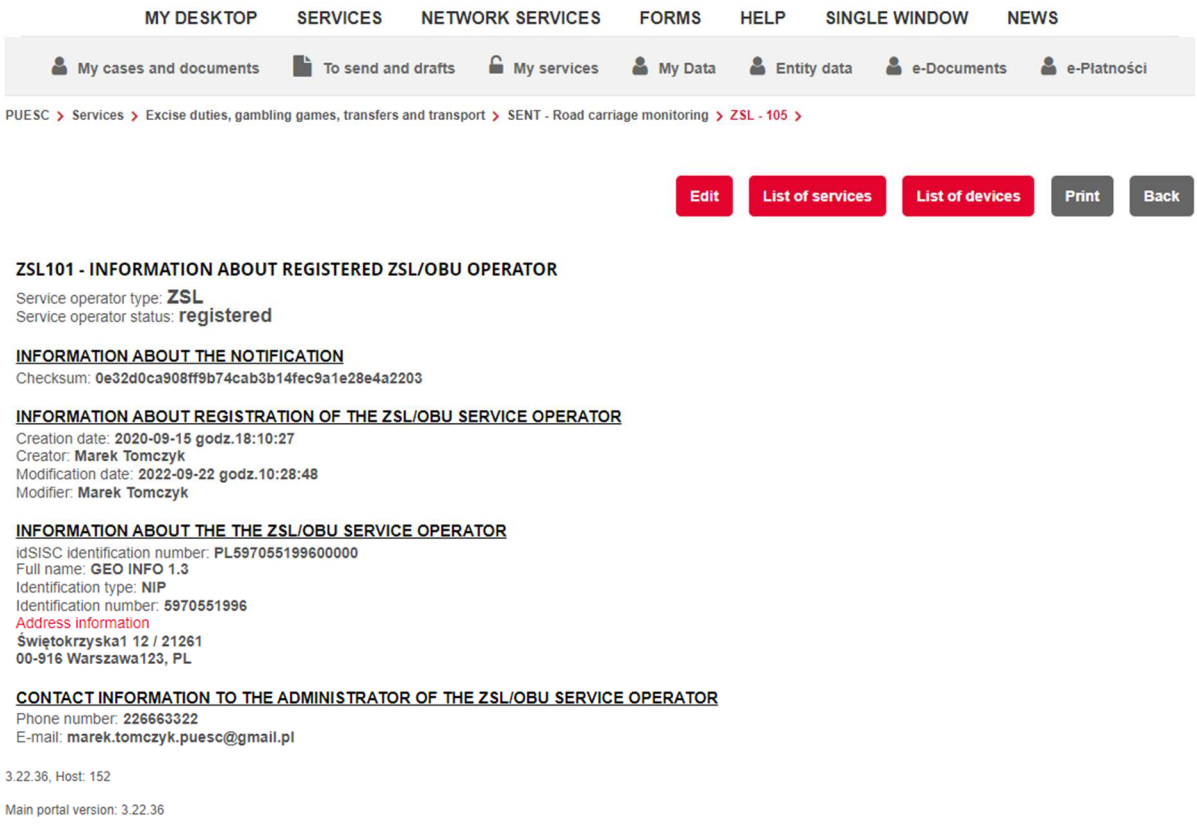
Schritt 1
- gehen Sie zur Seite https://puesc.gov.pl
- loggen Sie sich in das Konto im Firmenkontext ein
- wählen Sie im Menü das Bookmark „Forms“ (Formulare)
- öffnen Sie die Leiste „Forms alphabetically“ (Formulare alphabetisch) und tragen Sie „ZSL105“ ein
- öffnen Sie den gefundenen Link



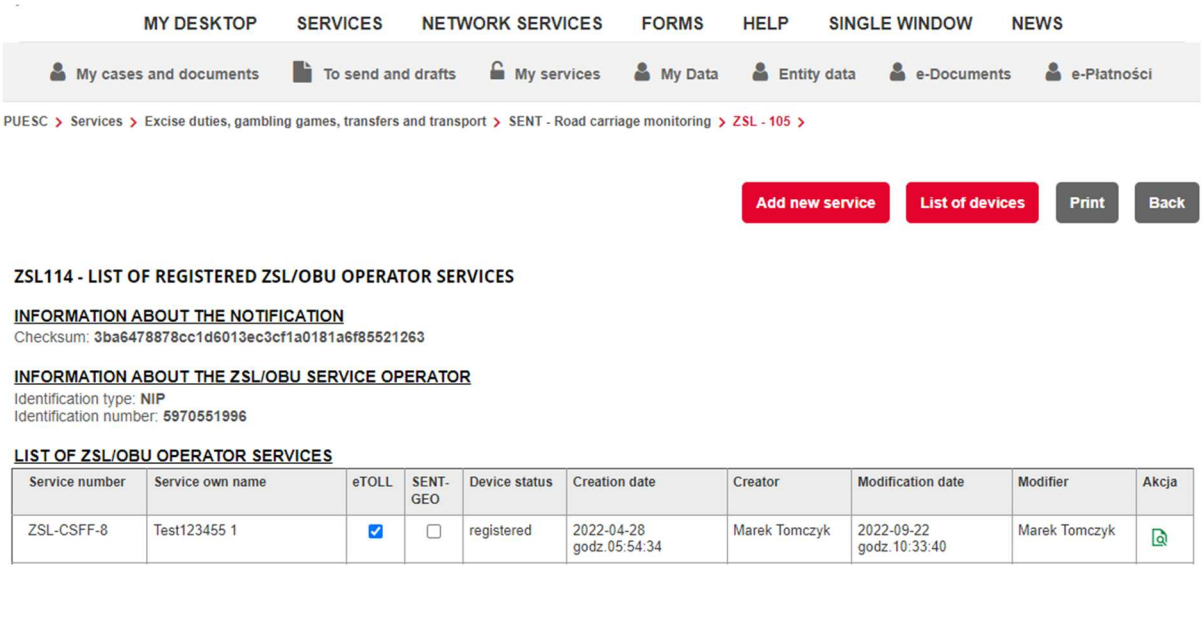
Schritt 2
- bestätigen Sie die angezeigte NIP-Nummer der Firma



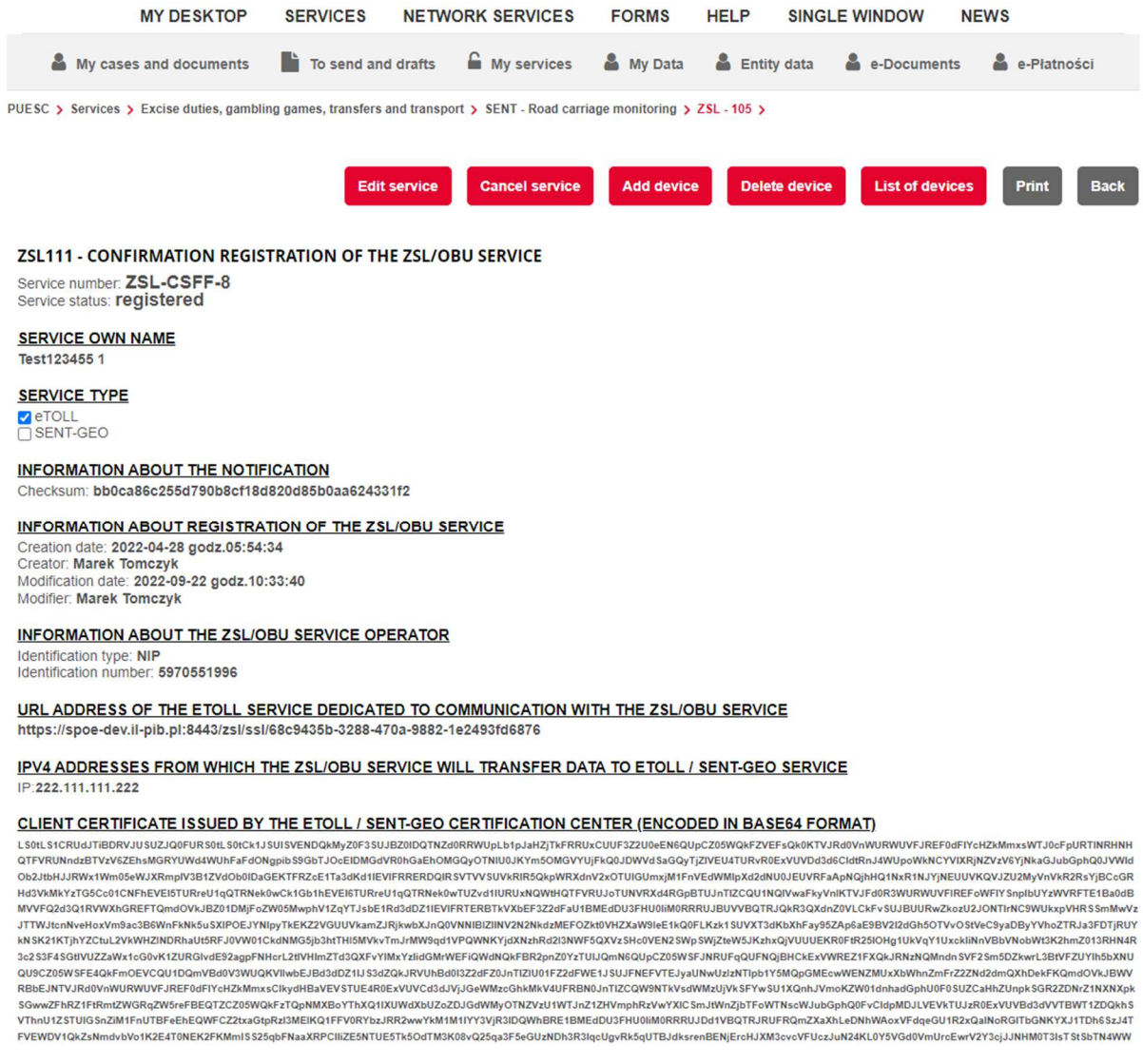
Schritt 3
- wählen Sie das Feld „List of services ” (Verzeichnis der Dienste) aus



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)



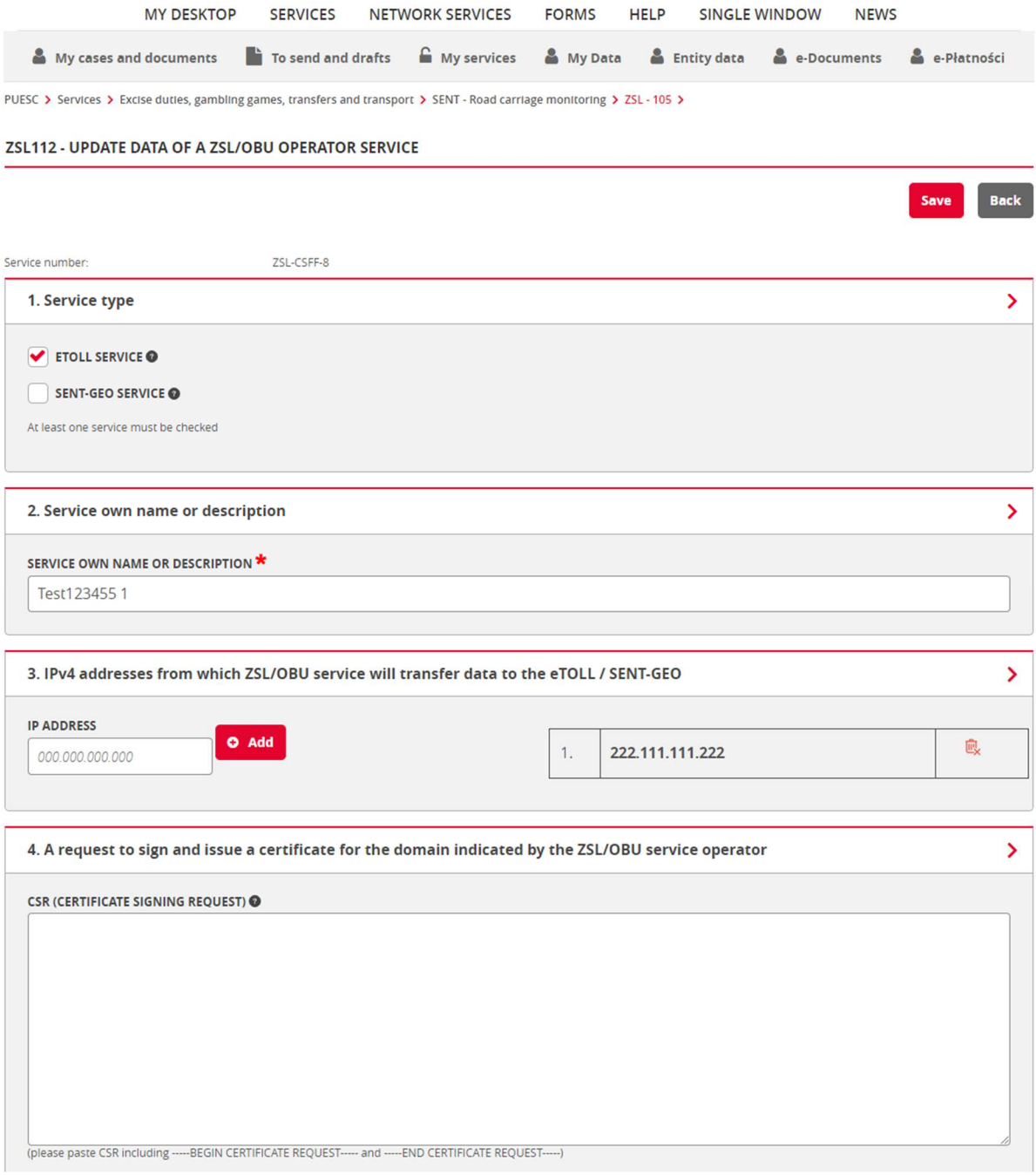
Schritt 5
- wählen Sie die Taste „Edit service ”(Dienstleistung bearbeiten)



LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUISVENDQkMyZ0F3SUJBZ0IDQTNZd0RRWUpLb1pJaHZjTkFRRUxCUUF3Z2U0eEN6QUpCZ05WQkFZVEFsQk0KTVJRd0VnWURWUVFJREF0dFIYcHZkMmxsWTJ0cFpURTINRHNH
QTFVRUNndzBTVzV6ZEhsMGRYUWd4WUhFaFdONgpib59GbTJOcElDMGdVR0hGaEhOMGQyOTNIU0JKYm5OMGVYUjFkQ0JDWVdSaGQyTjZIVEU4TURvR0ExVUVDd3d6ClddtRnJ4WUpoWkNCYVlXRjNZVzV6YjNkaGJubGphQ0JVWld
Ob2JtbHJJJRWx1Wm05eWJXRmplV3B1ZVdOb0lDaGEKTFRZcE1Ta3dKd1lEVlFRRERDQlRSVTVVSUVkRlR5QkpWRXdnV2xOTUlGUmxjM1FnVEdWMlpXd2dNU0JEUVRFaApNQjhHQ1NxR1NJYjNEUUVKQVJZU2MyVnVkR2RsYjBCcGR
Hd3VkMkYzTG5Cc01CNFhEVEI5TURreU1qQTRNek0wCk1Gb1hEVEI6TURreU1qQTRNek0wTUZvd1IURUxNQWtHQTFVRUJoTUNVRXd4RGpBTUJnTlZCQU1NQlVwaFkyVnlKTVJFd0R3WURWUVFIREFoWFIY SnplbUYzWVRFTE1Ba0dB
MVVFQ2d3Q1RVWXhGREFTQmdOVkJBZ01DMjFoZW05MwphV1ZqYTJsbE1Rd3dDZ1IEVlFRTERBTkVXbEF3Z2dFaU1BMEdDU3FHU0lIM0RRRUJBUVVBQTRJQkR3QXdnZ0VLCkFvSUJBUURwZkozU2JONTlrNC9WUkxpVHRS SmMwVzJTTWJtcnNveHoxVm9ac3B6WnFkNk5uSXlPOEJYNlpyTkEKZ2VGUUVkamZJRjkwbXJnQ0VNNlBIZlINV2N2NkdzMEFOZkt0VHZXaW9leE1kQ0FLKzk1SUVXT3dKbXhFay95ZAp6aE9BV2I2dGh5OTVvOStVeC9yaDByYVhoZTRJa3FDTjRUY
kNSK21KTjhYZCtuL2VkWHZlNDRhaUt5RFJ0VW01CkdNMG5jb3htTHI5MVkvTmJrMW9qd1VPQWNKYjdXNzhRd2l3NWF5QXVzSHc0VEN2SWpSWjZteW5JKzhxQjVUUUEKR0FtR25lOHg1UkVqY1UxckliNnVBbVNobWt3K2hmZ013RHN4R
3c2S3F4SGtlVUZZaWx1cG0vK1ZURGlvdE92aggpFNHcrL2tlVHlmZTd3QXFvYlMxYzlidGMrWEFiQWdNQkFBR2pnZ0YzTUlJQmN6QUpCZ05WSFJNRUFqQUFNQjBHCkExVWREZ1FXQkJRNzNQMndnSVF2Sm5DZkwrL3BtVFZUYlh5bXNU
QU9CZ05WSFE4QkFmOEVCQU1DQmVBd0V3WUQKVllwbEJBd3dDZ1IJS3dZQkJRVUhBd0I3Z2dFZ0JnTlZlU01FZ2dFWE1JSUJFNEFVTEJyaUNwUzlzNTlpb1Y5MQpGMEcwWENZMUxXbWhnZmFrZ2ZNd2dmQXhDekFKQmdOVkJBVV
RBbEJNTVJRd0VnWURWUVFJREF0dFlYcHZkMmxsCIkydHBaVEVSTUE4R0ExVUVCd3dJVjJGeWMzcGhkMkV4UFRBN0JnTlZCQW9NTkVsdWMzUjVkSFYwSU1XQnhJVmoKZW01dnhadGphU0F0SUZCaHhZUnpkSGR2ZDNrZ1NXNXpk
SGwwZFhRZ1FtRmtZWGRqZW5reFBEQTZCZ05WQkFzTQpNMXBoYThXQ1lXUWdXbUZoZDJGdWMyOTNZVzU1WTJnZ1ZHVmphRzVwYXIC SmJtWnZjbTFoWTNscWJubGphQ0FvCldpMDJLVEVkTUJzR0ExVUVBd3dVVTBWT1ZDQkhS
VThnU1ZSTUlGSnZiM1FnUTBFeEhEQWFCZ2txaGtpRzl3MEIKQ1FFV0RYbzJRR2wwYkM1M1lYY3VjR3lDQWhBRE1BMEdDU3FHU0lIM0RRRUJDd1VBQTRJRUFRQmZXaXhLeDNhWAoxVFdqeGU1R2xQalNoRGlTbGNKYXJ1TDh6SzJ4T
FVEWDV1QkZsNmdvbVo1K2E4T0NEK2FKMmlSS25qbFNaaXRPCliiZE5NTUE5Tk5OdTM3K08vQ25qa3F5eGUzNDh3R3lqcUgvRk5qUTBJdksrenBENjErcHJXM3cvcVFUczJuN24KL0Y5VGd0VmUrcEwrV2Y3cjJJNHM0T3IsTStSbTN4WW

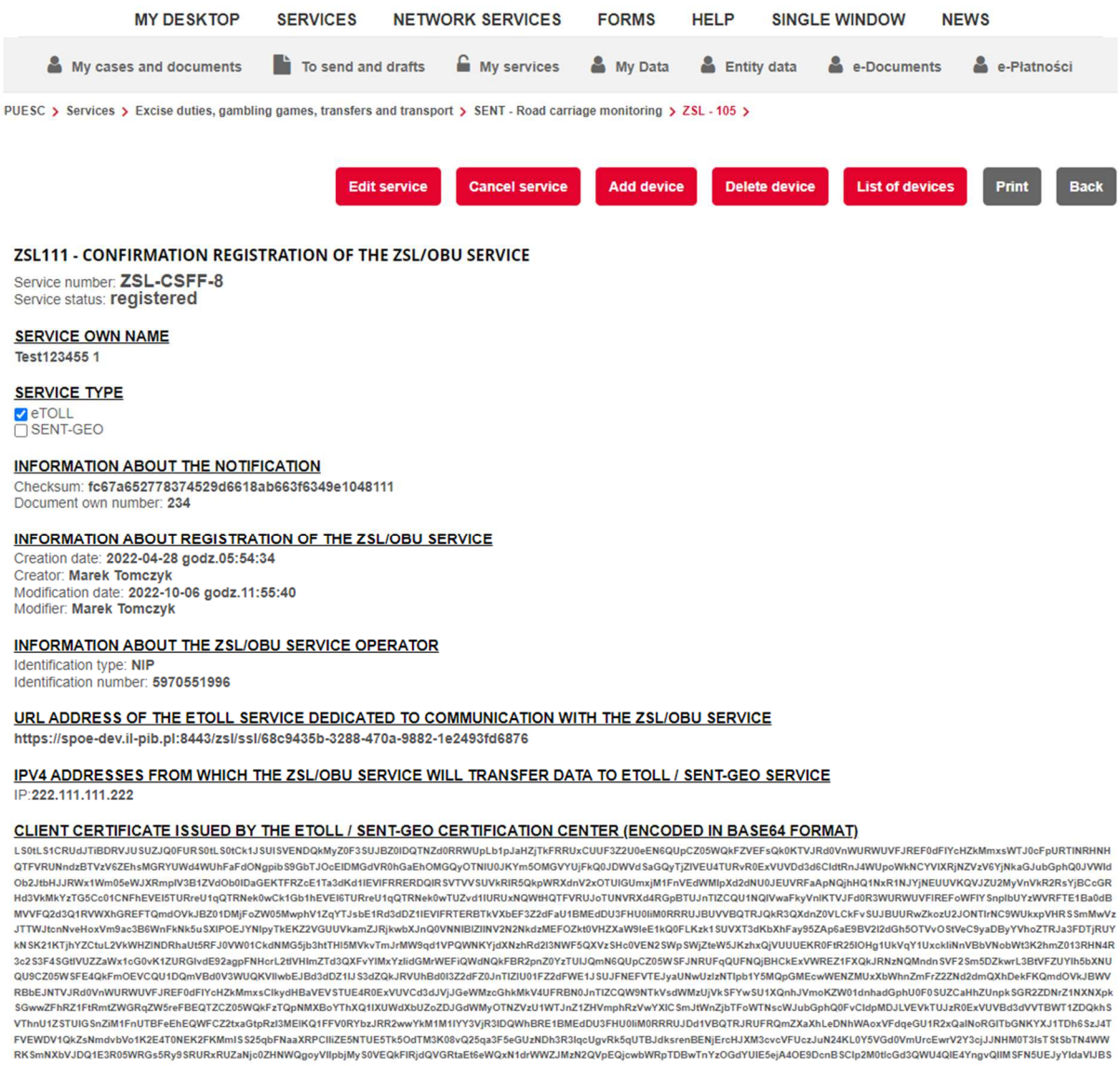
Schritt 6

- 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)



Schritt 7

- Erhalt der Bestätigung der Aktualisierung der Dienstleistung



LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUISVENDQkMyZ0F3SUJBZ0IDQTNZd0RRWUpLb1pJaHZjTkFRUxCUUF3Z2U0eEN6QUpCZ05WQkFZVEFsQk0KTVJRd0VnWURWUVFJREF0dFIYcHZkMmxsWTJ0cFpURTINRHNH
QTFVRUNndzBTVzV6ZEhsMGRYUWd4WUhFaFdONgpibS9GbTJOcEIDMGdVR0hGaEhOMGQyOTNlU0JKYm5OMGVYUjFkQ0JDWVdSaGQyTjZlVEU4TURvR0ExVUVDd3d6CldtRnJ4WUpoWkNCYVIXRjNZVzV6YjNkaGJubGphQ0JVWld
Ob2JtbHJJRWx1Wm05eWJXRmpIV3B1ZVdOb0lDaGEKTFRZcE1Ta3dKd1IEVIFRRERDQIRSVTVVSUVkRlR5QkpWRXdnV2xOTUlGUmxjM1FnVEdWMlpXd2dNU0JEUVRFaApNQjhHQ1NxR1NJYjNEUUVKQVJZU2MyVnVkR2RsYjBCcGR
Hd3VkMkYzTG5Cc01CNFhEVEI5TURreU1qQTRNek0wCk1Gb1hEVEI6TURreU1qQTRNek0wTUZvd1IURUxNQWtHQTFVRUJoTUNVRXd4RGpBTUJnTlZCQU1NQlVwaFkyVnlKTVJFd0R3WURWUVFIREFoWFlYSnplbUYzWVRFTE1Ba0dB
MVVFQ2d3Q1RVWXhGREFTQmdOVkJBZ01DMjFoZW05MwphV1ZqYTJsbE1Rd3dDZ1IEVIFRTERBTkVXbEF3Z2dFaU1BMEdDU3FHU0lIM0RRRUJBUVVBQTRJQkR3QXdnZ0VLCkFvSUJBUURwZkozU2JONTlrNC9WUkxpVHRSSmMwVz
JTTWJtcnNveHoxVm9ac3B6WnFkNk5uSXlPOEJYNlpyTkEKZ2VGUUVkamZJRjkwbXJnQ0VNNIBlZlINV2N2NkdzMEFOZkt0VHZXaW9leE1kQ0FLKzk1SUVXT3dKbXhFay95ZAp6aE9BV2l2dGh5OTVvOStVeC9yaDByYVhoZTRJa3FDTjRUY
kNSK21KTjhYZCtuL2VkWHZlNDRhaUt5RFJ0VW01CkdNMG5jb3htTHI5MVkvTmJrMW9qd1VPQWNKYjdXNzhRd2I3NWF5QXVzSHc0VEN2SWpSWjZteW5JKzhxQjVUUUEKR0FtR25lOHg1UkxqY1UxckliNnVBbVNobWt3K2hmZ013RHN4R
3c2S3F4SGtlVUZZaWx1cG0vK1ZURGlvdE92agpFNHcrL2tlVHlmZTd3QXFvYlMxYzlidGMrWEFiQWdNQkFBR2pnZ0YzTUlQamN6QUpCZ05WSFJNRUFqQUFNQjBHCkExVWREZ1FXQkJRNzNQMndnSVF2Sm5DZkwrL3BtVFZUYlh5bXNU
QU9CZ05WSFE4QkFmOEVCQU1DQmVBd0V3WUQKVlIwbEJBd3dDZ1IJS3dZQkJRVUhBd0I3Z2dFZ0JnTlZIU01FZ2dFWE1JSUJFNEFVTEJyaUNwUzlzNTlpb1Y5MQpGMEcwWENZMUxXbWhnZmFrZ2ZNd2dmQXhDekFKQmdOVkJBWV
RBbEJNTVJRd0VnWURWUVFJREF0dFIYcHZkMmxsYlkydHBaVEVSTUE4R0ExVUVCd3dJVjJGeWMzcGhkMkV4UFRBN0JnTlZCQW9NTkVsdWMzUjVkSFYwSU1XQnhJVmoKZW01dnhadGphU0F0SUZCaHhZUnpkSGR2ZDNrZ1NXNXpk
SGwwZFhRZ1FtRmtZWGRqZW5reFBEQTZCZ05WQkFzTQpNMXBoYThxQ1lXUWdXbUZoZDJGdWMyOTNZVzU1WTJnZ1ZHVmphRzVwYXlC SmJtWnZjbTFoWTNscWJubGphQ0FvVGldpMDJLVEVkTUJzR0ExVUVBd3dVVTBWT1ZDQkhS
VThnU1ZSTUlGSnZiM1FnUTBFeEhEQWFCZ2txaGtpRzl3MElKQ1FFV0RYbzJRR2wwYkM1M1IYY3VjR3lDQWhBRE1BMEdDU3FHU0lIM0RRRUJDd1VBQTRJRUFRQmZXaXhLeDNhWAoxVFdqeGU1R2xQalNoRGlTbGNKYXJ1TDh6SzJ4T
FVEWDV1QkZsNmdvbVo1K2E4T0NEK2FKMmlSS25qbFNaaXRPCllIZE5NTUE5Tk5OdTM3K08vQ25qa3F5eGUzNDh3R3lqcUgvRk5qUTBJdksrenBENjErcHJXM3cvcVFUczJuN24KL0Y5VGd0VmUrcEwrV2Y3cjJJNHM0T3IsTStSbTN4WW
RKSmNXbVJDQ1E3R05WRGs5Ry9SRURxRUZaNjc0ZHNWQgoyVIlpbjMyS0VEQkFIRjdQVGRtaEt6eWQxN1drWWZJMzN2QVpEQjcwbWRpTDBwTnYzOGdYUlE5ejA4OE9DcnBSClp2M0tlcGd3QWU4QlE4Ynl gvQlIMSFN5UEJyYldaVlJBS

ZUSATZINFORMATIONEN

Der Nutzer füllt die Felder des Formulars. Im Feld **A request to sign and issue a certificate for domain indicated by the ZSL/OBU service operator** (Forderung der Unterzeichnung und Ausstellung des Zertifikats für die vom Anbieter der Dienstleistung ZSL/OBU genannte Domain) fügt er die CSR (engl. Certificate Signing Request) ein. Die CSR generiert sich anhand des Privatschlüssels. Mann kann dazu openssl (www.openssl.org) nutzen. Wenn der Benutzer schonen einen privaten Schlüssel hat (z.B. Datei private.key), wird das Befehl im Linux-Milieu folgenden Aufbau haben wird:

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

Falls der Benutzer keinen privaten Schlüssel hat, kann er ihn generieren, z. B. bei:

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

(Länge 4096 Bits gibt besseres Sicherheitsniveau als der Schlüssel 2048).

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

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAua
SvEsSeMUYYdw4fC0WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB
lmKuux1XP0tCsHXgPJOezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMR1D4G3cPBD
dOOZqSmX7tHp97q+PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7
KGFjwEl+UxDgsNaSp7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyf
kW4k8gvltwueKScsc9/Ordlr6YopGg5xwQr+TQIDAQABAoIBAQDePSF9cqTf9X4I
TVqkl6cqkQQqSU5sokTQSidbkRQmKlS/JCrqQ5VZ6Ldz+l260DCYiiA2g1pdcy7a
zCz0lldhtHsWfVBI5HdTleu2iJO/8Ig2DGQOgC8chQbpQ8HQ1WqVIBaF+ha3W64d
VJlH7f4ctfxoGi8S5XH8Jtgq3JoLdeH9YqaNzQ2LKSx91/PxO6J7sLya82KKUBrp
M3AOumtEt0YRy57JkV7j1YeYUFLpWT7cR5rh2cZs5r1fQTGQjQorWBu/e4Po7PMn
Vbp/qDBqnifemd/dxDWydtXtJukp1mLdUSK15jAXApr2ZSXZ56espTnuIxkkvuzZ
mnyl5mItAoGBAP34wh8DZwvUeKIn408osSQzHEtMnefIMB0u0yoj94RQZuv8VwAR
eoTeFIEPOQqgdB7MSgkgZpNuyYxW+OrQI4mMl9Wh9DyHwnWTxNO7pDJEb6BCukQb
/+bdjLSytmDyVhkGMlMQlE0l7MdncrQRSURvByNRXbDzzoP7wlL2bASTAoGBAPGb
HIDDlxcHZkdOWNof2RDE+UbgaU86aI3dtGSsoTo6bmPkXxfe6PJPu8pLwzhVOaf2
EXH4qJ9CiOE4r6PelyA944KDwx8mlBsU7E6fEchJaR6xykW8u25Nr5P304szxCTI
987eJmQq+BGUUp7LgC/QlcpiR7yyP+h5CNNkAp2fAoGAEcSaiCLrzacSvX1+6KXX
Jsowm5ADqBiYTSJegZ88jNQ3LyFbUNToNm13D8Rp4DVzikgOke7jXkMs9JWNGphv
NAtTAA4xkR6KW0F4Trvc8+tXx+WDNIqk75jmZCnwmn25ykxlruwJflA97YFuQ+zF
rHT8Edt6a4vTEebGJJm62uMCgYA06NMFH9AmgugrFW0/11mh4oD0lJB7WT8sUjD/
Gw7zwXgLSCfLAnXhGrT1SEIoRAGsUE0RuHK07c0sBU3xhP1zghogqtpAKCKnC530
WcF7KxhqMGUrgHlLXpfkv5EEGwIJTDl4hA3EQeSxdNnjDI216ufiukMbf62fK2JT
aMNp4QKBgDxQkHSX8E7FhlUijf3C8IMZsZ7frzCbdIfNX6/PcVrcx3UKSVWmB9/v
auOMEHZmoo/FRZXdcZPI0wzcGb4oz4few2Dp2savew5QEGq4v3DZDEhGK5X7Yc+M
skL3MCgqGqVN1+fV4uFHzGqPpMKMXZHUKlpLTVWNvswe0SBfZ5U5
-----END RSA PRIVATE KEY-----
```

Abb. 4. Beispiel einer Datei mit privatem Schlüssel

Beispiel einer Datei mit CSR zeigt die Abb. 5.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1zCCAb8CAQAwgZExCzAJBgNVBAYTAlBMMRQwEgYDVQQIDAtNQVpPV0lFQ0tJ
RTERMA8GA1UEBwwIV0FSU1pBV0ExDDAKBgNVBAoMA05JVDELMAkGA1UECwwCWjYx
FzAVBgNVBAMMDnd3dy5pdGwud2F3LnBsMSUwIwYJKoZIhvcNAQkBFhZlLmtsaW1h
c2FyYUBpdGwud2F3LnBsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAuaSvEsSeMUYYdw4fC0
WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB1mKuux1XP0tCsHXg
PJOezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMR1D4G3cPBDdOOZqSmX7tHp97q+
PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7KGFjwEl+UxDgsNaS
p7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyfkW4k8gvltwueKScs
c9/Ordlr6YopGg5xwQr+TQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBADjODu11
Wqp2GJ/8nam/bjnh2WNSczQ0FjQ6IiK/+rh1BfOREky0J9cz+hRsZt5m9D8UVWkC
u4a/iJicrMZHPhTbC9tKuAk2c29ErxKJeSXr/anRKg9EbD7AB4RFmEjsJo/yRauL
oHetcTqxNPDBspkCmo2eRrKb2LdhCGFQRG4Wx/Gg6iuzd7zZKnOVKMuELpOP/vTz
Gu6QUDi2kpg/cr5A1rwq4d5uIEaglvi9G8YXNa/wkqOrNsuP660Wj8u9QgIWpWdV
ikYJShaHRHFxk3Qr//3P3lg0vgc4AuDcs/r4aOlET7dzuIt0qZymoQKPuOwXpfgY
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.

Abb. 6. In Base64 verschlüsseltes Zertifikat

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

Abb. 7. Beispiel eines entschlüsselten Zertifikats

Nach Entschlüsselung erhält man eine Datei, die max. drei Zertifikate im PEM-Format enthält:

1. Client-Zertifikat,
2. Zertifikat CA (Autorisierungs-Zentrum) Niveau 1, das das Client-Zertifikat ausgestellt hat,
3. Zertifikat CA (Autorisierungs-Zentrum) Niveau 0, das das Zertifikat Niveau 1 ausgestellt hat.

Jedes Zertifikat beginnt und endet mit folgenden Linien:

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

Diese Linien bedeuten Anfang und Ende der jeweiligen Zertifikate.

Umfang und Art der Nutzung der Daten, die zur Sicherung der TLS-Kommunikation verwendet werden, sind unterschiedlich und hängen vom durch die Einheit verwendeten Systems / Anwendung. Typische Anforderungen an SSL/TLS-Tools/-Komponenten umfassen jedoch Verwendung folgender Elemente bei der SSL-Authentifizierung:

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. Certyfikat.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 ./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/10000000-0001-1001-0001-0000000000001

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 kostenlosem 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