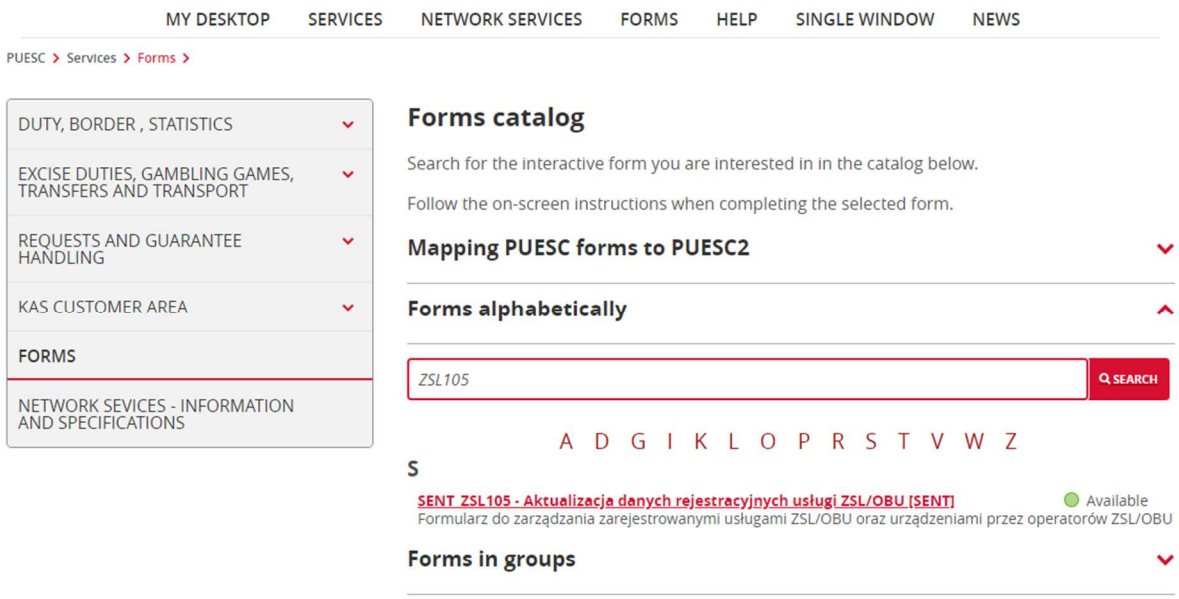
ІНСТРУКЦІЯ для операторів OBU/ZSL в рамках оновлення сертифіката SSL

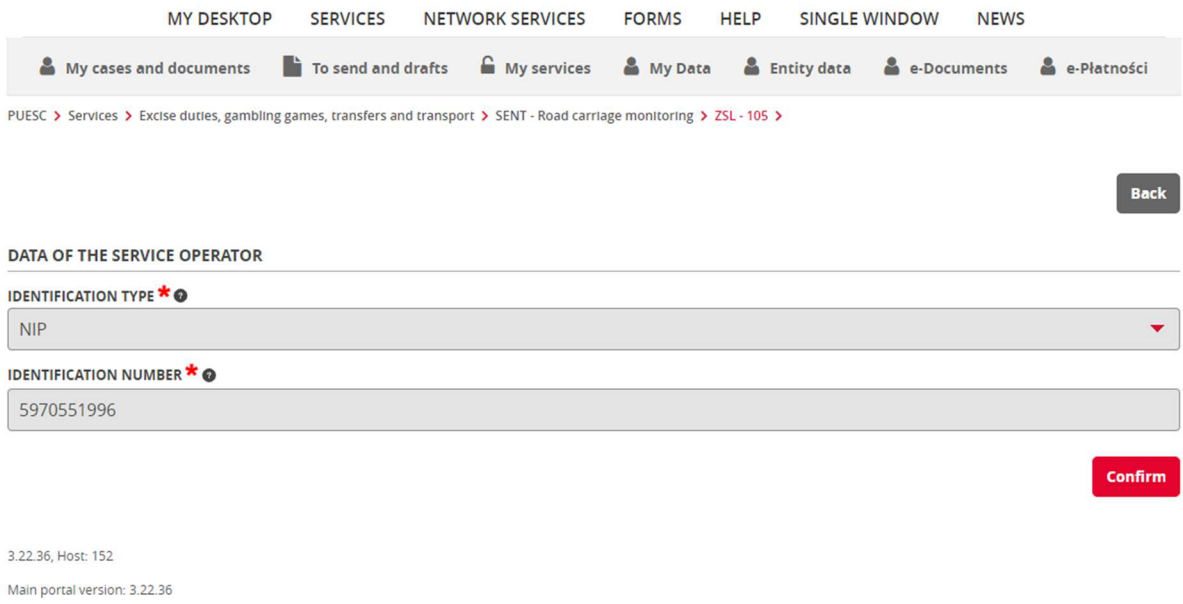
Термін дії SSL-сертифіката дійсний протягом 1 року з дати його видачі та є однією з умов належного функціонування зв'язку ІКТ-інфраструктури оператора з системою e-TOLL. Сертифікат SSL — це мережевий протокол , який використовується для безпечного підключення до Інтернету в області шифрування на веб-сайтах, захисту транзакцій і безпеки інформації, надісланої електронною поштою та веб-сайтом, як-от паролі, логіни, особисті дані тощо.
Відсутність сертифіката SSL, оновленого оператором OBU/ZSL, наражає користувачів системи e-TOLL на неможливість використання функціональних можливостей системи, включаючи передачу даних геолокації з метою розрахунку належної плати.

(*приклад*)

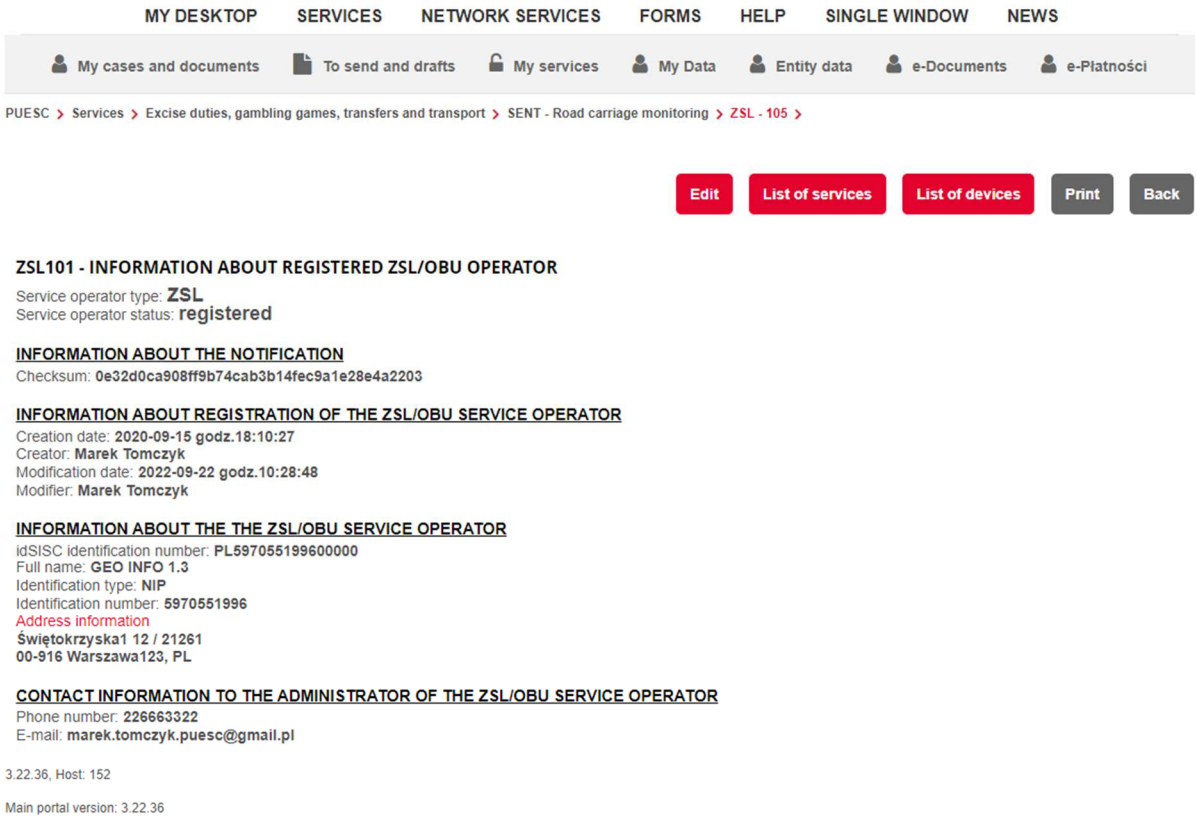
Крок 1
- перейдіть на сайт https://puesc.gov.pl
- увійдіть в обліковий запис в корпоративному контексті
- виберіть в меню вкладку „Forms".
- розгорніть рядок „Forms alphabetically" і введіть „ZSL105"
- відкрийте знайдене посилання



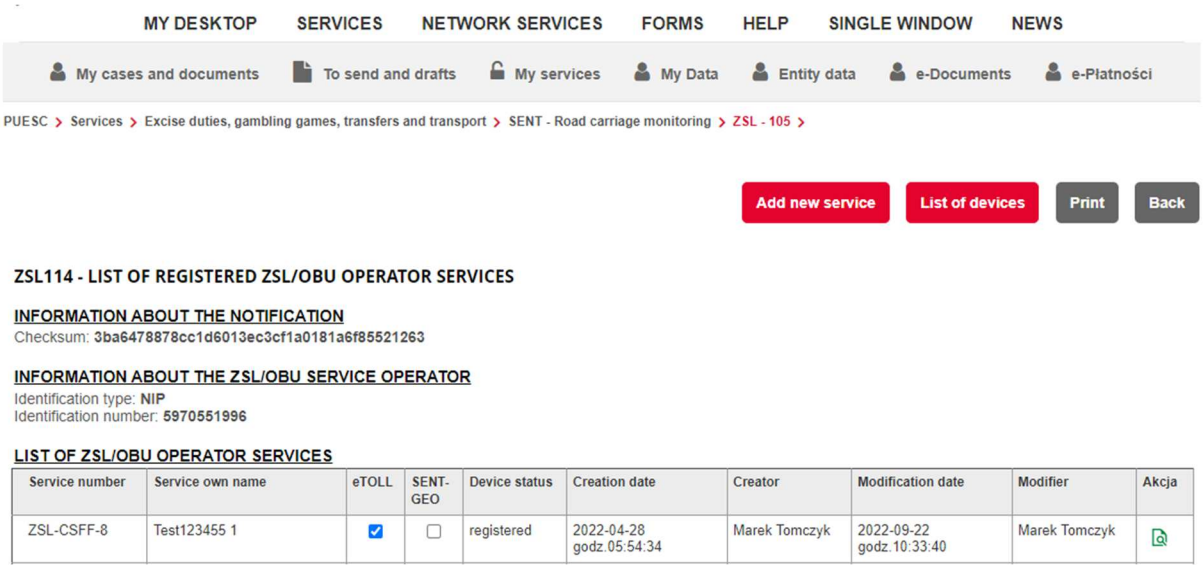
Крок 2
- підтвердіть відображений NIP компанії



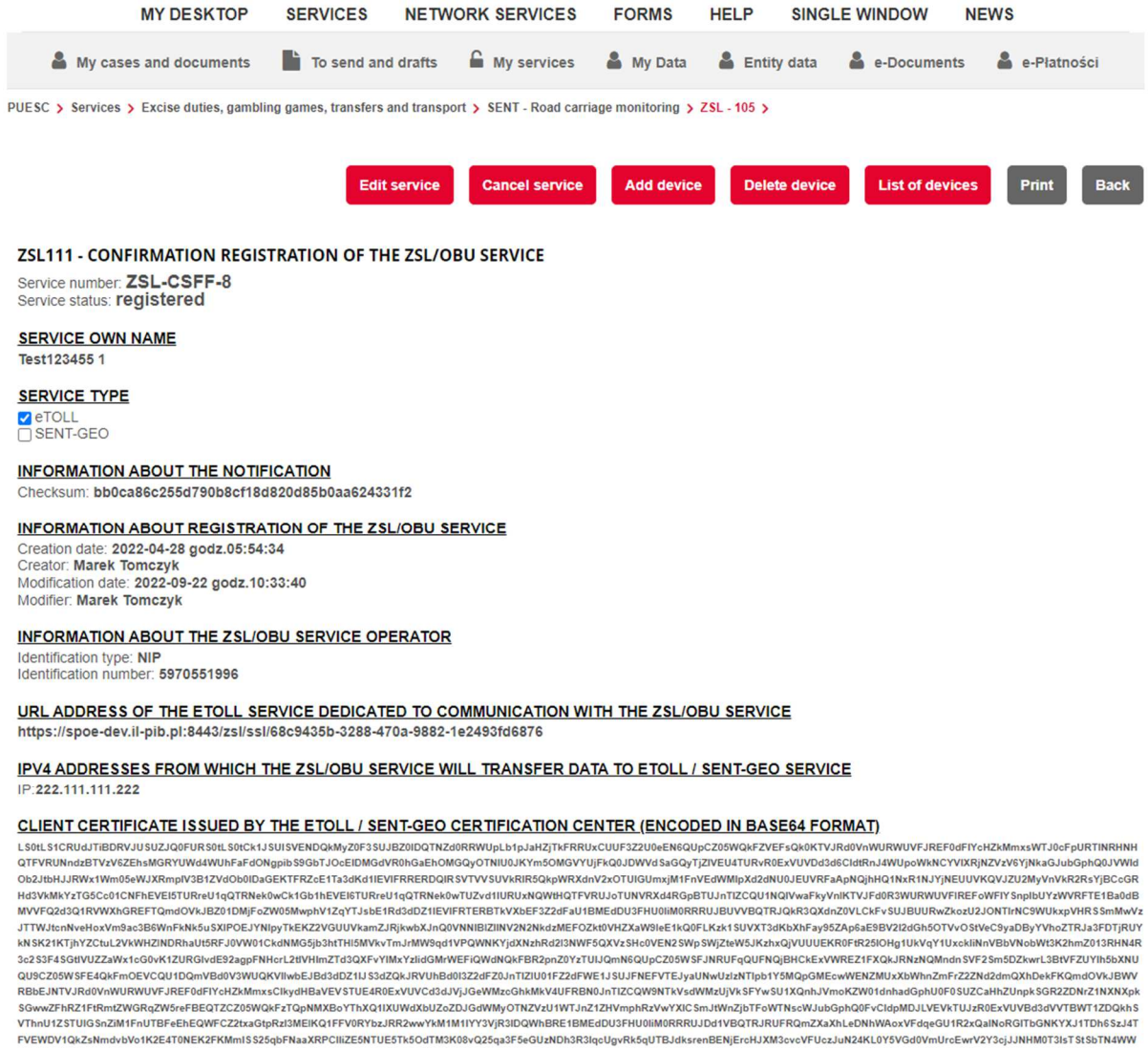
Крок 3
- виберіть поле " List of services "



Крок 4
- у графі «Akcja» виберіть іконку навпроти сервісу, який потрібно оновити (символ документа з лупою зеленого кольору)

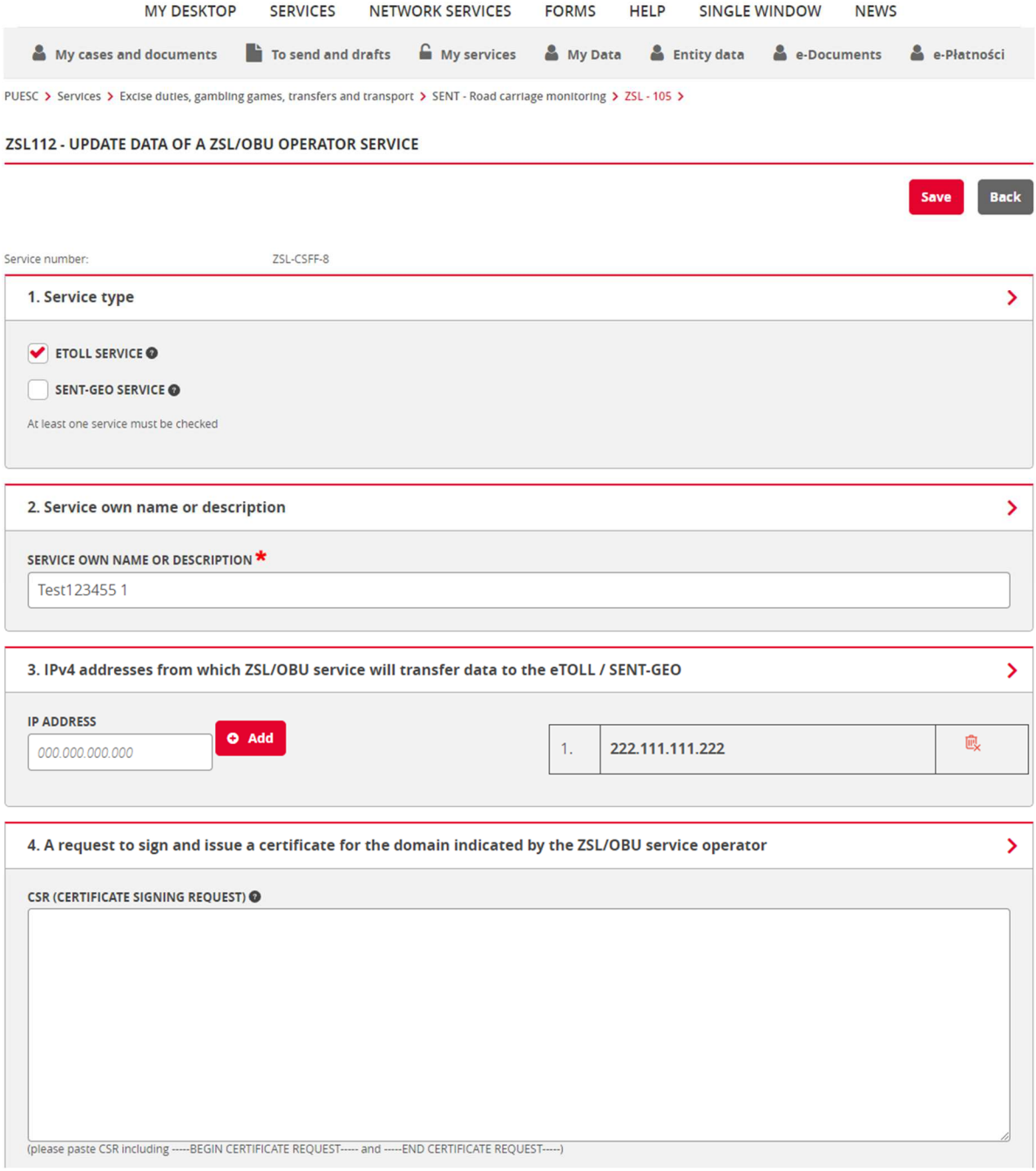


Крок 5
- виберіть кнопку «Edit service»

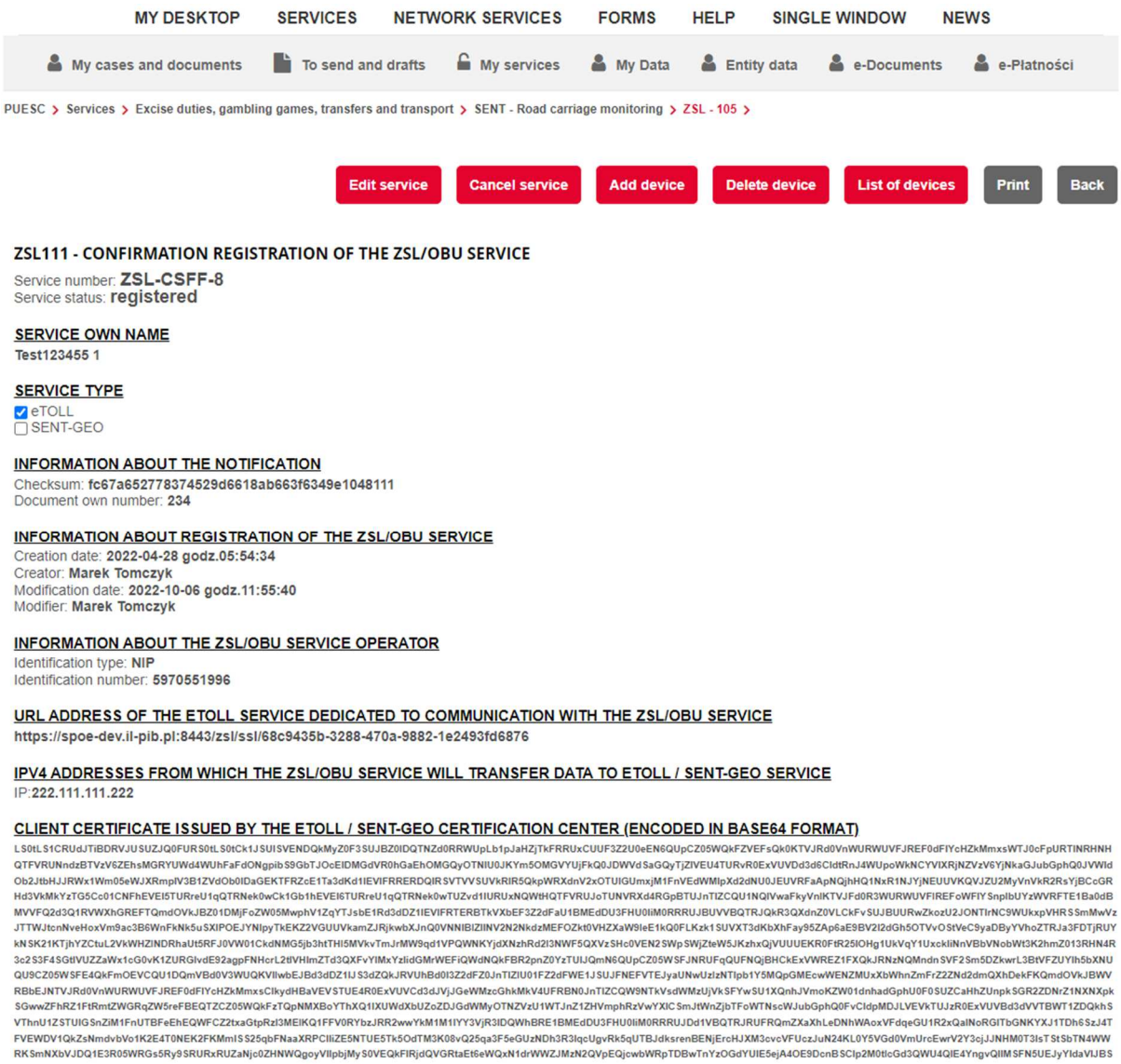


LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUISVENDQkMyZ0F3SUJBZ0IDQTNZd0RRWUpLb1pJaHZjTkFRRUxCUUF3Z2U0eEN6QUpCZ05WQkFZVEFsQk0KTVJRd0VnWURWUVFJREF0dFlYcHZkMmxsWTJ0cFpURTINRHNH
QTFVRUNndzBTVzV6ZEhsMGRYUWd4WUhFaFdONgpibS9GbTJOcElDMGdVR0hGaEhOMGQyOTNIU0JKYm5OMGVYUjFkQ0JDWVd5aGQyTjZlVEU4TURvR0ExVUVDd3d6CldtRnJ4WUpoWkNCYVlXRjNZVzV6YjNkaGJubGphQ0JVWld
Ob2JtbHJJRWx1Wm05eWJXRmpIV3B1ZVdOb0IDaGEKTFRZcE1Ta3dKd1lEVlFRRERDQIRSVTVVSUVkRlR5QkpWRXdnV2xOTUlGUmxjM1FnVEdWMlpXd2dNU0JEUVRFaApNQjhHQ1NxR1NJYjNEUUVKQVJZU2MyVnVkR2RsYjBCcGR
Hd3VkMkYzTG5Cc01CNFhEVEI5TURreU1qQTRNek0wCk1Gb1hEVEI6TURreU1qQTRNek0wTUZvd1IURUxNQWtHQTFVRUJoTUNVRXd4RGpBTUJnTlZCQU1NQlVwaFkyVnlKTVJFd0R3WURWUVFIREFoWFlYSnplbUYzWVRFTE1Ba0dB
MVVFQ2d3Q1RVWXhGREFTQmdOVkJBZ01DMjFoZW05MwphV1ZqYTJsbE1Rd3dDZ1FHU0liM0RRRUJBUVVBQTRJQkR3QXdnZ0VLCkFvSUJBUURwZkozU2JONTlrNC9WUkxpVHRSSmMwVz
JTTWJtcnNveHoxVm9ac3B6WnFkNk5uSXlPOEJYNlpyTkEKZ2VGUUVkamZJRjkwbXJnQ0VNNlBIZlINV2N2NkdzMEFOZkt0VHZXaW9leE1kQ0FLKzk1SUVXT3dKbXhFay95ZAp6aE9BV2l2dGh5OTVvOStVeC9yaDByYVhoZTRJa3FDTjRUY
kNSK21KTjhYZCtuL2VkWHZlNDRhaUt5RFJ0VW01CkdNMG5jb3htTHI5MVkvTmJrMW9qd1VPQWNKYjdXNzhRd2I3NWF5QXVzSHc0VEN2SWpSWjZteW5JKzhxQjVUUUEKR0Ft2SlVXT3dKbXhFay95ZAp6aE9BV2l2dGh5OTVvOStVeC9yaDByYVhoZTRJa3FDTjRUY
3c2S3F4SGtlVUZZaWx1cG0vK1ZURGlvdE92agpFNHcrL2tfVHlmZTd3QXFvYlMxYzlidGMrWEFiQWdNQkFBR2pnZ0YzTUlJQmN6QUpCZ05WSFJNRUFqQUFNQjBHCkExVWREZ1FXQkJRNzNQMndn SVF2Sm5DZkwrL3BtVFZUYlh5bXNU
QU9CZ05WSFE4QkFmOEVCQU1DQmVBd0V3WUQKVllwbEJBd3dDZ1lJS3dZQkJRVUhBd0l3Z2dFZ0JnTlZlU01FZ2dFWE1JSUJFNEFVTEJyaUNwUzlzNTlpb1Y5MQpGMEcwWENZMUxXbWhnZmFrZ2ZNd2dmQXhDekFKQmdOVkJBWV
RBbEJNTVJRd0VnWURWUVFJREF0dFlYcHZkMmxsClkydHBaVEVSTUE4R0ExVUVCd3dJVjJGeWMzcGhkMkV4UFRBN0JnTlZCQW9NTkVsdWMzUjVkSFYwSU1XQnhJVmoKZW01dnhadGphU0F0SUZCaHhZUnpkSGR2ZDNrZ1NXNXpk
SGwwZFhRZ1FtRmtZWGRqZW5reFBEQTZCZ05WQkFzTQpNMXBoYThXQ1lXUWdXbUZoZDJGdWMyOTNZVzU1WTJnZ1ZHVmphRzVwYXlCSmJtWnZjbTFoWTNscWJubGphQ0FvCldpMDJLVEVkTUJzR0ExVUVBd3dVVTBWT1ZDQkhS
VThnU1ZSTUlGSnZiM1FnUTBFeEhEQWFCZ2txaGtpRzl3MEIKQ1FFV0RYbzJRR2wwYkM1M1lYY3VjR3lDQWhBRE1BMEdDU3FHU0liM0RRRUJDd1VBQTRJRUFRQmZXaXhLeDNhWAoxVFdqeGU1R2xQalNoRGlTbGNKYXJ1TDh6SzJ4T
FVEWDV1QkZsNmdvbVo1K2E4T0NEK2FKMmlSS25qbFNaaXRPCliiZE5NTUE5Tk5OdTM3K08vQ25qa3F5eGUzNDh3R3lqcUgvRk5qUTBJdksrenBENjErcHJXM3cvcVFUczJuN24KL0Y5VGd0VmUrcEwrV2Y3cjJJNHM0T3IsTStSbTN4WW

Крок 6:
- у пункті 4 (*A request to sign and issue a certificate for the domain indicated by the ZSL/OBU services operator*) відображеного вигляду (*ZSL112 – UPDATE DATA OF A ZSL/OBU OPERATOR SERVICE*) вставте новий CSR (CERTIFICATE SIGNING REQUEST)
- виберіть кнопку „Save” на формі ZSL112



Крок 7
- отримання підтвердження про оновлення сервісу



ДОДАТКОВА ІНФОРМАЦІЯ

Користувач заповнює поля форми. У поле **A request to sign and issue a certificate for domain indicated by the ZSL/OBU service operator**, вставляється CSR (ang. Certificate Signing Request). CSR генерується з вашого закритого ключа. Для цього можна використовувати openssl (www.openssl.org). Якщо користувач уже має закритий ключ (наприклад, файл private.key), то в середовищі Linux команда має таку структуру:

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

Якщо у користувача немає закритого ключа, його можна згенерувати, наприклад:

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

(довжина 4096 біт забезпечує кращий рівень безпеки, ніж ключ 2048)

Приклад файлу, що містить закритий ключ, представлений на Рис. 4.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAua
SvEsSeMUYYdw4fC0WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB
lmKuux1XP0tCsHXgPJOezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMRlD4G3cPBD
dOOZqSmX7tHp97q+PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7
KGFjwEl+UxDgsNaSp7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VT2jyf
kW4k8gvltwueKScsc9/Ordlr6YopGg5xwQr+TQIDAQABAoIBAQDePSF9cqTf9X4I
TVqkl6cqkQQqSU5sokTQSidbkRQmKlS/JCrqQ5VZ6Ldz+I260DCYiiA2g1pdcy7a
zCz0lldhtHsWfVBI5HdTleu2iJO/8Ig2DGQOgC8chQbpQ8HQ1WqVIBaF+ha3W64d
VJlH7f4ctfxoGi8S5XH8Jtgq3JoLdeH9YqaNzQ2LKSx91/PxO6J7sLya82KKUBrp
M3AOumtEt0YRy57JkV7j1YeYUFLpWT7cR5rh2cZs5r1fQTGQjQorWBu/e4Po7PMn
Vbp/qDBqnifemd/dxDWydtXtJukp1mLdUSK15jAXApr2ZSXZ56espTnuIxkkvuzZ
mny15mItAoGBAP34wh8DZwvUeKIn408osSQzHEtMnefIMB0u0yoj94RQZuv8VwAR
eoTeFIEPOQqgdB7MSgkgZpNuyYxW+OrQI4mMl9Wh9DyHwnWTxNO7pDJEb6BCukQb
/+bdjLSytmDyVhkGMlMQlE017MdncrQRSURvByNRXbDzzoP7wlL2bASTAoGBAPGb
HIDDlxcHZkdOWNof2RDE+UbgaU86aI3dtGSsoTo6bmPkXxfe6PJPu8pLwzhVOafZ
EXH4qJ9CiOE4r6PelyA944KDwx8mlBsU7E6fEchJaR6xykW8u25Nr5P304szxCTI
987eJmQq+BGUUp7LgC/QlcpiR7yyP+h5CNNkAp2fAoGAEcSaiCLrzacSvX1+6KXX
Jsowm5ADqBiYTSJegZ88jNQ3LyFbUNToNml3D8Rp4DVzikgOke7jXkMs9JWNGphv
NAtTAA4xkR6KW0F4Trvc8+tXx+WDNIqk75jmZCnwmn25ykxlruwJflA97YFuQ+zF
rHT8Edt6a4vTEebGJJm62uMCgYA06NMFH9AmqugrFW0/11mh4oD01JB7WT8sUjD/
Gw7zwXgLSCfLAnXhGrT1SEIoRAGsUE0RuHK07c0sBU3xhP1zghoggqtpAKCKnC530
WcF7KxhqMGUrgHlLXpfkv5EEGwIJTDl4hA3EQeSxdNnjDI216ufiukMbf62fK2JT
aMNp4QKBgDxQkHSX8E7FhlUijf3C8IMZsZ7frzCbdIfNX6/PcVrcx3UKSVWmB9/v
auOMEHZmoo/FRZXdcZPI0wzcGb4oz4few2Dp2savew5QEGq4v3DZDEhGK5X7Yc+M
skL3MCgqGqVN1+fV4uFHzGqPpMKMXZHUKlpLTVWNvswe0SBfZ5U5
-----END RSA PRIVATE KEY-----
```

Рис. 4. Приклад файлу з закритим ключем

У свою чергу, приклад файлу, що містить CSR , показаний на Рис. 5.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1zCCAb8CAQAwgZExCzAJBgNVBAYTAlBMMRQwEgYDVQQIDAtNQVpPV01FQ0tJ
RTERMA8GA1UEBwwIV0FSU1pBV0ExDDAKBgNVBAoMA05JVDELMAkGA1UECwwCWjYx
FzAVBgNVBAMMDnd3dy5pdGwud2F3LnBsMSUwIwYJKoZIhvcNAQkBFhZlLmtsaW1h
c2FyYUBpdGwud2F3LnBsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAuaSvEsSeMUYYdw4fC0
WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB1mKuux1XP0tCsHXg
PJOezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMRlD4G3cPBDdOOZqSmX7tHp97q+
PbVbWwvUg6eISxsgQl6SZTbAoi1aG8HgIO+5i2RRdZOFj++7KGFjwEl+UxDgsNaS
p7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyfkW4k8gvltwueKScs
c9/Ordlr6YopGg5xwQr+TQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBADjODul1
Wqp2GJ/8nam/bjnh2WNSczQ0FjQ6IiK/+rhlBfOREky0J9cz+hRsZt5m9D8UVWkC
u4a/iJicrMZHPhTbC9tKuAk2c29ErxKJeSXr/anRKg9EbD7AB4RFmEjsJo/yRauL
oHetcTqxNPDBspkCmo2eRrKb2LdhCGFQRG4Wx/Gg6iuzd7zZKnOVKMuELpOP/vTz
Gu6QUDi2kpg/cr5A1rwq4d5uIEag1vi9G8YXNa/wkqOrNsuP660Wj8u9QgIWpWdV
ikYJShaHRHFxk3Qr//3P3lg0vgc4AuDcs/r4aOlET7dzuIt0qZymoQKPuOwXpfgY
gxjEmtwLRv5BgM8=
-----END CERTIFICATE REQUEST-----
```

Рис. 5. Приклад файлу, що містить CSR

Більш детальну інформацію можна знайти за адресою:
https://tech-itcore.pl/2012/07/04/generowanie-wlasnego-c certatu-ssl/
https://uk.godaddy.com/help/apache-generate-csr-certificate-signing-request-5269

У формі **повинна бути можливість** ввести адресу електронної пошти, на яку користувач отримає форму з відповіддю.

У формі відповіді Оператора ZSL, Оператор OBU отримує Сертифікат клієнта, закодований у форматі base64.
Його слід розшифрувати. **Не треба додавати до нього рядок BEGIN/END CERTIFICATE** , потрібно лише використати інструмент, який може декодувати текст, закодований у Base64, наприклад:

3. Notepad ++> Плагіни > Mime Tools> Base64 Decode

4. openssl base64 -d -in file_with_encrypted_certificate.txt -out certificate.pem

5. Сайт https://www.base64decode.org/

6. Certutil -decode file_with_encrypted_certificate.txt certificate.pem (для Windows за допомогою командного рядка).

Приклад сертифіката в base64 показаний на Рис. 6.

Рис. 6. Сертифікат, закодований за допомогою Base64

З іншого боку, приклад сертифіката, декодованого у форматі PEM (англ. Privacy-Enhaced Mail), показаний на Рис. 7.

Рис. 7. Приклад декодованого сертифіката

Після декодування ви отримуєте файл, що містить максимум три сертифікати у форматі PEM:

1. Сертифікат клієнта,
2. Сертифікат ЦА (Центр авторизації) (CA) рівня 1, який видав сертифікат клієнта,
3. Сертифікат ЦА (Центр авторизації) (CA) рівня 0, який видав сертифікат CA рівня 1.

Кожен сертифікат починається і закінчується рядками:
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
Рядки вище вказують на початок і кінець кожного сертифіката.
Обсяг і спосіб використання даних, які використовуються для захисту зв’язку TLS, змінюються та залежать від системи/програми, яку використовує суб’єкт. Однак типові вимоги до інструментів/компонентів SSL/TLS передбачають використання в автентифікації SSL наступного:

1. сертифікату клієнта;
2. закритого ключа - забезпечує можливість використання сертифіката клієнта лише суб'єктом, який є його адміністратором;
3. ланцюг сертифікації / ланцюжок сертифікатів (англ. certificate chain), який засвідчує сертифікат клієнта як сертифікат, виданий відповідним CA, і включає:
    1. Сертифікат CA (Центр авторизації) рівня 1, який видав сертифікат клієнта,
    2. Сертифікат CA (Центр авторизації) рівня 0, який видав сертифікат CA рівня 1,

У середовищі Linux підключення до SPOE KAS можна перевірити за допомогою інструменту curl. Послідовність команд показана нижче. Certificate.pem означає отриманий сертифікат, який був декодований з формату base64 у формат PEM. A fd1.key — це закритий ключ (розшифрований), який використовується для створення CSR.

curl -X POST --cert ./certificate.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, "": 15.17, "gpsHeading": 0.0} ", {" :" 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

Примітка 1: Адресу https://cloud.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001 слід замінити на адресу, отриману з форми, отриманої e-mail, йдеться про вміст поля **URL-адреса послуги e-TOLL, призначена для зв'язку зі службою Оператора ZSL або Оператора OBU**.

Примітка 2: Сертифікат клієнта X.509 SSL/TLS з боку Оператора ZSL або оператора OBU

Обов'язки оператора ZSL або оператора OBU включають:

1. отримання вищезазначеного сертифікату:
    а. першого - в результаті реєстрації послуги,
    б. кожного наступного протягом 365 днів з моменту видачі попереднього сертифіката;
2. використання поточного сертифіката клієнта X.509 SSL/TLS для автентифікації зв'язку з інтерфейсом даних SPOE KAS.

Перший клієнтський сертифікат X.509 SSL/TLS видається у відповідь на надсилання до SPOE KAS через спеціальний портал для запиту клієнтського сертифіката SSL/TLS X.509 за допомогою однієї з двох доступних форм зв'язку:

1. документу XML;
2. реєстраційної форми служби, заповнену на веб-сайті служби SPOE KAS на спеціальному порталі SPOE KAS.

Черговий сертифікат можна отримати, надіславши запит на сертифікат клієнта SSL/TLS X.509 до SPOE KAS через спеціальний портал за допомогою однієї з двох доступних форм зв'язку:

1. документу XML;
2. форми оновлення даних про послугу, заповнену на сайті e-TOLL у спеціальному порталі.

Клієнтський сертифікат X.509 SSL/TLS, який використовується для автентифікації Оператора ZSL або Оператора OBU під час зв'язку з інтерфейсом даних SPOE KAS, є першим із сертифікатів, які повертає SPOE KAS у відповідь на надсилання форми/документа XML. Кожен із повернених

сертифікатів починається з рядка "----- BEGIN CERTIFICATE -----" і закінчується рядком "----- END CERTIFICATE -----".

Термін дії сертифіката клієнта X.509 SSL/TLS можна переглянути за допомогою безкоштовного інструментарію OpenSSL за допомогою такої команди:

openssl x509 -inform PEM -enddate –noout –in file_with_client_certificate_x509.pem

де:

1. plik_z_certyfikatem_klienta_x509.pem - це приклад назви файлу, що містить клієнтський сертифікат SSL/TLS X.509, виданий SPOE KAS.

Приклад відповіді на вищезгадану команду наведено нижче:

notAfter=Sep 30 08:30:58 2020 GMT

де:

1. notAfter - мітка поля "не пізніше" сертифіката X.509, яка містить дату закінчення терміну дії сертифіката, після якої його не можна використовувати або йому довіряти;
2. Sep - трибуквена абревіатура назви місяця, в даному випадку це абревіатура September, тобто Вересень;
3. 30 - день;
4. 08:30:58 - година, хвилина і секунда;
5. 2020 рік;
6. GMT - трибуквена абревіатура назви часового поясу, позначення часового поясу, в даному випадку це абревіатура Greenwich Mean Time, що означає, що для отримання часу для європейського/варшавського часового поясу додайте 2 години до заданого часу у випадку літнього часу та одну годину у разі зимового часу.

Примітка 3: Конфігурація "mutual TLS"
У випадку взаємної конфігурації TLS слід зазначити, що зміна сертифіката сервера завадить правильній автентифікації зв’язку. Інформація про зміну сертифіката сервера буде пропагувана Операторам, а при виникненні проблем з перевіркою сертифіката сервера ви можете скористатися командами для перегляду сертифіката, а саме:

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 | більше