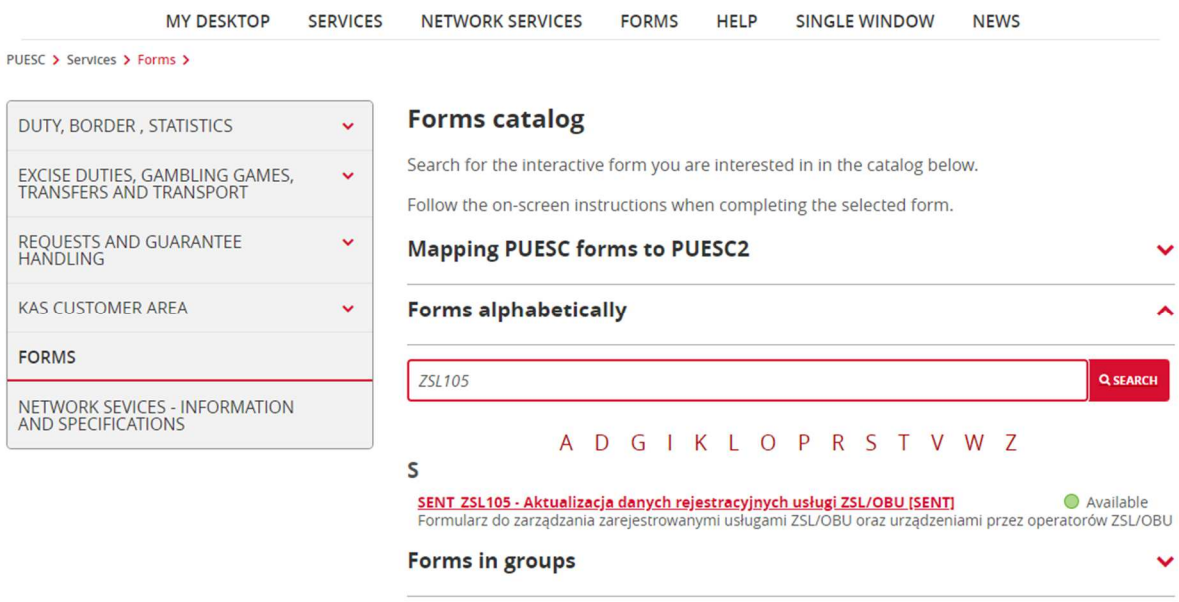
ИНСТРУКЦИЯ для операторов OBU/ZSL по обновлению SSL-сертификата

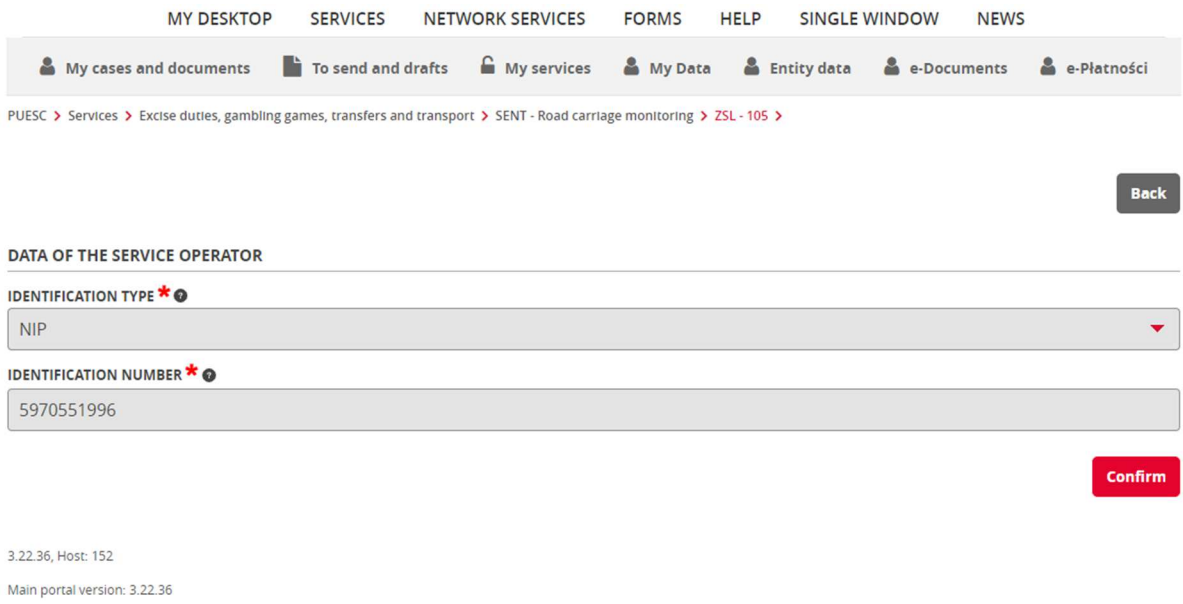
Актуальность SSL-сертификата действительна в течение 1 года, считая со дня его выдачи, и является одним из условий правильного функционирования связи ИКТ-инфраструктуры оператора с системой e-TOLL. SSL-сертификат - это сетевой протокол, используемый для безопасных Интернет-соединений с точки зрения шифрования 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*)

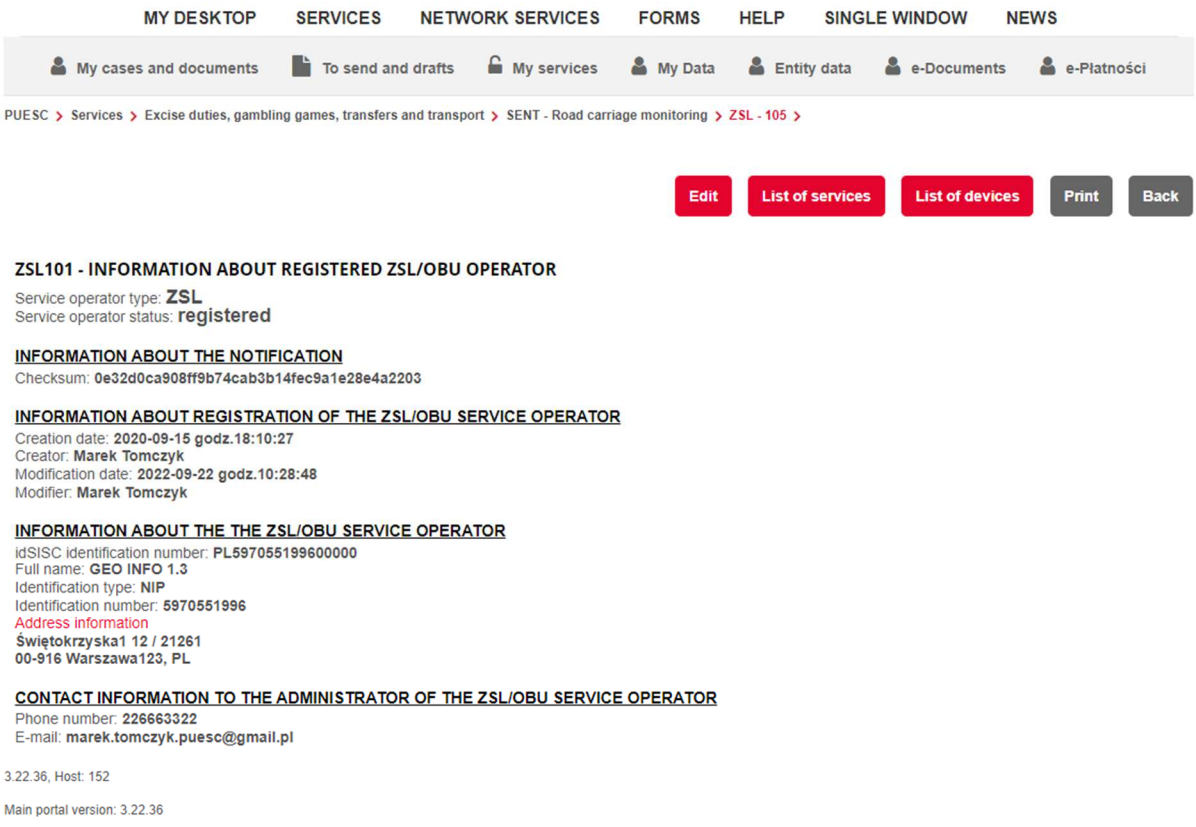
Шаг 1
- перейдите на страницу https://puesc.gov.pl
- войдите в учетную запись в поле компании
- выберите в меню вкладку „Forms”
- разверните панель „Forms alphabetically” и введите „ZSL105”
- откройте поисковую ссылку



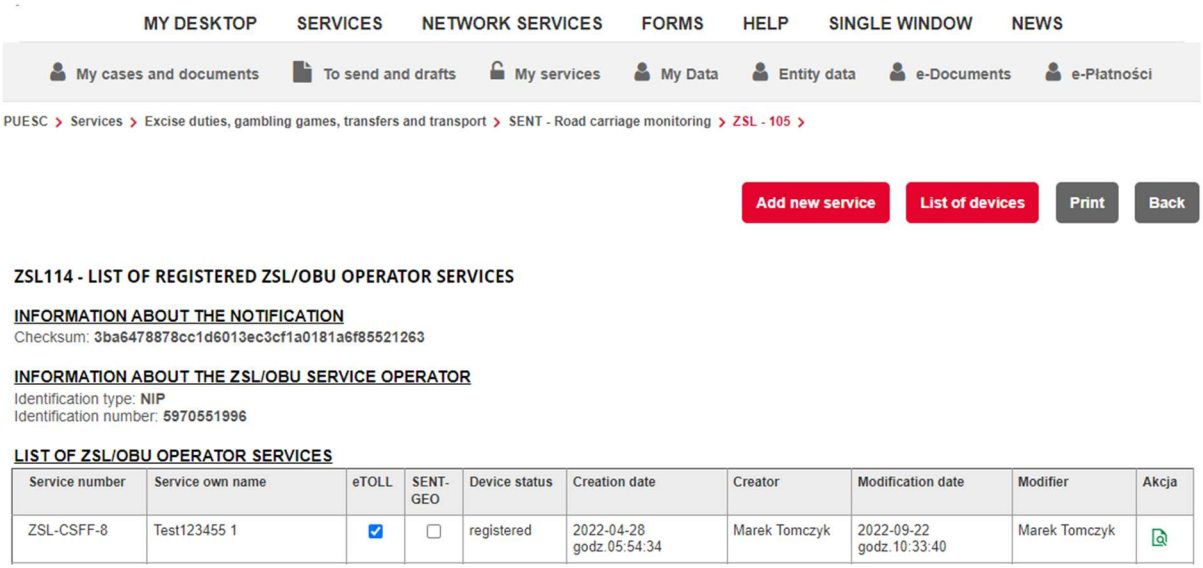
Шаг 2
- подтвердите отображаемый NIP компании



Шаг 3
- выберите поле „List of services”

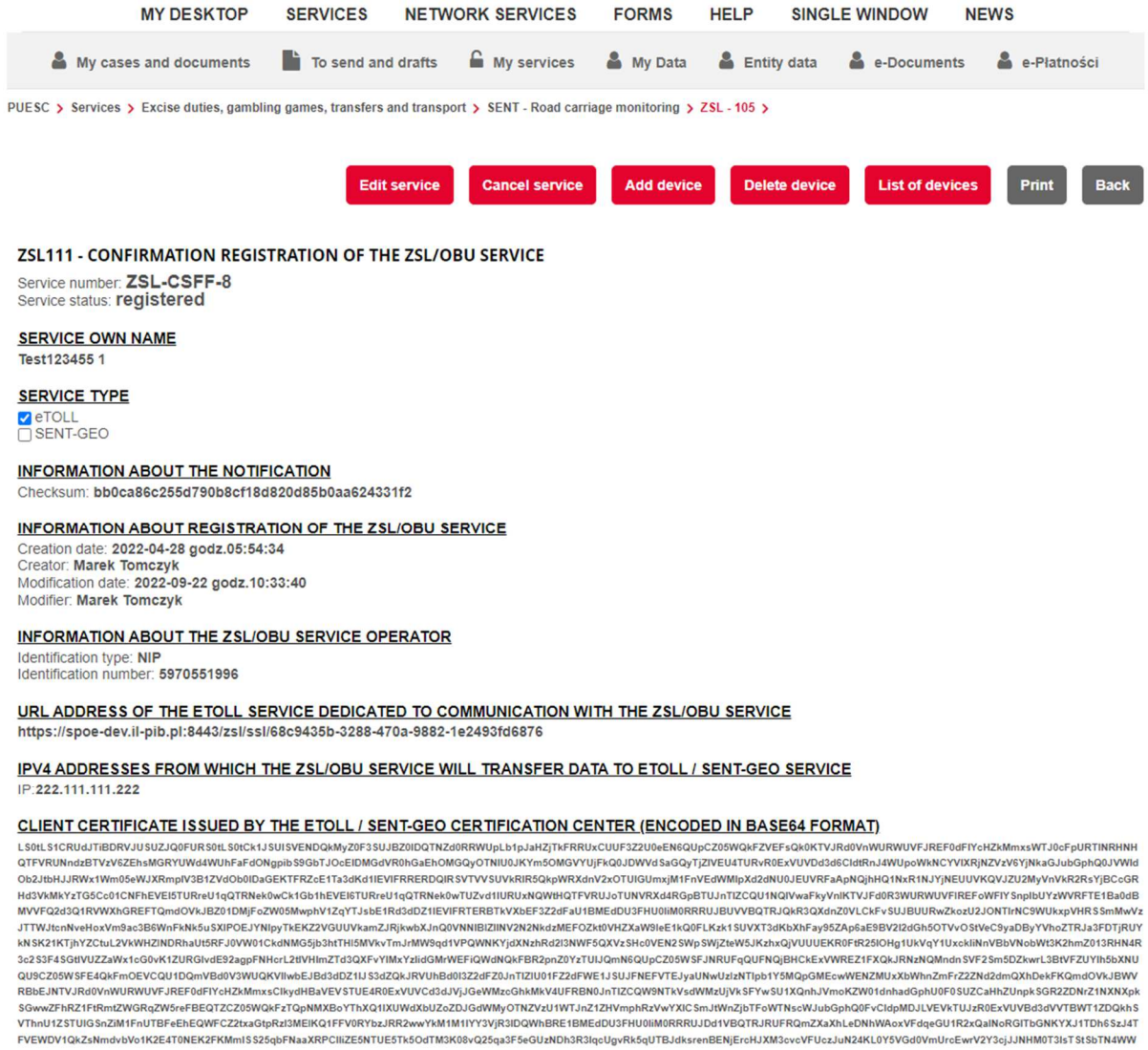


Шаг 4
- в столбце „Akcja” выберите значок рядом с услугой, которую вы хотите обновить (символ документа с лупой зеленого цвета)



Шаг 5

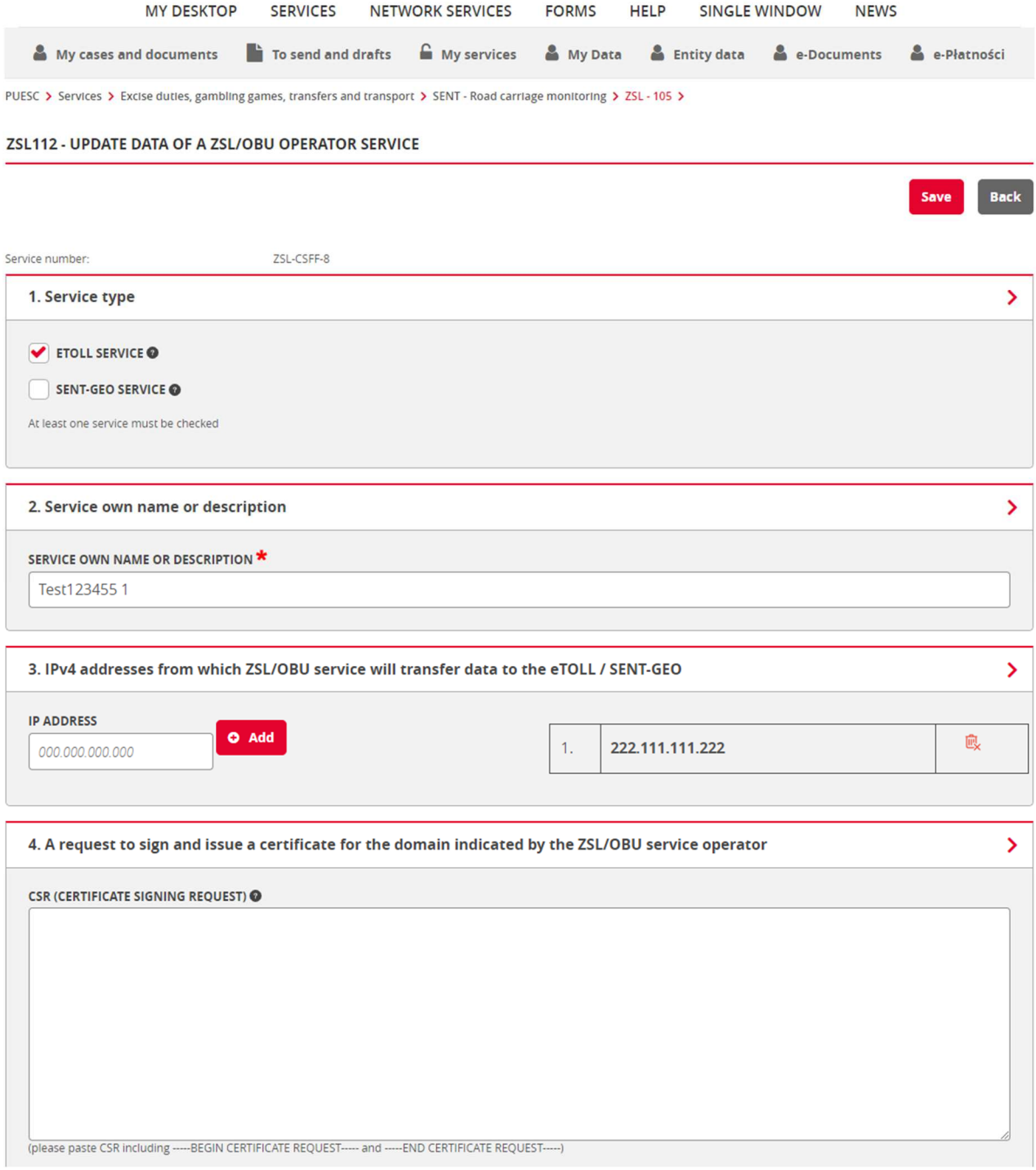
- выберите кнопку „Edit service”



LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUISVENDQkMyZ0F3SUJBZ0IDQTNZd0RRWUpLb1pJaHZjTkFRRUxCUUF3Z2U0eEN6QUpCZ05WQkFZVEFsQk0KTVJRd0VnWURWUVFJREF0dFlYcHZkMmxsWTJ0cFpURTINRHNH
QTFVRUNndzBTVzV6ZEhsMGRYUWd4WUhFaFdONgpibS9GbTJOcElDMGdVR0hGaEhOMGQyOTNIU0JKYm5OMGVYUjFkQ0JDWVd5aGQyTjZlVEU4TURvR0ExVUVDd3d6ClJdtRnJ4WUpoWkNCYVlXRjNZVzV6YjNkaGJubGphQ0JVWld
Ob2JtbHJJRWx1Wm05eWJXRmpIV3B1ZVdOb0IDaGEKTFRZcE1Ta3dKd1lEVlFRRERDQIRSVTVVSUVkRlR5QkpWRXdnV2xOTUlGUmxjM1FnVEdWMlpXd2dNU0JEUVRFaApNQjhHQ1NxR1NJYjNEUUVKQVJZU2MyVnVkR2RsYjBCcGR
Hd3VkMkYzTG5Cc01CNFhEVEI5TURreU1qQTRNek0wCk1Gb1hEVEI6TURreU1qQTRNek0wTUZvd1IURUxNQWtHQTFVRUJoTUNVRXd4RGpBTUJnTlZCQU1NQlVwaFkyVnlKTVJFd0R3WURWUVFIREFoWFlYSnplbUYzWVRFTE1Ba0dB
MVVFQ2d3Q1RVWXhGREFTQmdOVkJBZ01DMjFoZW05MwphV1ZqYTJsbE1Rd3dDZ1FHU0liM0RRRUJBUVVBQTRJQkR3QXdnZ0VLCkFvSUJBUURwZkozU2JONTlrNC9WUkxpVHRSSmMwVz
JTTWJtcnNveHoxVm9ac3B6WnFkNk5uSXlPOEJYNlpyTkEKZ2VGUUVkamZJRjkwbXJnQ0VNNlBIZlINV2N2NkdzMEFOZkt0VHZXaW9leE1kQ0FLKzk1SUVXT3dKbXhFay95ZAp6aE9BV2I2dGh5OTVvOStVeC9yaDByYVhoZTRJa3FDTjRUY
kNSK21KTjhYZCtuL2VkWHZlNDRhaUt5RFJ0VW01CkdNMG5jb3htTHI5MVkvTmJrMW9qd1VPQWNKYjdXNzhRd2I3NWF5QXVzSHc0VEN2SWpSWjZteW5JKzhxQjVUUUEKR0Ft2SlVXT1UxckliNnVBbVNobWt3K2hmZ013RHN4R
3c2S3F4SGtlVUZZaWx1cG0vK1ZURGlvdE92agpFNHcrL2tfVHlmZTd3QXFvYlMxYzlidGMrWEFiQWdNQkFBR2pnZ0YzTUlJQmN6QUpCZ05WSFJNRUFqQUFNQjBHCkExVWREZ1FXQkJRNzNQMndn SVF2Sm5DZkwrL3BtVFZUYlh5bXNU
QU9CZ05WSFE4QkFmOEVCQU1DQmVBd0V3WUQKVllwbEJBd3dDZ1IJS3dZQkJRVUhBd0l3Z2dFZ0JnTlZlU01FZ2dFWE1JSUJFNEFVTEJyaUNwUzlzNTlpb1Y5MQpGMEcwWENZMUxXbWhnZmFrZ2ZNd2dmQXhDekFKQmdOVkJBWV
RBbEJNTVJRd0VnWURWUVFJREF0dFlYcHZkMmxsClkydHBaVEVSTUE4R0ExVUVCd3dJVjJGeWMzcGhkMkV4UFRBN0JnTlZCQW9NTkVsdWMzUjVkSFYwSU1XQnhJVmoKZW01dnhadGphU0F0SUZCaHhZUnpkSGR2ZDNrZ1NXNXpk
SGwwZFhRZ1FtRmtZWGRqZW5reFBEQTZCZ05WQkFzTQpNMXBoYThXQ1lXUWdXbUZoZDJGdWMyOTNZVzU1WTJnZ1ZHVmphRzVwYXlCSmJtWnZjbTFoWTNscWJubGphQ0FvCldpMDJLVEVkTUJzR0ExVUVBd3dVVTBWT1ZDQkhS
VThnU1ZSTUlGSnZiM1FnUTBFeEhEQWFCZ2txaGtpRzl3MEIKQ1FFV0RYbzJRR2wwYkM1M1lYY3VjR3lDQWhBRE1BMEdDU3FHU0liM0RRRUJDd1VBQTRJRUFRQmZXaXhLeDNhWAoxVFdqeGU1R2xQalNoRGlTbGNKYXJ1TDh6SzJ4T
FVEWDV1QkZsNmdvbVo1K2E4T0NEK2FKMmlSS25qbFNaaXRPCliiZE5NTUE5Tk5OdTM3K08vQ25qa3F5eGUzNDh3R3lqcUgvRk5qUTBJdksrenBENjErcHJXM3cvcVFUczJuN24KL0Y5VGd0VmUrcEwrV2Y3cjJJNHM0T3IsTStSbTN4WW

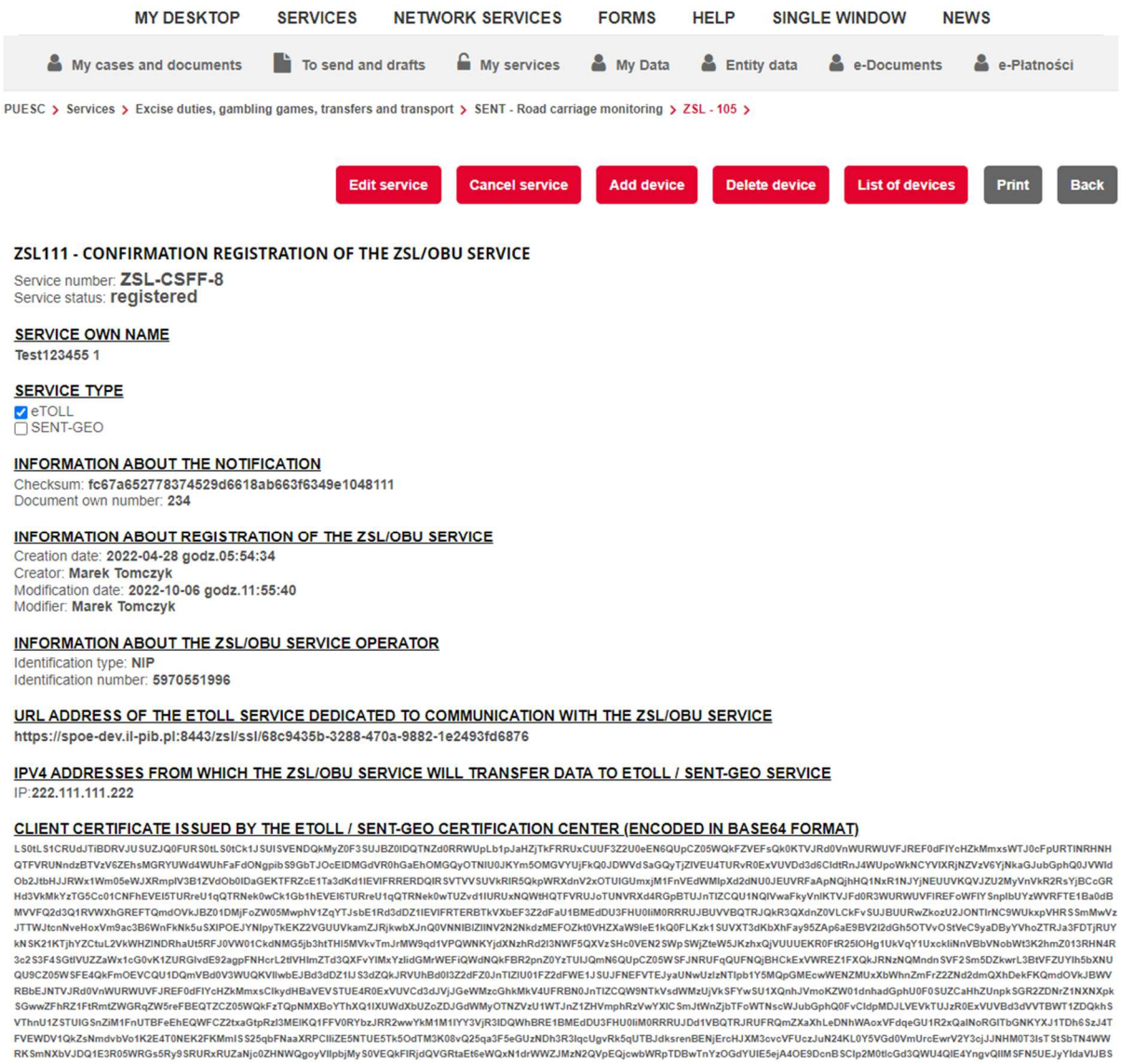
Шаг 6

- 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



Шаг 7

- получение подтверждения обновления услуги



LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUISVENDQkMyZ0F3SUJBZ0IDQTNZd0RRWUpLb1pJaHZjTkFRRUxCUUF3Z2U0eEN6QUpCZ05WQkFZVEFsQk0KTVJRd0VnWURWUVFJREF0dFIYcHZkMmxsWTJ0cFpURTINRHNH
QTFVRUNndzBTVzV6ZEhsMGRYUWd4WUhFaFdONgpib S9GbTJOcElDMGdVR0hGaEhOMGQyOTNlU0JKYm5OMGVYUjFkQ0JDWVdSaGQyTjZlVEU4TURvR0ExVUDd3d6CldtRnJ4WUpoWkNCYVlXRjNZVzV6YjNkaGJubGphQ0JVWld
Ob2JtbHJJRWx1Wm05eWJXRmpIV3B1ZVdOb0lDaGEKTFRZcE1Ta3dKd1IEVlFRRERDQlRSVTVVSUVkRlR5QkpWRXdnV2xOTUlGUmxjM1FnVEdWMlpXd2dNU0JEUVRFaApNQjhHQ1NxR1NJYjNEUUVKQVJZU2MyVnVkR2RsYjBCcGR
Hd3VkMkYzTG5Cc01CNFhEVEI5TURreU1qQTRNek0wCk1Gb1hEVEI6TURreU1qQTRNek0wTUZvd1IURUxNQWtHQTFVRUJoTUNVRXd4RGpBTUJnTlZCQU1NQlVwaFkyVnlKTVJFd0R3WURWUVFIREFoWFIYSnplbUYzWVRFTE1Ba0dB
MVVFQ2d3Q1RVWXhGREFTQmdOVkJBZ01DMjFoZW05MwphV1ZqYTJsbE1Rd3dDZ1IEVIFRTERBTkVXbEF3Z2dFaU1BMEdDU3FHU0lIM0RRRUJBUVVBQTRJQkR3QXdnZ0VLCkFvSUJBUURwZkozU2JONTlrNC9WUkxpVHRSSmMwVz
JTTWJtcnNveHoxVm9ac3B6WnFkNk5uSXlPOEJYNlpyTkEKZ2VGUUVkamZJRjkwbXJnQ0VNNIBlZIINV2N2NkdzMEFOZkt0VHZXaW9leE1kQ0FLKzk1SUVXT3dKbXhFay95ZAp6aE9BV2l2dGh5OTVvOStVeC9yaDByYVhoZTRJa3FDTjRUY
kNSK21KTjhYZCtuL2VkWHZlNDRhaUt5RFJ0VW01CkdNMG5jb3htTHI5MVkvTmJrMW9qd1VPQWNKYjdXNzhRd2I3NWF5QXVzSHc0VEN2SWpSWjZteW5JKzhxQjVUUUEKR0FtR25lOHg1UkYyY1UxckliNnVBbVNobWt3K2hmZ013RHN4R
3c2S3F4SGtlVUZZaWx1cG0vK1ZURGlvdE92agpFNHcrL2tlVHlmZTd3QXFvYlMxYzlidGMrWEFiQWdNQkFBR2pnZ0YzTUlJQmN6QUpCZ05WSFJNRUFqQUFNQjBHCkExVWREZ1FXQkJRNzNQMndnSVF2Sm5DZkwrL3BtVFZUYlh5bXNU
QU9CZ05WSFE4QkFmOEVCQU1DQmVBd0V3WUQKVlIwbEJBd3dDZ1IJS3dZQkJRVUhBd0l3Z2dFZ0JnTlZlU01FZ2dFWE1JSUJFNEFVTEJyaUNwUzlzNTlpb1Y5MQpGMEcwWENZMUxXbWhnZmFrZ2ZNd2dmQXhDekFKQmdOVkJBVV
RBbEJNTVJRd0VnWURWUVFJREF0dFIYcHZkMmxsCIkydHBaVEVSTUE4R0ExVUVCd3dJVjJGeWMzcGhkMkV4UFRBN0JnTlZCQW9NTkVsdWMzUjVkSFYwSU1XQnhJVmoKZW01dnhadGphU0F0SUZCaHhZUnpkSGR2ZDNrZ1NXNXpk
SGwwZFhRZ1FtRmtZWGRqZW5reFBEQTZCZ05WQkFzTQpNMXBoYThXQ1IXUWdXbUZoZDJGdWMyOTNZVzU1WTJnZ1ZHVmphRzVwYXlC SmJtWnZjbTFoWTNscWJubGphQ0FvCldpMDJLVEVkTUJzR0ExVUVBd3dVVTBWT1ZDQkhS
VThnU1ZSTUlGSnZiM1FnUTBFeEhEQWFCZ2txaGtpRzl3MEIKQ1FFV0RYbzJRR2wwYkM1M1IYY3VjR3lDQWhBRE1BMEdDU3FHU0liM0RRRUJDd1VBQTRJRUFRQmZXaXhLeDNhWAoxVFdqeGU1R2xQalNoRGlTbGNKYXJ1TDh6SzJ4T
FVEWDV1QkZsNmdvbVo1K2E4T0NEK2FKMmlSS25qbFNaaXRPCIliZE5NTUE5Tk5OdTM3K08vQ25qa3F5eGUzNDh3R3lqcUgvRk5qUTBJdksrenBENjErcHJXM3cvcVFUczJuN24KL0Y5VGd0VmUrcEwrV2Y3cjJJNHM0T3IsTStSbTN4WW
RKSmNXbVJDQ1E3R05WRGs5Ry9SRURxRUZaNjc0ZHNWQgoyVIlpbjMyS0VEQkFIRjdQVGRtaEt6eWQxN1drWWZJMzN2QVpEQjcwbWRpTDBwTnYzOGdYUlE5ejA4OE9DcnBSClp2M0tlcGd3QWU4QlE4YngvQlIMSFN5UEJyYldaV1JBS

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.

Рис. 4. Пример файла с закрытым ключом

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

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 certyfikat.pem

5. Страница https://www.base64decode.org/

6. Certutil -decode файл_с_закодированным_сертификатом.txt certyfikat.pem (для Windows с помощью командной строки).

Пример сертификата в base64 показан на Рис. 6.

Рис. 6. Сертификат, закодированный в Base64

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

Рис. 7. Пример декодированного сертификата

После декодирования вы получаете файл, содержащий максимум три сертификата в формате PEM:

1. Сертификат клиента,
2. Сертификат CA (Centrum Autoryzacji) уровня 1, выдавший сертификат клиента,
3. Сертификат CA (Centrum Autoryzacji) уровня 0, выдавший сертификат CA уровня 1.

Каждый сертификат начинается и заканчивается строками:
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
Приведенные выше строки обозначают начало и конец отдельных сертификатов.
Объем и использование данных, которые используются для защиты связи TLS, различаются и зависят от системы / приложения, используемого субъектом. Тем не менее, общие требования

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.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001

Примечание 1: Адрес https://cloud.spoe-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 просмотреть, 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 сделает 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