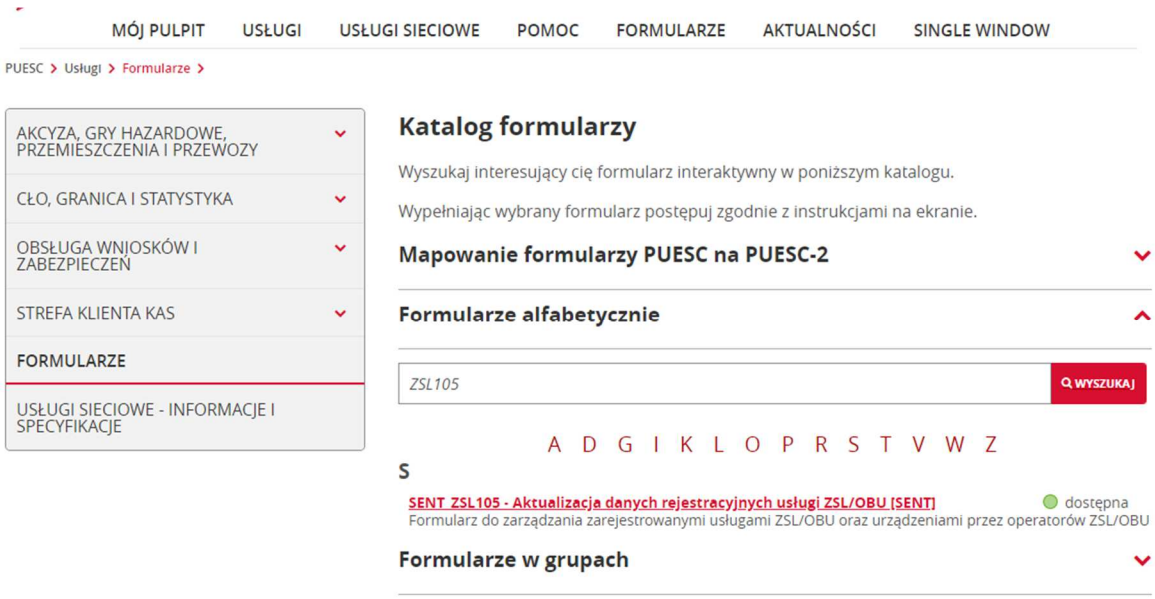
INSTRUKCJA dla Operatorów OBU/ZSL w zakresie aktualizacji certyfikatu SSL

Aktualność certyfikatu SSL ważna jest przez 1 rok licząc od dnia jego wystawienia i jest jednym z warunków prawidłowego funkcjonowania komunikacji infrastruktury teleinformatycznej operatora z systemem e-TOLL. Certyfikat SSL jest protokołem sieciowym używanym do bezpiecznych połączeń internetowych w zakresie szyfrowania na stronach WWW, chroniącym transakcje i zabezpieczającym przesyłane przez pocztę i stronę WWW informacje takie jak hasła, loginy, dane osobowe, itp.
Brak zaktualizowanego przez operatora OBU/ZSL certyfikatu SSL naraża użytkowników systemu e-TOLL na brak możliwości korzystania z funkcjonalności systemu, w tym dotyczącej przekazywania danych geolokalizacyjnych do celów naliczenia należnej opłaty.

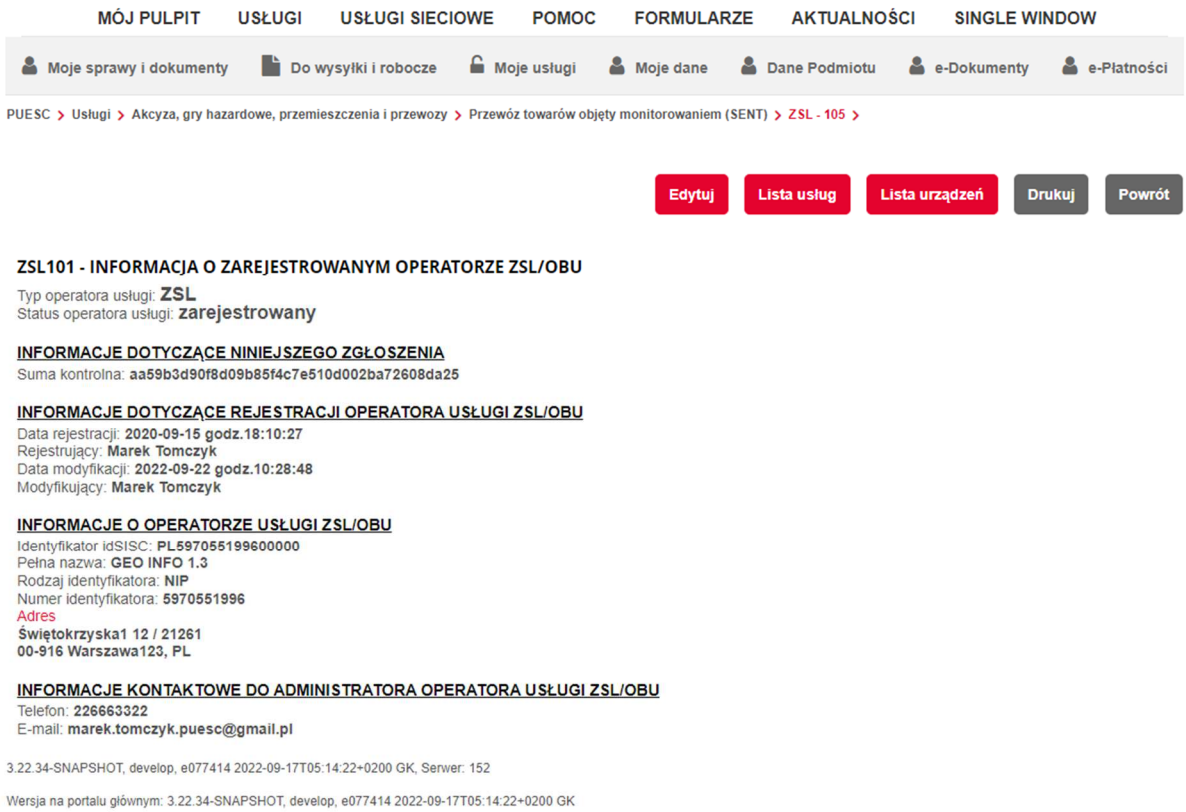
(*przykład*)

Krok 1
- wejdź na stronę https://puesc.gov.pl
- zaloguj się na konto w kontekście firmowym
- wybierz w menu zakładkę „Formularze”
- rozwiń pasek „Formularze alfabetycznie” i wpisz „ZSL105”
- otwórz w wyszukany link

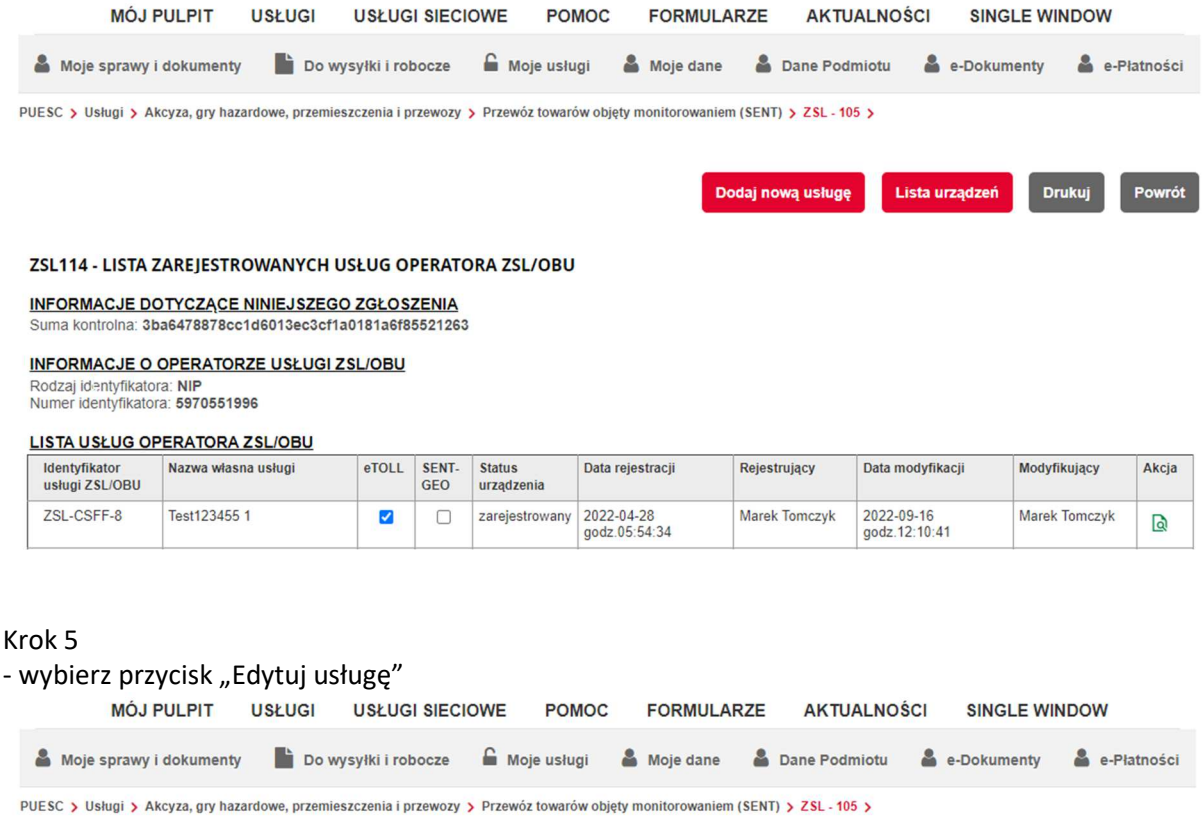


Krok 2
- zatwierdź wyświetlony NIP firmy

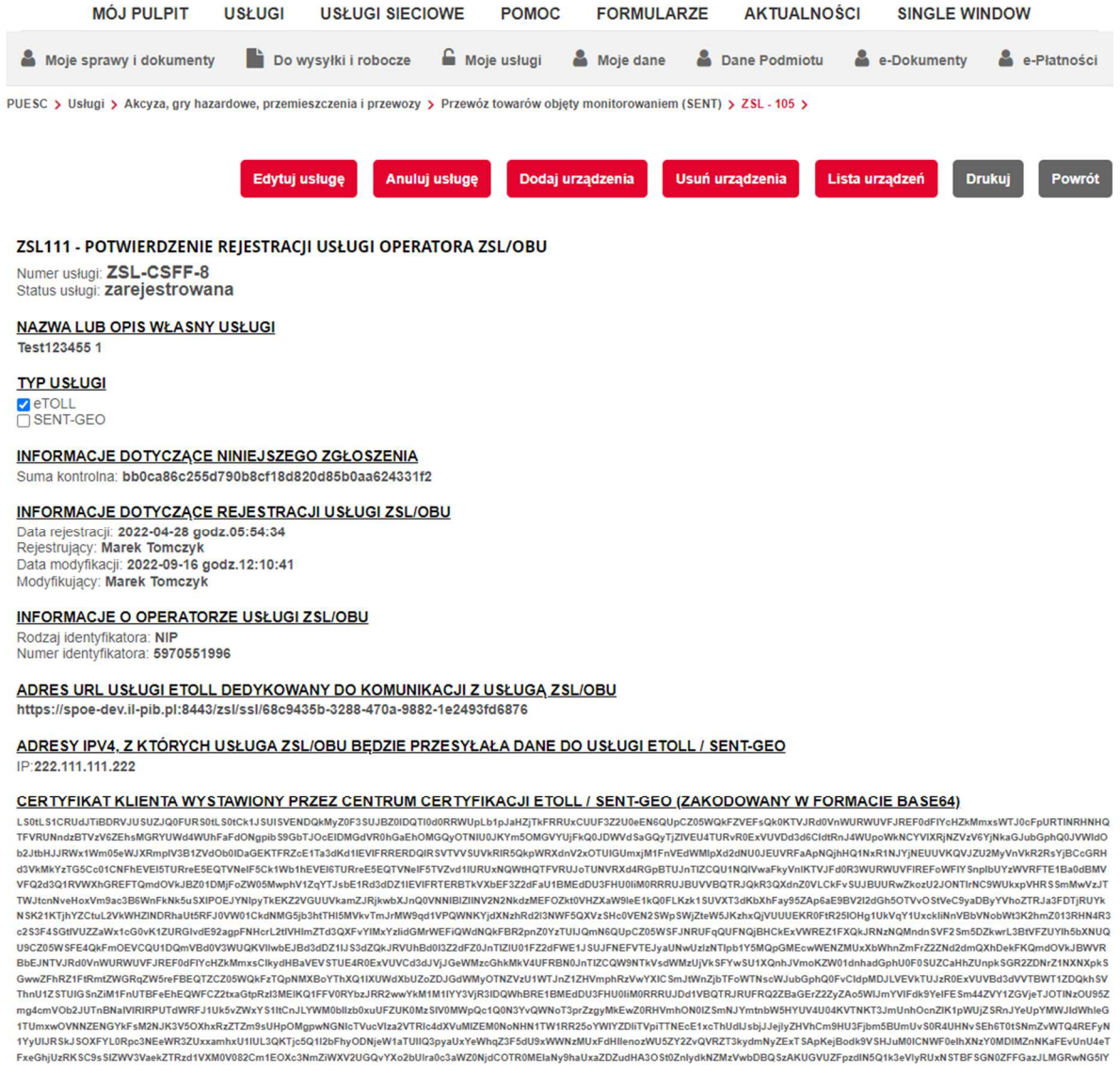
Krok 3
- wybierz pole „Lista usług”



Krok 4
- w kolumnie „Akcja” wybierz ikonę przy usłudze, którą chcesz zaktualizować (symbol dokumentu z lupą w kolorze zielonym)

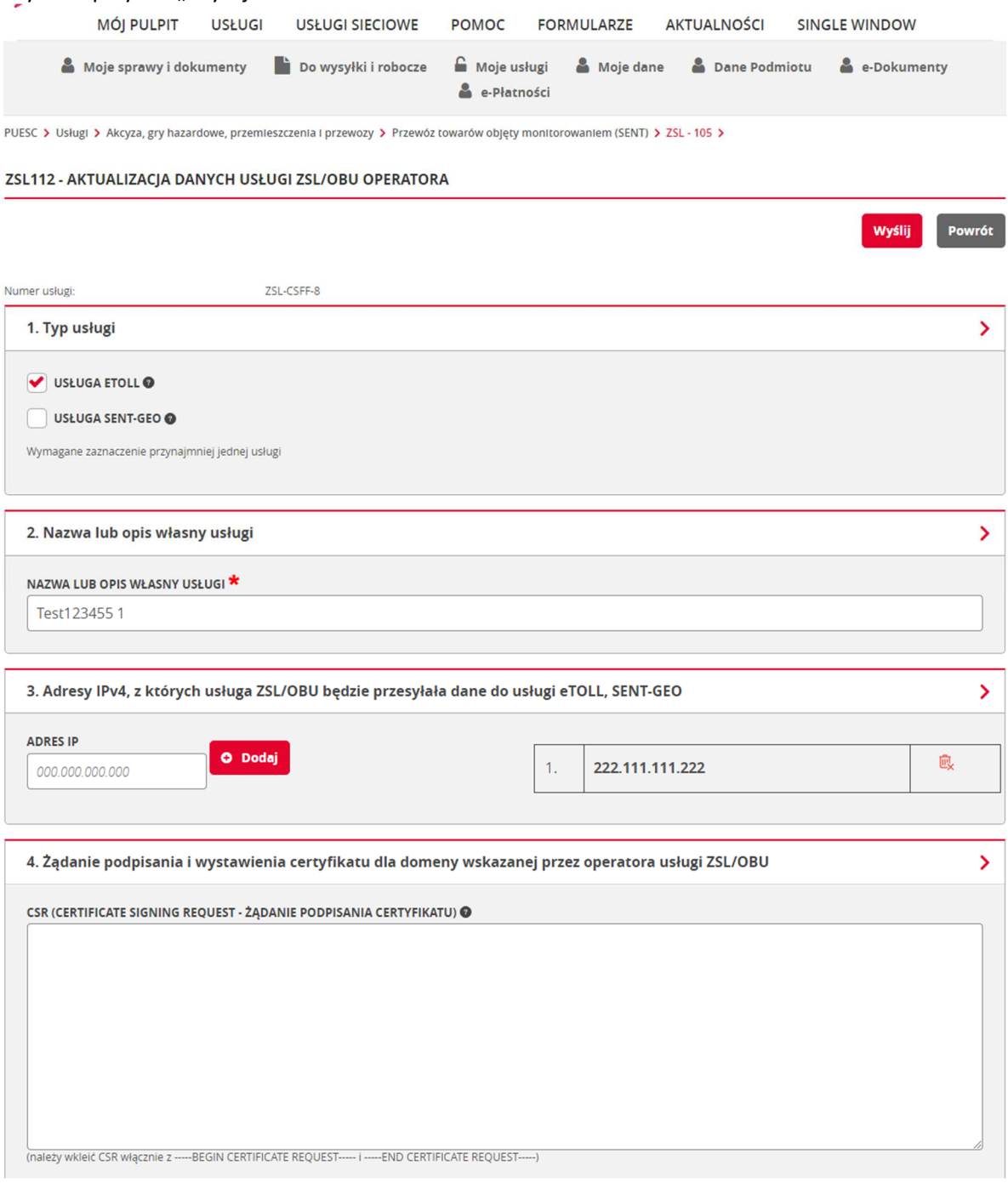


Krok 5
- wybierz przycisk „Edytuj usługę”

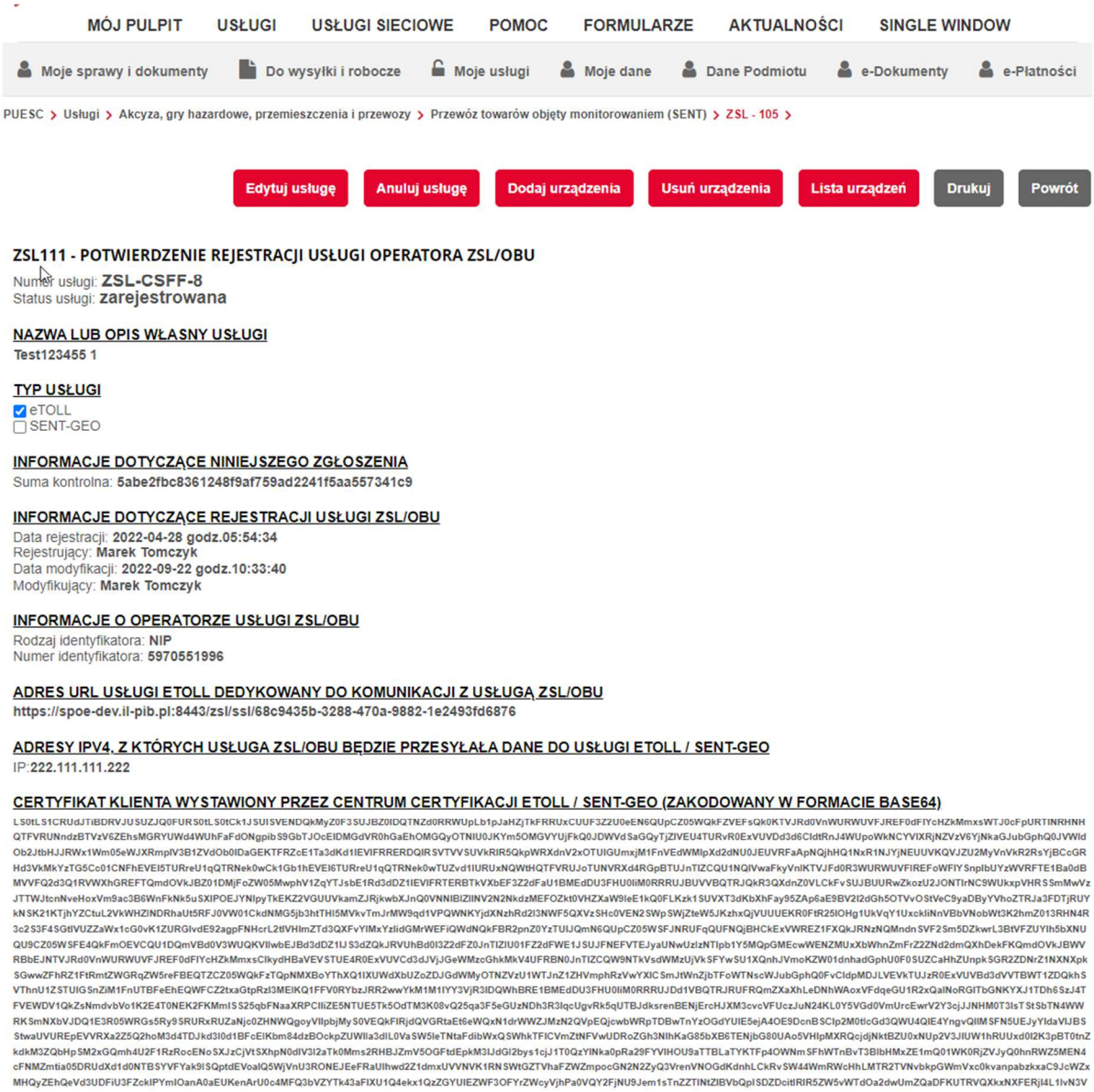


LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUISVENDQkMyZ0F3SUJBZ0IDQTI0d0RRWUpLb1pJaHZjTkFRRUxCUUF3Z2U0eEN6QUpCZ05WQkFZVEFsQk0KTVJRd0VnWURWUVFJREF0dFlYcHZkMmxsWTJ0cFpURTlNRHNHQ
TFVRUNndzBTVzV6ZEhsMGRYUWd4WUhFaFdONgpib S9GbTJOcEIDMGdVR0hGaEhOMGQyOTNIU0JKYm5OMGVYUjFkQ0JDWVdSaGQyTjZlVEU4TURVR0ExVUVDd3d6ClJdtRnJ4WUpoWkNCYVlXRjNZVzV6YjNkaGJubGphQ0JVWldO
b2JtbHJJRWx1Wm05eWJXRmpIV3B1ZVdOb0IDaGEKTFRZcE1Ta3dKd1IEVlFRERDQlRSVTVVSUVkRlR5QkpWRXdnV2xOTUlGUmxjM1FnVEdWMlpXd2dNU0JEUVRFaApNQjhHQ1NxR1NJYjNEUUVKQVJZU2MyVnVkR2RsYjBCcGRH
d3VkMkYzTG5Cc01CNFhEVEI5TURReE5EQTVNelF5Ck1Wb1hEVEI6TURreE5EQTVNelF5TVZvd1IURUxNQWtHQTFVRUJoTUNVRXd4RGpBTUJnTlZCQU1NQlVwaFkyVnlKTVJFd0R3WURWUVFIREFoWFlY SnplbUYzWVRFTE1Ba0dBMV
VFQ2d3Q1RVWXhGREFTQmdOVkJBZ01DMjFoZW05MwphV1ZqYTJsbE1Rd3dDZ1IEVlFRTERBTkVXbEF3Z2dFaU1BMEdDU3FHU0liM0RRRUJBUVVBQTRJQkR3QXdnZ0VLCkFvSUJBUURwZkozU2JONTlrNC9WUkxpVHRSSmMwVzJT
TWJtcnNveHoxVm9ac3B6WnFkNk5uSXlPOEJYNlpyTkEKZ2VGUUVkamZJRjkwbXJnQ0VNNIBlZIINV2N2NkdzMEFOZkt0VHZXaW9leE1kQ0FLKzk1SUVXT3dKbXhFay95ZAp6aE9BV2l2dGh5OTVvOStVeC9yaDByYVhoZTRJa3FDTjRUYk
NSK21KTjhYZCtuL2VkWHZlNDRhaUt5RFJ0VW01CkdNMG5jb3htTHI5MVkvTmJrMW9qd1VPQWNKYjdXNzhRd2l3NWF5QXVzSHc0VEN2SWpSWjZteW5JKzhxQjVUUEKR0FtR25lOHg1UkVqY1UxckliNnVBbVNobWt3K2hmZ013RHN4R3
c2S3F4SGtlVUZZaWx1cG0vK1ZURGlvdE92aggpFNHcrL2tlVHlmZTd3QXFvYlMxYzlidGMrWEFiQWdNQkFBR2pnZ0YzTUlJQmN6QUpCZ05WSFJNRUFqQUFNQjBHCkExVWREZ1FXQkJRNzNQMndnSVF2Sm5DZkwrL3BtVFZUYlh5bXNUQ
U9CZ05WSFE4QkFmOEVCQU1DQmVBd0V3WUQKVllwbEJBd3dDZ1lJS3dZQkJRVUhBd0I3Z2dFZ0JnTlZIU01FZ2dFWE1JSUJFNEFVTEJyaUNwUzlzNTlpb1Y5MGpGMEcwWENZMUxXbWhnZmFrZ2ZNd2dmQXhDekFKQmdOVkJBWVR
BbEJNTVJRd0VnWURWUVFJREF0dFlYcHZkMmxsClkydHBaVEVSTUE4R0ExVUVCd3dJVjJGeWMzcGhkMkV4UFRBN0JnTlZCQW9NTkVsdWMzUjVkSFYwSU1XQnhJVmoKZW01dnhadGphU0F0SUZCaHhZUnpkSGR2ZDNrZ1NXNXpkS
GwwZFhRZ1FtRmtZWGRqZW5reFBEQTZCZ05WQkFzTQpNMXBoYThXQ1lXUWdXbUZoZDJGdWMyOTNZVzU1WTJnZ1ZHVmphRzVwYXlC SmJtWnZjbTFoWTNscWJubGphQ0FvCldpMDJLVEVkTUJzR0ExVUVBd3dVVTBWT1ZDQkhSV
ThnU1ZSTUlGSnZiM1FnUTBFeEhEQWFCZ2txaGtpRzl3MEIKQ1FFV0RYbzJRR2wwYkM1M1IYY3VjR3IDQWhBRE1BMEdDU3FHU0liM0RRRUJDd1VBQTRJRUFRQ2ZBaGErZ2ZyZAo5WlJmYVIFdk9YelFESm44ZVY1ZGVjeTJOTINzOU95Z
mg4cmVOb2JUTnBNaIVIRlRPUTdWRFJ1Uk5vZWxYS1ltCnJLYWM0blzb0xuUFZUK0MzSlV0MWpQc1Q0N3YvQWNoT3prZzgyMkEwZ0RHVmhON0lZSmNJYmtnbW5HYUV4U04KVTNKT3JmUnhOcnZlK1pWUjZSRnJYeUpYMWJJdWhleG
1TUmxwOVNNZENGYkFsM2NJK3V5OXhxRzZTZm9sUHpOMgpwNGNlcTVucVlza2VTRlc4dXVuMlZEM0NoNHN1TW1RR25oYWlYZDliTVpiTTNEcE1xcThUdlJsbjJJejlyZHhCm9HU3Fjbm5BUmUvS0R4UHNvSEh6T0tSNmZvWTQ4REFyN
1YyUlJRSkJSOXFYL0Rpc3NEeWR3ZUxxamhxU1lUL3QKTjc5Q1l2bFhyODNjeW1aTUlIQ3pyaUxYeWhqZ3F5dU9xWWNzMUxFdHllenozWU5ZY2ZvQVRZT3kydmNyZExT SApKejBodk9VSHJuM0lCNWF0elhXNzY0MDlMZnNKaFEvUnU4eT
FxeGhjUzRKSC9sSlZWV3VaekZTRzd1VXM0V082Cm1EOXc3NmZiWXV2UGQvYXo2bUlra0c3aWZ0NjdCOTR0MElaNy9haUxaZDZudHA3OSt0ZnlydkNZMzVwbDBQSzAKUGVUZFpzdlN5Q1k3eVlyRUxNSTBFSGN0ZFFGazJLMGRwNG5lY

Krok 6
- w pkt 4 (*Żądanie podpisania i wystawienia certyfikatu dla domeny wskazanej przez operatora usługi ZSL/OBU*) wyświetlonego widoku (*ZSL112 – Aktualizacja danych usługi ZSL/OBU Operatora*) wklej nowy CSR (Żądanie podpisania certyfikatu)
- wybierz przycisk „Wyślij” na formularzu ZSL112



Krok 7
- otrzymanie potwierdzenia zaktualizowania usługi



DODATKOWE INFORMACJE

Wyciąg z dokumentacji ***„Wymogi techniczne przekazywania danych geolokalizacyjnych niezbędnych do poboru opłaty elektronicznej dla Operatorów OBU i ZSL”*** w zakresie zastosowania certyfikatów SSL:

„W celu uzyskania certyfikatu dla domeny wykorzystywanej przez Operatora OBU lub Operatora ZSL do wysyłki danych lokalizacyjnych do SPOE KAS w ramach usługi e-TOLL, uprawniony przedstawiciel Operatora powinien użyć konta w serwisie https://puesc.gov.pl/. Po zalogowaniu i wyświetleniu głównego okna tego portalu, przedstawiciel Operatora wybiera w menu Formularze → Formularze SPOE KAS.

Następnie, w zakładce Rejestracja usług dla Operatora ZSL lub Operatora OBU i urządzeń GPS w ramach usług wybiera formularz: REJESTRACJA USŁUG ZEWNĘTRZNYCH SYSTEMÓW LOKALIZACYJNYCH (ZSL) OPERATORA.

Użytkownik wypełnia pola formularza. W polu **Żądanie podpisania i wystawienia certyfikatu dla domeny wskazanej przez Operatora ZSL lub Operatora OBU** wkleja CSR (ang. Certificate Signing Request). CSR generuje się na podstawie swojego klucza prywatnego. Można do tego użyć openssl'a (www.openssl.org). Jeżeli użytkownik posiada już klucz prywatny (np. plik private.key) to w środowisku Linux polecenie ma następującą budowę:

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

Jeżeli użytkownik nie ma klucza prywatnego można go wygenerować na przykład:

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

(długość 4096 bitów daje lepszy poziom zabezpieczeń niż klucz 2048)

Przykład pliku zawierającego klucz prywatny prezentuje Rys. 4.

Rys. 4. Przykład pliku z kluczem prywatnym

Z kolei przykład pliku zawierającego CSR przedstawia Rys. 5.

Rys. 5. Przykład pliku zawierającego CSR

Więcej szczegółów można znaleźć pod adresem:
https://tech-itcore.pl/2012/07/04/generowanie-wlasnego-certyfikatu-ssl/
https://uk.godaddy.com/help/apache-generate-csr-certificate-signing-request-5269

W formularzu **musi być możliwość** podania **adresu e-mail**, na który użytkownik otrzyma formularz z odpowiedzią.

W formularzu z odpowiedzią Operator ZSL, Operator OBU otrzymuje Certyfikat klienta zakodowany w formacie base64.
Należy go rozkodować. **Nie należy dodawać do niego linii BEGIN/END CERTIFICATE**, trzeba tylko użyć narzędzia potrafiącego odkodować tekst zakodowany w Base64, np.:

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

4. openssl base64 -d -in plik_z_zakodowanym_certyfikatem.txt -out certyfikat.pem

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

6. Certutil -decode plik_z_zakodowanym_certyfikatem.txt certyfikat.pem (dla Windows korzystając z linii poleceń).

Przykład certyfikatu w base64 prezentuje Rys. 6.

Rys. 6. Certyfikat zakodowany w Base64

Natomiast przykład certyfikatu odkodowanego w formacie PEM (ang. Privacy-Enhaced Mail) pokazano na Rys. 7.

Rys. 7. Przykład odkodowanego certyfikatu

Po odkodowaniu otrzymuje się plik zawierający maksymalnie trzy certyfikaty w formacie PEM:

1. Certyfikat klienta,
2. Certyfikat CA (Centrum Autoryzacji) poziomu 1, które wystawiło certyfikat klienta,
3. Certyfikat CA (Centrum Autoryzacji) poziomu 0, które wystawiło certyfikat CA poziomu 1.

Każdy certyfikat rozpoczyna się i kończy liniami:
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
Powyższe linie oznaczają początek i koniec poszczególnych certyfikatów.
Zakres i sposób użycia danych, które są stosowane do zabezpieczenia komunikacji TLS, jest różny i zależy od użytkowanego przez podmiot systemu / aplikacji. Niemniej, typowe wymagania narzędzi

/komponentów SSL/TLS obejmują wykorzystanie w trakcie uwierzytelniania SSL następujących elementów:

1. certyfikatu klienta;
2. klucza prywatnego – który zabezpiecza możliwość użycia certyfikatu klienta wyłącznie przez podmiot będący jego dysponentem;
3. łańcuch certyfikacji / łańcuch certyfikatów (ang. certificate chain), który uwierzytelnia certyfikat klienta jako certyfikat wystawiony przez właściwe CA i zawiera:
    1. certyfikat CA (Centrum Autoryzacji) poziomu 1, które wystawiło certyfikat klienta,
    2. certyfikat CA (Centrum Autoryzacji) poziomu 0, która wystawiło certyfikat CA poziomu 1.

W środowisku Linux połączenie z SPOE KAS można przetestować z wykorzystaniem narzędzia curl. Sekwencję komend przedstawiono poniżej. Certyfikat.pem oznacza otrzymany certyfikat, który został odkodowany z formatu base64 do formatu PEM. Natomiast fd1.key oznacza klucz prywatny (odszyfrowany) użyty do generowania 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

Uwaga 1: Adres https://cloud.spoe-dev.il-pib.pl:8443/zsl/ssl/10000000-0001-1001-0001-0000000000001 należy zastąpić otrzymanym adresem z formularza otrzymanego pocztą elektroniczną, chodzi o zawartość pola **Adres URL usługi e-TOLL dedykowany do komunikacji z usługą Operatora ZSL lub Operatora OBU**.

Uwaga 2: Certyfikat X.509 klienta SSL/TLS po stronie Operatora ZSL lub Operatora OBU

Do obowiązków Operatora ZSL lub Operatora OBU należy:

1. uzyskanie w/w certyfikatu:
    a. pierwszego - w wyniku rejestracji usługi,
    b. każdego kolejnego przed upływem 365 dni od wystawienia poprzedniego certyfikatu;
2. stosowanie aktualnego certyfikatu X.509 klienta SSL/TLS do uwierzytelnienia komunikacji z interfejsem danych SPOE KAS.

Pierwszy certyfikat X.509 klienta SSL/TLS jest wydawany w odpowiedzi na przesłanie do SPOE KAS poprzez dedykowany portal żądania wydania certyfikatu X.509 klienta SSL/TLS za pośrednictwem jednego z dwóch dostępnych form komunikacji:

1. dokumentu XML;
2. formularza rejestracji usługi wypełnianego na stronie usługi SPOE KAS w dedykowanym portalu SPOE KAS.

Kolejny certyfikat można uzyskać poprzez przesłanie do SPOE KAS za pośrednictwem dedykowanego portalu żądania wydania certyfikatu X.509 klienta SSL/TLS za pośrednictwem jednego z dwóch dostępnych form komunikacji:

1. dokumentu XML;
2. formularza aktualizacji danych usługi wypełnianego na stronie usługi e-TOLL w dedykowanym portalu.

Certyfikat X.509 klienta SSL/TLS służący do uwierzytelniania Operatora ZSL lub Operatora OBU w trakcie komunikacji z interfejsem danych SPOE KAS jest pierwszym z certyfikatów zwracanych przez SPOE KAS w odpowiedzi na przesłanie formularza/dokumentu XML. Każdy ze zwróconych certyfikatów rozpoczyna się od linii „-----BEGIN CERTIFICATE-----" a kończy się linią „-----END CERTIFICATE-----".

Datę ważności certyfikatu X.509 klienta SSL/TLS można podejrzeć za pomocą bezpłatnego pakietu narzędzi OpenSSL przy użyciu następującego polecenia:

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

gdzie:

1. plik_z_certyfikatem_klienta_x509.pem - stanowi przykładową nazwę pliku zawierającego certyfikat X.509 klienta SSL/TLS wystawiony przez SPOE KAS.

Poniżej podano przykładową odpowiedź na w/w polecenie:

notAfter=Sep 30 08:30:58 2020 GMT

gdzie:

1. notAfter - etykieta pola „nie później" z certyfikatu X.509, które zawiera ostateczny termin ważności certyfikatu, po którym, nie należy ani go używać ani mu ufać;
2. Sep – trzy literowy skrót nazwy miesiąca, w tym przypadku to skrót od September , czyli Wrzesień;
3. 30 – dzień;
4. 08:30:58 – godzina, minuta i sekunda;
5. 2020 – rok;
6. GMT – trzy literowy skrót nazwy strefy czasowej, oznaczenie strefy czasowej, w tym przypadku jest to skrót od Greenwich Mean Time, oznaczający, że aby uzyskać godzinę dla strefy czasowej Europa/Warszawa należy do podanej godziny dodać 2 godziny w przypadku czasu letniego i jedną godzinę w przypadku czasu zimowego.

Uwaga 3: Konfiguracja „mutual TLS"
W przypadku konfiguracji mutual TLS należy zwrócić uwagę, że zmiana certyfikatu serwera uniemożliwi poprawną autentykację komunikacji. Informacja o zmianie certyfikatu serwera będzie propagowana do Operatorów, natomiast w przypadku jakichkolwiek problemów z weryfikacją certyfikatu serwera można wykorzystać komendy umożliwiające podgląd certyfikatu, tj.:

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