

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

The screenshot shows the PUESC website interface. At the top, there is a navigation bar with the following items: MÓJ PULPIT, USŁUGI, USŁUGI SIECIOWE, POMOC, FORMULARZE, AKTUALNOŚCI, and SINGLE WINDOW. Below the navigation bar, there is a breadcrumb trail: PUESC > Usługi > Formularze >. On the left side, there is a vertical menu with several categories, each with a dropdown arrow. The categories are: AKCYZA, GRY HAZARDOWE, PRZEMIESZCZENIA I PRZEWOZY; CŁO, GRANICA I STATYSTYKA; OBSŁUGA WNIOSKÓW I ZABEZPIECZEN; STREFA KLIENTA KAS; FORMULARZE (highlighted with a red border); and USŁUGI SIECIOWE - INFORMACJE I SPECYFIKACJE. The main content area is titled 'Katalog formularzy' and contains the following text: 'Wyszukaj interesujący cię formularz interaktywny w poniższym katalogu.' and 'Wypełniając wybrany formularz postępuj zgodnie z instrukcjami na ekranie.' Below this text, there are two sections: 'Mapowanie formularzy PUESC na PUESC-2' with a dropdown arrow pointing down, and 'Formularze alfabetycznie' with a dropdown arrow pointing up. A search bar is located below the 'Formularze alfabetycznie' section, containing the text 'ZSL105' and a red button labeled 'WYSZUKAJ'. Below the search bar, there is a horizontal list of letters: A D G I K L O P R S T V W Z. The letter 'S' is highlighted in red. Below the letters, there is a red link: 'SENT ZSL105 - Aktualizacja danych rejestracyjnych usługi ZSL/OBU [SENT]' with a green dot and the text 'dostępna'. Below the link, there is a description: 'Formularz do zarządzania zarejestrowanymi usługami ZSL/OBU oraz urządzeniami przez operatorów ZSL/OBU'. At the bottom of the main content area, there is a section titled 'Formularze w grupach' with a dropdown arrow pointing down.

Krok 2

- zatwierdź wyświetlony NIP firmy

Powrót

DANE OPERATORA USŁUGI

TYP IDENTYFIKATORA *

NIP

NUMER IDENTYFIKATORA *

5970551996

Zatwierdź

3.22.34-SNAPSHOT, develop, e077414 2022-09-17T05:14:22+0200 GK, Serwer: 152

Wersja na portalu głównym: 3.22.34-SNAPSHOT, develop, e077414 2022-09-17T05:14:22+0200 GK

Krok 3
- wybierz pole „Lista usług”

Edytuj Lista usług Lista urzędzeń Drukuj Powrót

ZSL101 - INFORMACJA O ZAREJESTROWANYM OPERATORZE ZSL/OBU

Typ operatora usługi: **ZSL**
Status operatora usługi: zarejestrowany

INFORMACJE DOTYCZĄCE NINIEJSZEGO ZGŁOSZENIA

Suma kontrolna: aa59b3d90f8d09b85f4c7e510d002ba72608da25

INFORMACJE DOTYCZĄCE REJESTRACJI OPERATORA USŁUGI ZSL/OBU

Data rejestracji: 2020-09-15 godz.18:10:27
Rejestrujący: Marek Tomczyk
Data modyfikacji: 2022-09-22 godz.10:28:48
Modyfikujący: Marek Tomczyk

INFORMACJE O OPERATORZE USŁUGI ZSL/OBU

Identyfikator idSISC: PL597055199600000
Pełna nazwa: GEO INFO 1.3
Rodzaj identyfikatora: NIP
Numer identyfikatora: 5970551996
Adres
Świętokrzyska1 12 / 21261
00-916 Warszawa123, PL

INFORMACJE KONTAKTOWE DO ADMINISTRATORA OPERATORA USŁUGI ZSL/OBU

Telefon: 226663322
E-mail: marek.tomczyk.puesc@gmail.pl

3.22.34-SNAPSHOT, develop, e077414 2022-09-17T05:14:22+0200 GK, Serwer: 152

Wersja na portalu głównym: 3.22.34-SNAPSHOT, develop, e077414 2022-09-17T05:14:22+0200 GK

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

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

MÓJ PULPIT USŁUGI USŁUGI SIECIOWE POMOC FORMULARZE AKTUALNOŚCI SINGLE WINDOW

Moje sprawy i dokumenty Do wysyłki i robocze Moje usługi Moje dane Dane Podmiotu e-Dokumenty e-Płatności

PUESC > Usługi > Akcyza, gry hazardowe, przemieszczenia i przewozy > Przewóz towarów objęty monitorowaniem (SENT) > ZSL - 105 >

ZSL112 - AKTUALIZACJA DANYCH USŁUGI ZSL/OBU OPERATORA

Wyślij **Powrót**

Numer usługi: ZSL-CSFF-8

1. Typ usługi

USŁUGA ETOLL

USŁUGA SENT-GEO

Wymagane zaznaczenie przynajmniej jednej usługi

2. Nazwa lub opis własny usługi

NAZWA LUB OPIS WŁASNY USŁUGI *

Test123455 1

3. Adresy IPv4, z których usługa ZSL/OBU będzie przysyłała dane do usługi eTOLL, SENT-GEO

ADRES IP

Dodaj

1.	222.111.111.222	
----	-----------------	--

4. Żądanie podpisania i wystawienia certyfikatu dla domeny wskazanej przez operatora usługi ZSL/OBU

CSR (CERTIFICATE SIGNING REQUEST - ŻĄDANIE PODPISANIA CERTYFIKATU)

(należy wkleić CSR włącznie z -----BEGIN CERTIFICATE REQUEST----- i -----END CERTIFICATE REQUEST-----)

Krok 7

- otrzymanie potwierdzenia zaktualizowania usługi

Edytuj usługę Anuluj usługę Dodaj urządzenia Usuń urządzenia Lista urządzeń Drukuj Powrót

ZSL111 - POTWIERDZENIE REJESTRACJI USŁUGI OPERATORA ZSL/OBU

Numer usługi: **ZSL-CSFF-8**
Status usługi: **zarejestrowana**

NAZWA LUB OPIS WŁASNY USŁUGI

Test123455 1

TYP USŁUGI

eTOLL
 SENT-GEO

INFORMACJE DOTYCZĄCE NINIEJSZEGO ZGŁOSZENIA

Suma kontrolna: 5abe2fbc8361248f9af759ad2241f5aa557341c9

INFORMACJE DOTYCZĄCE REJESTRACJI USŁUGI ZSL/OBU

Data rejestracji: 2022-04-28 godz.05:54:34
Rejestrujący: Marek Tomczyk
Data modyfikacji: 2022-09-22 godz.10:33:40
Modyfikujący: Marek Tomczyk

INFORMACJE O OPERATORZE USŁUGI ZSL/OBU

Rodzaj identyfikatora: NIP
Numer identyfikatora: 5970551996

ADRES URL USŁUGI ETOLL DEDYKOWANY DO KOMUNIKACJI Z USŁUGĄ ZSL/OBU

https://spoe-dev.il-pib.pl:8443/zsl/ssl/68c9435b-3288-470a-9882-1e2493fd6876

ADRESY IPV4, Z KTÓRYCH USŁUGA ZSL/OBU BĘDZIE PRZESYŁAŁA DANE DO USŁUGI ETOLL / SENT-GEO

IP: 222.111.111.222

CERTYFIKAT KLIENTA WYSTAWIONY PRZEZ CENTRUM CERTYFIKACJI ETOLL / SENT-GEO (ZAKODOWANY W FORMACIE BASE64)

LS0L51CRUdJtIBDRJU SUZJQ0FUR S0H S0Ck1J SUI SVENDQkMyZ0F3 SUJBJZ0IDQTNZd0RRWUplb1pJaHzJtKFRRUxUUFU3Z2U0eEN6QUlPCZ05WQkFZVEFSQk0KTVJRd0VnWURWUUVJREF0dFYcH2kMmxsJt0cFpURTINRHHN QTFVRUNdzbTVzV6ZehsMGRYUW4dWUhfAfD0NgpbS9GbTJocEIDMGdVR0hGaEhOMGQyOTNIIJKYm5OMGVYUJFkQ0JDWVdSaGQyTJZIVEU4TURVR0EXVUUD3d6CldRnJ4WUjpoWkNCYVIXRjNZv6YjNkaGJubGphQ0JVVld Ob2JtbJJRWx1Wm05eWJXRmpIV3B1ZVdOb0lDaGEKTFRZcE1Ta3dKdIEVFRFRERDQIR SVTVV SUVkRiRSQkPWRXdnV2x0TUIGUmXjM1FnEdWmMpXzd2dNUUJEUVRFApNqJhHQ1Nxr1NJYNEUUVKQVJZU2MvNnVKR2RSYjBCcGR Hd3VMkMYzT5G5Cc01CNFhEVEI5TURreU1qQTRNek0wCk1Gb1hEVEI6TURreU1qQTRNek0wTUZvd1IURUxNqWQHQT FVRUJoTUNVRX4dRGPBTUJnTIZCQU1NQIvWfkyVniKTVJFd0R3WURWUUVFIREoWfY SnpIbUyZVVRFE1Ba0dM MVVQ2d3Q1RVWxhGREFT QmdOVKBZ01DMJFozW05MwpHY1ZqYTYjbeE1Rd3dD2I1EIVFRTERBTkVxbEF3Z2dFau1BMEdDU3FHU0lMORRRUJBUVVBQTRJQkR3QXdnZ0LkCkFvSUJBUURWZkozU2JONTInC9WUkxpVHR5S5mMwVz JTTWJtonVehoxVm9ac3B6Wfknk5uSXIP0EJYNjpyTKEKZ2VGUUVkamZJRjkwXJnQ0VNNIBIZIN2N2kzMEFOZk0VHZXaW9leE1kQ0FLKz1 SUVXT3dKbXhFay95ZAp6aE9BV2I2dGh50TVOStVcC9yaByYVhoZTRJa3FDJRUy kN5K21KTjYzCtUL2VWkHZINDRhaU5RFJ0VW01CkdNMG5j3hTtH5MvkvTmJmW9qd1VPQWNYjdXNzhRd213NWFSQXZvSH0VEN2 SWp SWjZteWSJkzhxQVUUEKRF0IR25IOHq1UkVqY1UxckliNvBbVnObW3K2hmZ013RHN4R 3c253F45GtVUZzaWx1cG0vK1ZURGIvde92agpFNHcrL2HlMzT3d3QXfYIMxYzlidGMrWEFIQWdNqkFBR2pnZ0YzTUJQmN6QUlPCZ05W SFJNRUFqQUFNqjBHCkEXVWREZ1FXQkRJRnZMQmdnSVF25m5DZkwrL3BVFZU1Yh5bXNU QUSCZ05W SF4QkFmOEVQCU1DQmVBd0V3WUQKvIlwEJBD3dD21U S3dZQkJRvUhb0i3Z2dFZ0JnTIZIU01F2ZdFWE1J SUJFNEFVTEJyaUJNWUzZNTIpb1Y5MqGMEcWENZMUxXbWhnZmFZ2ZNd2dmQXhDeFKQmdOVkJBWW RBbEJNTVJRd0VnWURWUUVJREF0dFYcH2kMmxsClykYdHBAveVSTUE4R0EXVUVCd3dJvJGwWmZcGhkMkV4UFRBNOJnTIZCQWNTKvSdWmZUjVksFYwSU1XQnhJVmoKZw01dnhadGpU0F0ZU2CaHhZUnpkSGR2ZDNzINXNpk SGwwZFhRZ1FIRmZWRGqZw5rFBEQTCZ05WQkFzQzPNMXBoYThQ1XUWdXUz0z0ZJGdWmYOTNzVzU1WTJnZ1ZHvmpRzVwYXICSmJWnZjTf0WtNseWJubGphQ0FvCldpMDJLVEVktUJzR0EXVUVD3dVVTBWT1ZDQkh5 VThnU1ZSTUIGSNZM1FntBFEhEOWQFCZ2tkaGpRzJ3MEIKQ1FFV0RYbzJRR2wwYkM1M11Y3Y3R3JDQWbBRE1BMEdDU3FHU0lMORRRUJd1VBQTRJURFQRmZKaXhLeDNhWAoxVFdqeGU1R2xQalNoRGITBGNKYXJ1TDh6SzJ4T FVEWDV1QkZaNmndvbV01K2E4T0NEK2FKMmIS252qbFNaaXRPcIIZ5ENTUJEST5OdtM3K08Q25q3F5eGUzNDh3R3lqcUgvrK5qLUTBJdksrenBENjErcHJM3cveVFUczLuN24KL0Y5Gd0VmlUreEwrV2Y3qJjJNHM013tS1SbTN4WW RKSmNxbVJDQIE3R05WRG55Ry9SRURUZMANj0ZHNWQggyVilpbjMyS0VEQfIRjdQVGRtEaEwQn1dRWWJZmZ2QVpEQjwWpRPTDBwTny4OgdYUIE5ejA0E8D0nB SClp2M0HlGd3QWU4QIE4YngvQIM SFN5UEjYyYdaVUBS SbaUUVREjEVRVXaZ25Q2hoM3d4Djkd0d1BFcEKIbm84dzB0cKpZUWlla3dlDv5 SW5ieTNaFdiWwKSWNkTFCVnzMFwU0R0aZGh2NihKaG58bXB6TEjNBjG0UAc5VhlpMXRQcjdjNHBZUaf02V3JUIW1hRUUud02K3pB0TnZ kdM3Z05h0SM2zG0mH4J2F1RzRocENo5XjzCjY5XhpNddiVj2aT0Mmz2RHBJZmV5OGfIdEpK3JldG12bys1j11T0QzYmka0pRa29FYVHOU9aTBL1YKTFpJ0WnM SFhWtTbV73BibHmXZe1mQ01Wk0RzVjYQ0hRWZSMEN4 cFNMZma05DRUdXcd1D0T5YVYfYak8iS0qptEVEoalQ5WjVn3RONEJEeFRALJhdwD21dmcUVVNVK1RN5WQZTfhaFZVZmpocG2N2ZyQ2VrenVNOGdkdnhLCKRvSW44WmRWcHhLMITZ2VnVbKpGwNvXo0kVampbzxxaC5JcWZx MHQYzEhQeVd3UDFIU3ZchPIPMIoanA0uEAnKerA0UcMFQ3bZYTK43afIXU1Q4ek1QzZGUYEIZWF3OFYRZw0yJhPa0VQY2FJN5Jem1sTnZZTINZIBVbQpISDZdihRIR5ZW5WTD0a2wJmZdQFKUFRVXkXNFERj4L1fvN3V

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.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA77EQo66h5dj4n0wrgLG8J9JTheXkiHnyHdCeoh/oXt+cSAua
SvEsSeMUYYdw4fCOWeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXB
lmKuuxlXP0tCshXgPJ0ezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMR1D4G3cPBD
dOOZqSmX7tHp97q+PbVbWwvUg6eISxsgQl6SETbAoilaG8HgIO+5i2RRdZOFj++7
KGFjwEl+UxDgsNaSp7Au/UGUCzH5liQIh9N3Kfj+cGgroGv5q66kUI27d5VT2jyf
kW4k8gvltwueKSsc9/Ordlr6YopGg5xwQx+TQIDAQABAoIBAQDePSF9cqTf9X4I
TVqk16cckQQqSU5sokTQSiDbkRQmKlS/JCrgQ5VZ6Ldz+I260DCYiiA2g1pdcy7a
zCz0l1dhtHsWfVBI5HdTleu2iJO/8Iq2DGOQgC8chQbpQ8HQ1WqVIBaF+ha3W64d
VJlH7f4ctfxoGi8S5XH8Jtgg3JoldeH9YgaNzQ2LKSx9l/PxO6J7sLya82KKUBrp
M3A0umtEt0YRy57JkV7j1YeYUFLpWT7cR5rh2c2s5r1fQGTGQjQorWBU/e4Po7PMn
Vbp/qDBqni femd/dxDWydtXtJukplmLdUSKl5jAXApr2ZSXZ56espTnuIxxkvuzZ
mny15mItAoGBAP34wh8DZwvUeKI408osSgzHEtMnefIMB0u0yoj94RQZuv8VwAR
eoTeFIEPOQqgdB7MSgkgZpNuyYxW+OrQI4mMl9Wh9DyHwnWTxNO7pDJEb6BCukQb
/+bdjLSytmDyVhkGm1MQ1E0l7MdnqrQSRURvByNRXbDzZoP7wlL2bASTAoGBAPGb
HIDdlxchZkdOWNof2RDE+Ubgau86aI3dtGSsTo6bmPkXxfe6PJPu8pLwzhVOafZ
EXH4qJ9CioE4r6PelyA944KDwx8mlBsU7E6fEchJaR6xykW8u25Nr5P304szzCTI
987eJmQq+BGUUp7LgC/QlcpIR7yyP+h5CNnkAp2fAoGAecSaiCLrzacSvXl+6KXX
Jsowm5ADqBiYTSJegZ88jNq3LyFbUNToNm13D8Rp4DVz1kgOke7jXkMs9JWNGphv
NAtTAA4xkr6KW0F4Trvc8+tXx+WDNIqk75jmZCnwmn25ykx1ruwJf1A97YFuQ+zF
rHT8Edt6a4vTEebGJJm62uMCgYA06NMFH9AmguqrFW0/1lmh4oD0lJB7WT8sUjd/
Gw7zwXgLSclAnXhGrT1SEIoRAGsUE0RuHK07c0sBU3xhPlzghogqtpAKCKnc530
WcF7KxhqMGUrgHllXpFkv5EEGwIJD14hA3EQeSxdNnjDI2l6ufiukMbf62fK2JT
aMnp4QKBgDxQkHSX8E7Fh1Ui jf3C8IMZsZ7frzCbdiFNX6/PcVrcx3UKSVWmB9/v
auOMENZmoo/FRZXdcZPI0wzcGb4oz4few2Dp2savew5QEGg4v3DZDEhGK5X7Yc+m
skL3MCgqGqVN1+fv4uFHZGqPpMKMX2HUKlpLTvWNVawe0SBf25U5
-----END RSA PRIVATE KEY-----
```

Rys. 4. Przykład pliku z kluczem prywatnym

Z kolei przykład pliku zawierającego CSR przedstawia Rys. 5.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1zCCAb8CAQAwZExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAtNQVpPV01FQ0tJ
RTERMA8GA1UEBwwIV0FSU1pBV0ExDDAKBgNVBAoMA05JVDELMAkGALUECwwCwjYx
FzAVBgNVBAMMDnd3dy5pdGwud2F3LnBsMSUwIwYJKoZIhvcNAQkBFhZlLmtsaWlh
c2FyYUBpdGwud2F3LnBsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
77EQo66h5dj4n0wrgLG8J9JTheXkIHnyHdCeoh/oXt+cSAuaSvEsSeMUYYdw4fC0
WeHUe55qNSphHeumgNZnyDP9vM4b+ZDWhhHeToWvwyY5iNXBlmKuux1XP0tCsHXg
PJOezrcbMTi5pM0QU9Fc4KKOpqIV65pjJ4IinMRLD4G3cPBd00ZqSmX7tHp97g+
PbVbWwvUg6eISxsgQl6SZTbAoilaG8HgIO+5i2RRdZOFj++7KGFjwEl+UxDgsNaS
p7Au/UGUCzH51iQIh9N3Kfj+cGgroGv5q66kUI27d5VTZjyfkW4k8qvltwueKScs
c9/Ordlr6YopGg5xwQr+TQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBADjODu1l
Wqp2GJ/8nam/bjnh2WNSczQ0FjQ6IiK/+rh1Bforeky0J9cz+hRsZt5m9D8UVWkC
u4a/iJicrMZHPhTbC9tKuAk2c29ErxKJeSxr/anRkq9EbD7AB4RFmEjsJo/yRauL
oHetcTqxNPDBspkCmo2eRrKb2LdhCGFQRG4Wx/Gg6iuzd7zZKnOVKMuELpOP/vTz
Gu6QUDi2kpg/cr5A1rwg4d5uIEag1vi9G8YXNa/wkqOrNsuP660Wj8u9QgIWPdV
ikyJShahrHFxk3Qr//3P3lg0vgc4AuDcs/r4a01ET7dzuIt0qZymoQKPUOWXpfgY
gxjEmtwLRv5BqM8=
-----END CERTIFICATE REQUEST-----
```

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.

```
LS0tLS1CRUdJTI8DRVJUSUZJQ0FUR50tLS0tck1J3SUvqekNOQw5jQ0FnR1hNQTlBNHQ1N3R1N3YjNEUUVQ3dVQ
U1DQXhIakFjQmdOVk3BTU1GVUSyV255cFptBGoKwVhSbE1FRjFkR2h2Y21sMGVUQWVGdzB4T0R8NU1USXhNRE
V3TpkYUZ3MhHPVEE1TVRjeE1ERXdnAeRhTU1HRgpNukF3RGdZRFZRUURFd2RvYjIxbEExuQnNU113RkZFRZ
RUUtFdZfVYjIxbEExuQnN3SE53TG1vdU1Rc3dDUV1EC1ZRUUdFd0pRVERFYk1Ca0dBMMVVFQ0JNU2VTRmpRz1r
Ym1sdmNHOXR1M0p6YTJsbE1SRXEdE11EV1FRSEV3aHoKZW10N1pxTnB1akVjTUJvR0NTcUdTSW1zRFFFSkFSW
USZV1J0YVc1QWFOXRauZv3YkRDQ0FTSXdEUV1KS29aSQpdmhOQVFFQkJRQUrnZ0VQUROQ0FRb0Nz0VCQU
1RMVp5Y1NnZ1hMRzRHSC9TNExxVhJZTjVsa3NCcTFpcXorCmVUcTBPMVkk0enR1RKYvZ1ZYWhpC1JwZEFnyWf
ieGNGZudTznJZYkVPMgtEeThjN1cVdnpMcVQw5GFuZEt3QUwKV1B5bndGaDawR2RjRHJaTVRNTG1jbE24aU9B
Nzhnd1Z5R3VzTTNSNhp2V0tvQ204bWpK2NVDEpOTENpWtdwQgpaRT1vZnN1R1hNkd2Z1Nj1OQMFMTZOT1FVS
1QyQj1hUKIwMjQVhZwQX11dkE5VhPfk2h2ZjIyQ290S9FMKh6CkE0wI0REFEM0dms1VDMnZmZ31UMhKbkm
c0e1Jpa1U5TGRpR05ja1VGm0FTUJQM1o3amZrPHgVw1JkRzgz3dWIKZWJW11DMERbj1vcURLc59LRW15d3p
jaH9wbHE1NW1QVzZ0QnFRTDNNAH8iOwNjczZVQ0F3RUFBYU55Tuh8dwpDUV1EV1IwVEJBSXd8BREFkQmdOVkhr
NEVGZ1FVNGFqcFRmekVtNmt1ZzJ1ckRXejV5S1Nr0wNvd0RnWURWjBQCkFRSC9CQVFQwdPSU1CTudBMVksS
1FRtU18b0dQ03NHQVFRKj3TUNNQjhHQTFVZE13UUVINQwFRk11bD1aQUQkck81NER1OTZkd1dNDUrc1Z3ck
NNQTBHQ1N3R1N3YjNEUUVQ3dVQ0FUR50tLS0tck1J3SUvqekNOQw5jQ0FnR1hNQTlBNHQ1N3R1N3YjNEU
xUmxzRHN3SU5wNHJWkhyCmpPQjFDdHcyan1NeU1obU1kOFJ1bm1hUURSvUk4Cn8XcXdhL1J0Q1J1dEdEL0pH
bEJzdnRSbzVJd3A2Tm9tVFB5TE55wVhLMUJUm03RwZXR1g3aH10SGRWih0aZCRkMTk0V2hucnR3SV1Ubw1NV
HkV13VubHh0U9ieG95MeRyZXkyOT1nYVROeThNbnVYNGNuNm03dmsURmRTVjKwptRGN4VUE5MjNlcX1JMe
V1M1FR0VpNdk5FanVE53d0eGhYnZMyRwdsE6ByYk5IwMvQVNBwXVBbEFqZw1JdfQzCktUeXRkMCT1amo1dFl
hS2tRkRSNGZVSVUFUjErB2xTYj1TUTU3dkQ5Rwc3ZUxabXhC3V0dHhwZ2JwZVdWfUkU1K1L0hZUvHwVnQ0
aDc2Rwd0c01V0WdVNI4cRwGzZ0thNjFDZTUybTRzY1h1YmpjMVBuTUE3eXRXaUNEgtoNq0SM5WVRkeF1oM
FdTcWUEy8zS11mVKJZe1Y0eHhZUwhuVh1VcndxNET1M3p2bXN1v2k5bmZNeXcvUEVpZTRNC1ZnUDRTUvpuYn
Byd1h1aU5M2FvVnhDvkJVRzZzemhheNvVhd4YnZBeT10Z1JGaEJ1S0g1TTE1Q0FrQ0p3HqKbk1CV3pXb3B
UY29EN1NXNuthVh84RVQyM29rZUpqMGYSk9EN1pOV2wrVzBSbk1ak0dYtk0Z0FWS0J1M3B1bgphdWiy1Vvk
T1NemW5obU9aUudNw1tpSU0R21wdXpJdHdraEN1OStwWE4T2xv0FBPN2NTHB5cUFp0FJJS3hDcndYbGwXV
1Ayk3hhbHZSunhudjhsVHZxc2VRPT0KLS0tLS1FTkQgQ0VSVe1GSUNBVEUTLS0tLQo=
```

Rys. 6. Certyfikat zakodowany w Base64

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


```

-----BEGIN CERTIFICATE-----
MIIDjCCBF6gAwIBAgICBEQwDQYJKoZIhvcNAQELBQAwge4xCzAJBgNVBAYTA1BM
MRQwEgYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6
bm/Fm2NpIC0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwz
WmFrxYJh2CBAyWF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoICha
LTYpMskwJwYDVQDDCBTRU5UIEdFTyBjVjEwGwlnNMIFRlc3QqTGv2ZwGMSBDQTEH
MB9GCSqGSIB3DQEJARYSc2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIw
NFoXDTE5MTAxODA3MDIwNFowZzExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAttYXpvd211
Y2tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6bm/Fm2NpIC0gUGHFhHN0d293e
SBjbnN0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwzWmFrxYJh2CBAyWF3YW5zb3dhbn1
jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoIChaLTYpMskwJwYDVQDDCBTRU5UIEdFTyBj
VjEwGwlnNMIFRlc3QqTGv2ZwGMSBDQTEHMB9GCSqGSIB3DQEJARYSc2VudGdlb0BpdG
wud2F3LnBsMB4XDTE4MTAxODA3MDIwNFoXDTE5MTAxODA3MDIwNFowZzExCzAJBgNVBAY
TA1BMMRQwEgYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6
bm/Fm2NpIC0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwzWmFrx
YJh2CBAyWF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoIChaLTYpMskwJw
YDVQDDCBTRU5UIEdFTyBjVjEwGwlnNMIFRlc3QqTGv2ZwGMSBDQTEHMB9GCSqGSIB3DQE
JARYSc2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIwNFoXDTE5MTAxODA3MDIw
NFowZzExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0
SW5zdH10dXQgXyHEhWn6bm/Fm2NpIC0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6
eTE8MDoGALUECwwzWmFrxYJh2CBAyWF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVje
WpueWNoIChaLTYpMskwJwYDVQDDCBTRU5UIEdFTyBjVjEwGwlnNMIFRlc3QqTGv2ZwGMS
BDQTEHMB9GCSqGSIB3DQEJARYSc2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIw
NFoXDTE5MTAxODA3MDIwNFowZzExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAttYXpvd211Y2
tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6bm/Fm2NpIC0gUGHFhHN0d293eSBjbn
N0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwzWmFrxYJh2CBAyWF3YW5zb3dhbn1jaCBUZW
NobmlrIEluZm9ybWVjeWpueWNoIChaLTYpMskwJwYDVQDDCBTRU5UIEdFTyBjVjEwGwln
NMIFRlc3QqTGv2ZwGMSBDQTEHMB9GCSqGSIB3DQEJARYSc2VudGdlb0BpdGwud2F3LnBs
MB4XDTE4MTAxODA3MDIwNFoXDTE5MTAxODA3MDIwNFowZzExCzAJBgNVBAYTA1BMMRQwE
gYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6bm/Fm2NpI
C0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwzWmFrxYJh2CBAy
WF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoIChaLTYpMskwJwYDVQDDC
BTRU5UIEdFTyBjVjEwGwlnNMIFRlc3QqTGv2ZwGMSBDQTEHMB9GCSqGSIB3DQEJARYSc
2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIwNFoXDTE5MTAxODA3MDIwNFowZz
ExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0SW5zdH10
dXQgXyHEhWn6bm/Fm2NpIC0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6eTE8MDoG
ALUECwwzWmFrxYJh2CBAyWF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoI
C
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIKwjCCBqggAwIBAgICEAMwDQYJKoZIhvcNAQELBQAwfAxzAJBgNVBAYTA1BM
MRQwEgYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6
Bm/Fm2NpIC0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwz
WmFrxYJh2CBAyWF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoICha
LTYpMskwJwYDVQDDCBTRU5UIEdFTyBjVjEwGwlnNMIFRlc3QqTGv2ZwGMSBDQTEH
MB9GCSqGSIB3DQEJARYSc2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIw
NFoXDTE5MTAxODA3MDIwNFowZzExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAttYXpvd211
Y2tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6bm/Fm2NpIC0gUGHFhHN0d293e
SBjbnN0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwzWmFrxYJh2CBAyWF3YW5zb3dhbn1
jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoIChaLTYpMskwJwYDVQDDCBTRU5UIEdFTyBj
VjEwGwlnNMIFRlc3QqTGv2ZwGMSBDQTEHMB9GCSqGSIB3DQEJARYSc2VudGdlb0BpdG
wud2F3LnBsMB4XDTE4MTAxODA3MDIwNFoXDTE5MTAxODA3MDIwNFowZzExCzAJBgNVBAY
TA1BMMRQwEgYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6
bm/Fm2NpIC0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwzWmFrx
YJh2CBAyWF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoIChaLTYpMskwJw
YDVQDDCBTRU5UIEdFTyBjVjEwGwlnNMIFRlc3QqTGv2ZwGMSBDQTEHMB9GCSqGSIB3DQE
JARYSc2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIwNFoXDTE5MTAxODA3MDIw
NFowZzExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0
SW5zdH10dXQgXyHEhWn6bm/Fm2NpIC0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6
eTE8MDoGALUECwwzWmFrxYJh2CBAyWF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVje
WpueWNoIChaLTYpMskwJwYDVQDDCBTRU5UIEdFTyBjVjEwGwlnNMIFRlc3QqTGv2ZwGMS
BDQTEHMB9GCSqGSIB3DQEJARYSc2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIw
NFoXDTE5MTAxODA3MDIwNFowZzExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAttYXpvd211Y2
tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6bm/Fm2NpIC0gUGHFhHN0d293eSBjbn
N0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwzWmFrxYJh2CBAyWF3YW5zb3dhbn1jaCBUZW
NobmlrIEluZm9ybWVjeWpueWNoIChaLTYpMskwJwYDVQDDCBTRU5UIEdFTyBjVjEwGwln
NMIFRlc3QqTGv2ZwGMSBDQTEHMB9GCSqGSIB3DQEJARYSc2VudGdlb0BpdGwud2F3LnBs
MB4XDTE4MTAxODA3MDIwNFoXDTE5MTAxODA3MDIwNFowZzExCzAJBgNVBAYTA1BMMRQwE
gYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0SW5zdH10dXQgXyHEhWn6bm/Fm2NpI
C0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6eTE8MDoGALUECwwzWmFrxYJh2CBAy
WF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoIChaLTYpMskwJwYDVQDDC
BTRU5UIEdFTyBjVjEwGwlnNMIFRlc3QqTGv2ZwGMSBDQTEHMB9GCSqGSIB3DQEJARYSc
2VudGdlb0BpdGwud2F3LnBsMB4XDTE4MTAxODA3MDIwNFoXDTE5MTAxODA3MDIwNFowZz
ExCzAJBgNVBAYTA1BMMRQwEgYDVQQIDAttYXpvd211Y2tpZTE9MDSGALUECgw0SW5zdH10
dXQgXyHEhWn6bm/Fm2NpIC0gUGHFhHN0d293eSBjbnN0eXR1dCBcyWRhd2N6eTE8MDoG
ALUECwwzWmFrxYJh2CBAyWF3YW5zb3dhbn1jaCBUZWNobmlrIEluZm9ybWVjeWpueWNoI
C
-----END CERTIFICATE-----

```

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 użytkownika 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 uwierzytelniania 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
```