KANCELARIA PREZESA RADY MINISTRÓW

e-Doręczenia
Instrukcja dodania systemu zewnętrznego - rozszerzona

Wersja 1.5

Spis treści

1. Wstęp

Systemy Twojej instytucji, na przykład EZD (elektronicznego zarządzania dokumentacją), mogą być bezpośrednio powiązane z jej skrzynką e-Doręczeń. System dodany do skrzynki ma uprawnienia do zarządzania i obserwowania wszystkich wiadomości Twojej instytucji.

Aby dodać do skrzynki taki system, trzeba najpierw wygenerować plik CSR. Należy go załączyć przy dodawaniu nowego systemu w Module uprawnień skrzynki. Gdy system e-Doręczeń zweryfikuje przekazany pliku CSR, doda system do skrzynki, wygeneruje certyfikat X.509 i udostępni go do pobrania. Certyfikat należy pobrać do folderu, w którym znajduje się wygenerowany wcześniej plik CSR oraz certyfikat publiczny i prywatny dodawanego systemu.

Wszystkie te kroki są szczegółowo opisane w kolejnych rozdziałach.

2. Początek pracy

Aby dodać system zewnętrzny integrowany ze skrzynką e-Doręczeń, użytkownik musi być zalogowany jako właściciel lub administrator skrzynki na środowisku testowym lub produkcyjnym e-Doręczeń.

Przedtem jednak trzeba wygenerować plik CSR (Certificate Signing Request). Jest to żądanie podpisania certyfikatu – niezbędne do utworzenia certyfikatu X.509. Plik ten generuje administrator serwera, na którym umieszczony jest zewnętrzy system integrowany ze skrzynką e-Doręczeń.

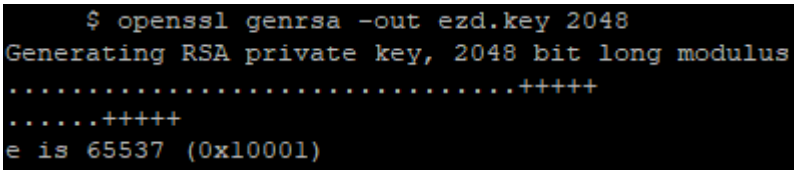
3. Generowanie kluczy

Jest wiele sposobów tworzenia kluczy prywatnych i publicznych, ale jednym z najpopularniejszych jest użycie narzędzia OpenSSL (open source). Jest ono dostępne na wszystkich głównych platformach i oferuje prosty interfejs wiersza polecenia służący do generowania kluczy.

3.1. Generowanie klucza prywatnego

Aby utworzyć **klucz prywatny**, który będzie używany z certyfikatem, wpisz poniższe polecenie OpenSSL w oknie terminala:

```
openssl genrsa -out ezd.key 2048
```

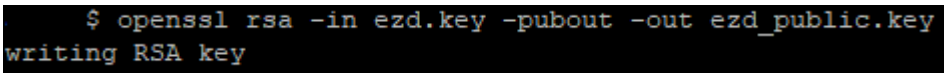


Wygenerowany klucz prywatny zachowaj w bezpiecznym miejscu bez dostępu osób trzecich. Wykonaj kopię bezpieczeństwa tego pliku. Jest on niezbędny do późniejszego używania certyfikatu. Powtórne wygenerowanie identycznego klucza prywatnego nie jest możliwe, więc jego utrata uniemożliwia zastosowanie certyfikatu.

3.2. Generowanie klucza publicznego

Aby utworzyć **klucz publiczny** na podstawie wcześniej wygenerowanego klucza prywatnego, użyj polecenia:

```
openssl rsa -in ezd.key -pubout -out ezd_public.key
```



3.3. Generowanie pliku żądania certyfikatu (Certificate Signing Request)

Aby utworzyć **plik żądania certyfikatu (CSR)** na podstawie klucza prywatnego, użyj polecenia:

```
openssl req -new -key ezd.key -out ezd.csr
```

```
$ openssl req -new -key ezd.key -out ezd.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:PL
State or Province Name (full name) []:MAZOWIECKIE
Locality Name (eg, city) []:WARSZAWA
Organization Name (eg, company) []:NAZWA FIRMY
Organizational Unit Name (eg, section) []:DZIAL IT
Common Name (eg, fully qualified host name) []:EZD.DOMENA.PL
Email Address []:IT@DOMENA.PL

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
$
```

Do tworzeniu pliku CSR podaj następujące informacje (**bez polskich znaków ani przecinka**):

- **Country Name (C)** – dwuliterowy kod kraju [PL],
- **State or Province Name (ST)** – nazwę województwa, w którym mieści się siedziba firmy [Wojewodztwo],
- **Locality Name (L)** – nazwę miejscowości, w której mieści się siedziba firmy [Miejscowosc],
- **Organization Name (O)** – pełną i dokładną nazwę firmy. Nazwa powinna się zgadzać z nazwą przedstawioną w dokumentach rejestrowych, czyli rejestr CEIDG lub KRS. W przypadku, gdy nazwa firmy przekracza 64 znaki dopuszczalne jest wprowadzenie nazwy skróconej do 64 znaków [Nazwa Firmy],
- **Organizational Unit Name (OU)** – nieobowiązkowo, opcjonalnie – nazwę działu firmy odpowiedzialnego za wdrożenie certyfikatu [Nazwa Dzialu IT],
- **Common Name (CN)** – nazwę domeny, dla której ma być wystawiony certyfikat, np. [ezd.domena.pl]. Dla certyfikatów typu Wildcard podajemy nazwę domeny w postaci [*.domena.pl],
- **Email Address [E]** – pole nieobowiązkowe,
- po tym pojawią się jeszcze dwa dodatkowe pytania (extra attributes), **pozostaw je puste** i zatwierdź klawiszem Enter:
  - **A challenge password** – puste,
  - **An optional company name** – puste.

Plik CSR to plik tekstowy. Przykład jego zawartości:

```
     $ cat ezd.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC2jCCAcICAQAwgZQxCzAJBgNVBAYTAlBMMRQwEgYDVQQIDAtNQVpPV0lFQ0tJ
RTERMA8GA1UEBwwIV0FSUlpBV0ExFDASBgNVBAoMC05BW1dBIEZJUklZMREwDwYD
VQQLDAhEWklBTCBJVDEWMBQGA1UEAwwNRVpELkRPTUVOQS5QTDEbMBkGCSqGSIb3
DQEJARYMSVRARE9NRU5BLlBMMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA37NYhe2Mx+p7zFXMim4s4yjlDFQrZeirx4NIbo9ljfFdFGLhtlnffc4B0Ooj
7TEqUCgmKJXHOfabivwRW0cIj0Vp+y0CMkAIQ4uBvPSQY4J4R5MXSf89awu0sCwx
MLHNRDAEJ4fS7j+CiUFlCj+aSPt2LXwu0WJtX8OQ/cTiwwhV5u44OAqnBvMR+wX0
qVB+lasWKpz3+itt2nSAgmoUZd7Tj3hgqP4c3vekq+E0F6nxCgm5Rw0QlEQXC/UP
nI6KmU/ZbFTn7GQDNVlI+zmsTwlFON6oerhs+rbklAVSQKBVxFSkDkkSg/LfEbxT
RmqGOZq2tYoWaPIlNyPdxzF8fQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAD18
59rOuz6e+JVOJG2zfXVG3lvFuh9ARJD4M7MGOpJKCjR9h/0TnUiEaVaIx8MwfwKj
/PRoH6+P2j6jPSQllCK4ilSeRkpLr/OcolMDpr3MGpMGwcBxjzkSwP6vCstwmUAS
+cuzrXqk/u+O5PNBqL76AXh0QXcbgBBi2xyjBrQb/iZY9zq4ASmVIfLUAvxJX7eB
FKhyQMd6CjMG4wpL7rQhGAxGWX+/2okAa4G/Mf/OcVq8NOz9KLfBvJUljlZ8tgEg
wAAKs9NjTLaRCBY+mSart+j/5fXH5rGAT2RxSFWthwhdaVXjxBrQNi9l0pNLeqFl
dk4kFYoTHWf9nXmQ/Zk=
-----END CERTIFICATE REQUEST-----
     $
```

3.4. Weryfikacja klucza prywatnego

Aby zweryfikować poprawność pliku z kluczem prywatnym, użyj polecenia:

```
openssl rsa -noout -text -in ezd.key
```

```
$ openssl rsa -noout -text -in ezd.key
RSA Private-Key: (2048 bit)
modulus:
    00:df:b3:58:85:ed:8c:c7:ea:7b:cc:55:cc:8a:6e:
    2c:e3:28:e5:0c:54:2b:65:e8:ab:c7:83:48:6e:8f:
    75:8d:f1:5d:14:62:e1:b7:59:df:7d:ce:01:d0:ea:
    23:ed:31:2a:50:28:26:28:95:c7:39:f6:9b:8a:fc:
    11:5b:47:08:8f:45:69:fb:2d:02:32:40:08:43:8b:
    81:bc:f4:90:63:82:78:47:93:17:49:ff:3d:6b:0b:
    b4:b0:2c:31:30:b1:cd:44:30:04:27:87:d2:ee:3f:
    82:89:41:75:0a:3f:9a:48:fb:76:2d:7c:2e:d1:62:
    6d:5f:c3:90:fd:c4:e2:c3:08:55:e6:ee:38:38:0a:
    a7:06:f3:11:fb:05:f4:a9:50:7e:d5:ab:16:2a:9c:
    f7:fa:2b:6d:da:74:80:82:6a:14:65:de:d3:8f:78:
    60:a8:fe:1c:de:f7:a4:ab:e1:34:17:a9:f1:0a:09:
    b9:47:0d:10:94:44:17:0b:f5:0f:9c:8e:8a:99:4f:
    d9:6c:54:e7:ec:64:03:35:59:48:fb:39:ac:4f:09:
    45:38:de:a8:7a:b8:6c:fa:b6:e4:94:05:52:40:a0:
    55:c4:54:a4:0e:49:12:83:f2:df:11:bc:53:46:6a:
    86:39:9a:b6:b5:8a:16:68:f2:25:37:23:dd:c7:31:
    7c:7d
publicExponent: 65537 (0x10001)
privateExponent:
    00:8f:de:83:6f:57:10:f4:be:1c:b2:94:f7:c0:8c:
    0d:38:67:63:b0:23:2d:ea:13:d2:ee:b4:c3:4f:bf:
    da:05:d9:16:58:f7:23:5d:cd:62:4c:41:c2:af:3e:
    f6:ae:24:b1:a6:ed:bb:64:dc:b7:4d:d3:09:c4:40:
    4b:55:5e:00:e6:4b:e9:56:4e:63:1c:38:4c:58:4c:
    8f:bb:1b:bb:05:14:b3:10:ad:4c:0c:1e:28:bd:00:
coefficient:
    5e:79:65:3f:55:46:1b:17:36:21:ad:ae:d6:3e:9b:
    98:a7:06:57:7f:9b:57:4e:f4:6a:92:f8:b6:74:bc:
    d2:9c:0f:48:f8:19:32:c0:47:2d:9a:ec:0d:6d:a6:
    32:e1:f6:0e:ca:51:0f:55:9d:e2:5e:d5:e9:d3:9e:
    a6:4c:c7:90:0d:9a:8d:8c:24:6a:70:d6:43:c5:6c:
    d6:ce:da:6b:44:58:45:4c:ee:a4:9f:69:1b:2f:23:
    02:45:8e:d2:8e:08:1a:ac:85:99:1c:05:2b:40:5f:
    80:33:6c:ff:f0:0f:2b:70:b2:b8:4b:fc:e5:ea:3f:
    00:5e:51:1e:e6:a2:d2:27
$
```

3.5. Weryfikacja poprawności wygenerowanego pliku CSR

Dzięki poleceniu `ls` zobaczymy wszystkie otrzymane dotychczas pliki :

- ezd.key - plik klucza prywatnego
- ezd_public.key - plik klucza publicznego
- ezd.csr - plik żądania certyfikatu

Poprawność utworzonego pliku żądania certyfikatu sprawdzisz poleceniem:

```
openssl req –text –in ezd.csr –noout –verify
```

Na poniższym przykładzie weryfikacja przebiegła prawidłowo. Dodatkowo pokazano wszystkie atrybuty wprowadzone podczas tworzenia pliku CSR i informację o kluczu publicznym razem z sygnaturą algorytmu.

```
    $ ls
      ezd.csr        ezd.key        ezd_public.key
    $ openssl req -text -in ezd.csr -noout -verify
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PL, ST=MAZOWIECKIE, L=WARSZAWA, O=NAZWA FIRMY, OU=DZIAL IT, CN=EZD.DOMENA.PL/emailAddress=IT@DOMENA.PL
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:df:b3:58:85:ed:8c:c7:ea:7b:cc:55:cc:8a:6e:
                    2c:e3:28:e5:0c:54:2b:65:e8:ab:c7:83:48:6e:8f:
                    75:8d:f1:5d:14:62:e1:b7:59:df:7d:ce:01:d0:ea:
                    23:ed:31:2a:50:28:26:28:95:c7:39:f6:9b:8a:fc:
                    11:5b:47:08:8f:45:69:fb:2d:02:32:40:08:43:8b:
                    81:bc:f4:90:63:82:78:47:93:17:49:ff:3d:6b:0b:
                    b4:b0:2c:31:30:b1:cd:44:30:04:27:87:d2:ee:3f:
                    82:89:41:75:0a:3f:9a:48:fb:76:2d:7c:2e:d1:62:
                    6d:5f:c3:90:fd:c4:e2:c3:08:55:e6:ee:38:38:0a:
                    a7:06:f3:11:fb:05:f4:a9:50:7e:d5:ab:16:2a:9c:
                    f7:fa:2b:6d:da:74:80:82:6a:14:65:de:d3:8f:78:
                    60:a8:fe:1c:de:f7:a4:ab:e1:34:17:a9:f1:0a:09:
                    b9:47:0d:10:94:44:17:0b:f5:0f:9c:8e:8a:99:4f:
                    d9:6c:54:e7:ec:64:03:35:59:48:fb:39:ac:4f:09:
                    45:38:de:a8:7a:b8:6c:fa:b6:e4:94:05:52:40:a0:
                    55:c4:54:a4:0e:49:12:83:f2:df:11:bc:53:46:6a:
                    86:39:9a:b6:b5:8a:16:68:f2:25:37:23:dd:c7:31:
                    7c:7d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         39:7c:e7:da:ce:bb:3e:9e:f8:95:4e:24:6d:b3:7d:75:46:df:
         5b:c5:ba:1f:40:44:90:f8:33:b3:06:3a:92:4a:0a:34:7d:87:
         fd:13:9d:48:84:69:56:88:c7:c3:30:7f:02:a3:fc:f4:68:1f:
         af:8f:da:3e:a3:3d:24:35:d4:22:b8:8a:54:9e:46:4a:4b:af:
         f3:9c:a3:53:03:a6:bd:cc:1a:93:06:c1:c0:71:8f:39:12:c0:
         fe:af:0a:cb:70:99:40:12:f9:cb:b3:ad:7a:a4:fe:ef:8e:e4:
         f3:41:a8:be:fa:01:78:74:41:77:1b:80:10:62:db:1c:a3:06:
         b4:1b:fe:26:58:f7:3a:b8:01:29:95:21:f2:d4:02:fc:49:5f:
         b7:81:14:a8:72:40:c7:7a:0a:33:06:e3:0a:4b:ee:b4:21:18:
         0c:46:59:7f:bf:da:89:00:6b:81:bf:31:ff:ce:71:5a:bc:34:
         ec:fd:28:b7:c1:bc:95:25:8e:56:7c:b6:01:20:c0:00:0a:b3:
         d3:63:4c:b6:91:08:16:3e:99:26:ab:b7:e8:ff:e5:f5:c7:e6:
         b1:80:4f:64:71:48:55:ad:87:08:5d:69:55:e3:c4:1a:d0:36:
         2f:75:d2:93:4b:7a:a1:65:76:4e:24:15:8a:13:1d:67:fd:9d:
         79:90:fd:99
    $
```

Poprawność pliku CSR zostanie sprawdzona podczas rejestracji integrowanego systemu (rozdział 4.1).

3.6. Wersje skrócone generowania pliku żądania wydania certyfikatu (CSR)

Przykłady z podaniem poniższych danych w wierszu instrukcji.

Country Name (C) – należy podać dwuliterowy kod kraju [PL].
State or Province Name (ST) – należy podać nazwę województwa, w którym mieści się siedziba firmy [Wojewodztwo].
Locality Name (L) – należy podać nazwę miejscowości, w której mieści się siedziba firmy [Miejscowosc].
Organization Name (O) – należy podać pełną i dokładną nazwę firmy. Nazwa powinna się zgadzać z nazwą przedstawioną w dokumentach rejestrowych, czyli rejestr CEIDG lub KRS. W przypadku, gdy nazwa firmy przekracza 64 znaki dopuszczalne jest wprowadzenie nazwy skróconej do 64 znaków [Nazwa Firmy].
Organizational Unit Name (OU) – pole nieobowiązkowe, opcjonalnie można podać nazwę działu firmy odpowiedzialnego za wdrożenie certyfikatu [Nazwa Dzialu IT].
Common Name (CN) – należy wpisać nazwę domeny, dla której ma być wystawiony certyfikat, np. [ezd.domena.pl]. Dla certyfikatów typu Wildcard podajemy nazwę domeny w postaci [*.domena.pl].
Email Address [E] – pole nieobowiązkowe.

- Instrukcja utworzenia pliku żądania certyfikatu:

```
openssl req -nodes -newkey rsa:2048 -keyout ed_2048_prv.key -out
ed_2048.csr -subj '/C=PL/ST=MAZOWIECKIE/L=WARSZAWA,Krolewska
17/O=ADE.EDMUND_KRAWIEC/OU=DZIAL
IT/CN=EZD3.DOMENA.PL/emailAddress=it@domena.pl
```

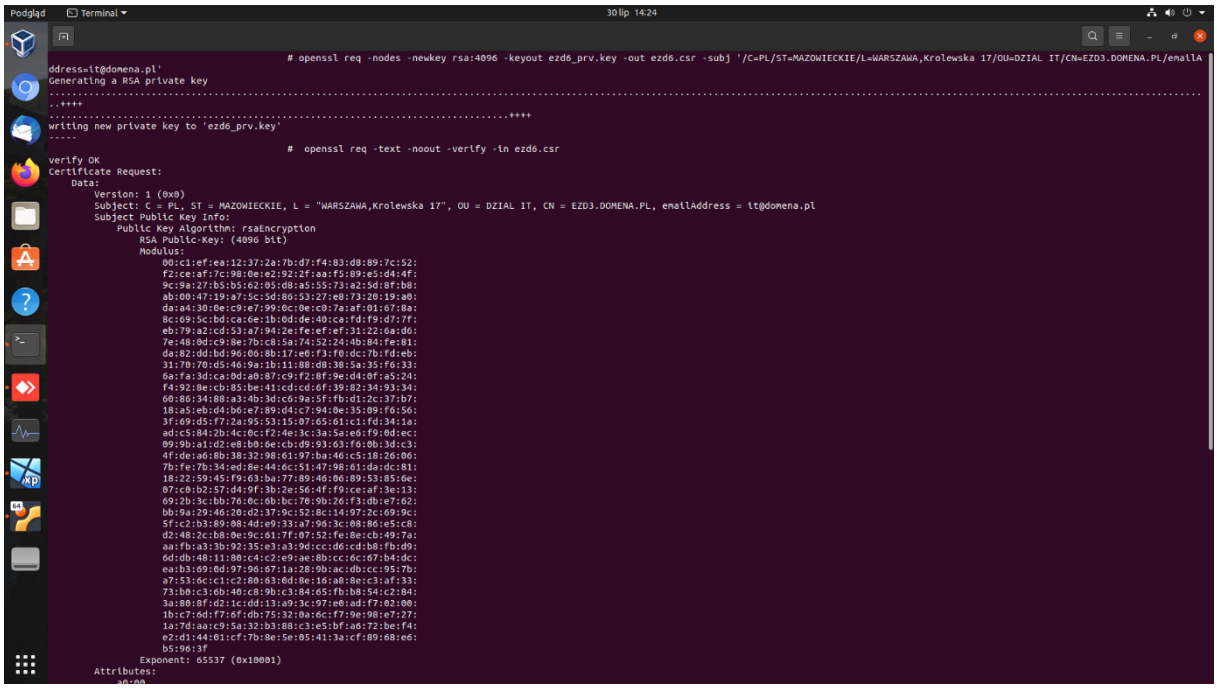
- Instrukcja weryfikacji utworzonego pliku żądania certyfikatu:

```
openssl req –text –in ed_2048.csr –noout -verify
```

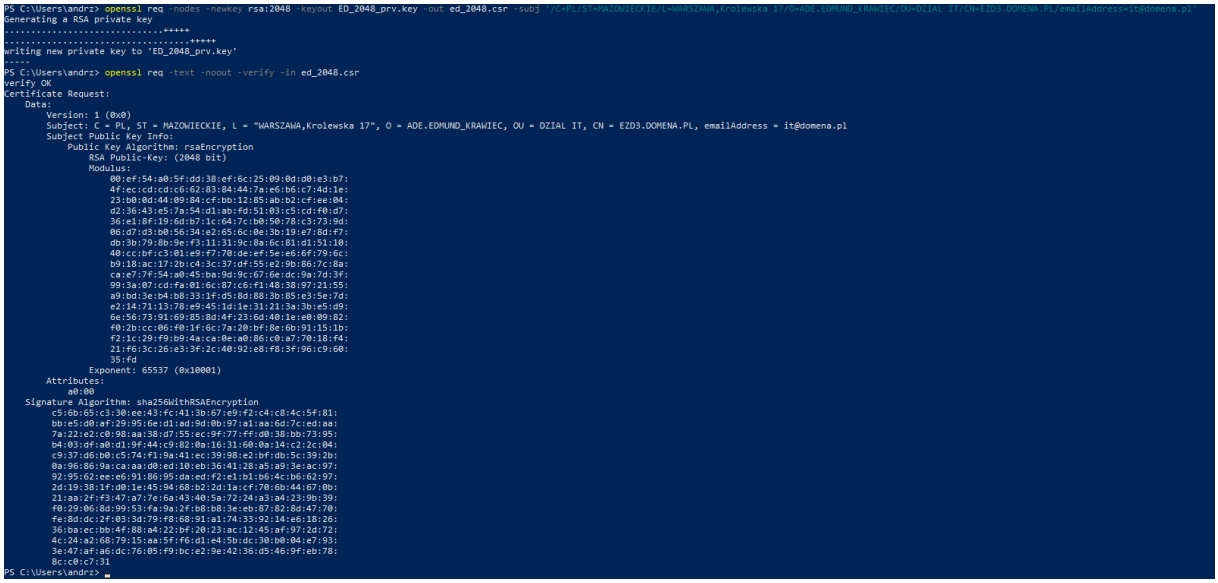
3.6.1. UNIX

```
araks# openssl req -nodes -newkey rsa:4096 -keyout ezd4_prv.key -out ezd4.csr -subj '/C=PL/ST=MAZOWIECKIE/L=WARSZAWA,Krolewska 17/OU=DZIAL IT/CN=EZD3.DOMENA.PL/emailAddress=it@domena.pl
Generating a 4096 bit RSA private key
...........++++
.....................++++
writing new private key to 'ezd4_prv.key'
-----
araks# openssl req -text -in ezd4.csr -noout -verify
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PL, ST=MAZOWIECKIE, L=WARSZAWA,Krolewska 17, OU=DZIAL IT, CN=EZD3.DOMENA.PL/emailAddress=it@domena.pl
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:b1:29:9c:4d:00:60:5b:89:27:27:75:df:36:37:
                    72:f7:79:b8:9a:69:7a:5b:45:16:2a:16:8c:5f:dd:
                    90:2d:15:5e:ef:6a:e1:6c:f0:d0:fd:f6:75:dc:e5:
                    65:24:0c:81:00:06:31:45:69:19:ee:f6:55:30:f2:
                    41:31:09:52:fa:6a:50:2e:e1:8d:da:5e:ad:2b:48:
                    5c:4e:47:40:ca:24:18:79:22:4c:9b:30:50:f3:06:
                    88:4f:e6:4d:d7:3b:10:89:47:78:86:69:ec:a8:a0:
                    4e:af:d3:bc:0e:ac:06:e2:dd:17:82:31:b9:bd:4b:
                    0e:8d:cf:23:98:e4:73:82:78:e1:a6:31:6b:d9:2e:
                    80:fc:7c:54:7d:94:3a:04:7b:db:68:aa:0f:9f:e8:
                    bc:29:9e:85:c9:89:50:c2:ef:53:e3:83:4e:ae:9c:
                    12:81:3c:cc:f9:2a:ef:4e:a5:a5:ef:e9:df:71:83:
                    31:78:17:9e:3f:5c:b3:e9:20:74:0d:bf:fc:9a:9b:
                    36:b3:14:8e:92:39:67:64:06:ac:4b:71:eb:bc:43:
                    46:aa:83:e1:87:1a:b0:ab:9b:f0:7b:93:b5:9d:13:
                    00:72:c5:9b:62:1a:da:84:b5:5a:f5:c6:bd:87:3c:
                    f6:6e:76:20:5a:86:c4:c7:d3:5f:e9:61:b2:f6:fd:
                    62:88:de:7d:d9:7c:f9:47:b0:50:e3:9a:40:83:ca:
                    7c:31:1b:07:86:16:22:9f:a5:99:52:eb:15:fa:95:
                    7e:3d:d8:ed:ab:7c:1b:fb:45:db:66:b2:13:53:4c:
                    15:f8:4d:7c:96:c2:e5:cb:24:fa:c4:41:da:7d:f1:
                    54:b5:79:47:73:7e:84:b3:6f:3d:4e:d6:cf:cb:30:
                    d1:da:bc:ab:69:67:2c:c1:ad:32:cc:21:ad:00:a5:
                    fd:73:ac:ee:48:a0:7f:70:26:5a:f4:d2:e2:fc:fd:
                    67:74:eb:1a:51:40:9d:c7:8d:02:56:1c:cf:c6:ff:
                    65:60:53:db:9a:5d:7c:8e:bc:2e:c7:06:e2:1c:ea:
                    87:db:bb:07:a7:22:ac:79:fb:13:5f:79:33:a3:4d:
                    86:a6:2a:1a:f1:df:54:c7:ad:f7:8e:12:01:6e:1c:
                    11:09:f5:aa:ce:a4:1a:79:d9:77:16:b8:df:08:a8:
                    59:9e:1b:3a:77:a2:7b:ac:c1:1c:bd:2d:15:f0:42:
                    da:00:b2:62:8c:50:ca:f3:f1:5e:6c:4a:87:a0:c1:
                    e7:6d:5c:af:d8:4b:c8:1c:0e:dc:39:73:59:ab:7a:
                    9b:03:67:ca:87:b7:4c:c4:61:a7:0f:49:8d:c3:5d:
                    06:e4:5c:03:01:98:19:87:73:65:8f:ec:36:ba:55:
                    70:d3:6f
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
```

3.6.2. LINUX



3.6.3. WINDOWS


PS C:\Users\andrz> openssl req -nodes -newkey rsa:2048 -keyout ED_2048_prv.key -out ed_2048.csr -subj "/C=PL/ST=MAZOWIECKIE/L=WARSZAWA,Krolewska 17/O=ADE.EDMUND_KRAWIEC/OU=DZIAL IT/CN=EZD3.DOMENA.PL/emailAddress=it@domena.pl"
Generating a RSA private key
writing new private key to 'ED_2048_prv.key'
PS C:\Users\andrz> openssl req -text -noout -verify -in ed_2048.csr
verify OK
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = PL, ST = MAZOWIECKIE, L = "WARSZAWA,Krolewska 17", O = ADE.EDMUND_KRAWIEC, OU = DZIAL IT, CN = EZD3.DOMENA.PL, emailAddress = it@domena.pl
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:ef:54:a0:5f:dd:38:ef:6c:25:09:0d:d0:e3:b7:
4f:ec:cd:cd:c6:62:83:84:44:7a:e6:b6:c7:4d:1e:
23:b0:0d:44:09:84:cf:bb:12:85:ab:b2:cf:ee:04:
d2:36:43:e5:7a:54:d1:ab:fd:51:03:c5:cd:f0:d7:
36:e1:8f:19:6d:b7:1c:64:7c:b0:50:78:c3:73:9d:
06:d7:d3:b0:56:34:e2:65:6c:0e:3b:19:e7:8d:f7:
db:3b:79:8b:9e:f3:11:31:9c:8a:6c:81:d1:51:10:
40:cc:bf:c3:01:e9:f7:70:de:ef:5e:e6:6f:79:6c:
b9:18:ac:17:2b:c4:3c:37:df:55:e2:9b:86:7c:8a:
ca:e7:7f:54:a0:45:ba:9d:0c:67:6e:dc:9a:7d:3f:
99:3a:07:cd:fa:01:6c:87:c6:f1:48:38:97:21:55:
a9:bd:3e:b4:b8:33:1f:d5:8d:88:3b:85:e3:5e:7d:
e2:14:71:13:78:e9:45:1d:1e:31:21:3a:3b:e5:d9:
6e:56:73:91:69:85:8d:4f:23:6d:40:1e:e0:09:82:
f0:2b:cc:06:f0:1f:6c:7a:20:bf:8e:6b:91:15:1b:
f2:1c:29:f9:b9:4a:ca:0e:a0:86:c0:a7:70:18:f4:
21:f6:3c:26:e3:3f:2c:40:92:e8:f8:3f:96:c9:60:
35:fd
Exponent: 65537 (0x10001)
Attributes:
a0:00
Signature Algorithm: sha256WithRSAEncryption
c5:6b:65:c3:30:ee:43:fc:41:3b:67:e9:f2:c4:c8:4c:5f:81:
bb:e5:d0:af:29:95:6e:d1:ad:9d:0b:97:a1:aa:6d:7c:ed:aa:
7a:22:e2:c0:98:aa:38:d7:55:ec:9f:77:ff:d0:38:bb:73:95:
b4:03:df:a0:d1:9f:44:c9:82:0a:16:31:60:0a:14:c2:2c:04:
c9:37:d6:b0:c5:74:f1:9a:41:ec:39:98:e2:bf:db:5c:39:2b:
0a:96:86:9a:ca:aa:d0:ed:10:eb:36:41:28:a5:a9:3e:ac:97:
92:95:62:ee:e6:91:86:95:da:ed:f2:e1:b1:b6:4c:b6:62:97:
2d:19:38:1f:d0:1e:45:94:68:b2:2d:1a:cf:70:6b:44:67:0b:
21:aa:2f:f3:47:a7:7e:6a:43:40:5a:72:24:a3:a4:23:0b:39:
f0:29:06:8d:99:53:fa:9a:2f:b8:b8:3e:eb:87:82:8d:47:70:
fe:8d:dc:2f:03:3d:79:f8:68:91:a1:74:33:92:14:e6:18:26:
36:ba:ec:bb:4f:88:a4:22:bf:20:23:ac:12:45:af:97:2d:72:
4c:24:a2:68:79:15:aa:5f:f6:d1:e4:5b:dc:30:b0:04:e7:93:
3e:47:af:a6:dc:76:05:f9:bc:e2:9e:42:36:d5:46:9f:eb:78:
8c:c0:c7:31
PS C:\Users\andrz>

3.7. Certyfikat klucza publicznego X.509

Weryfikacja certyfikatu – zwróć uwagę na informacje o nim (urząd podpisujący, data ważności itp.):

```
openssl x509 -in ed_2048.crt -text -noout
```

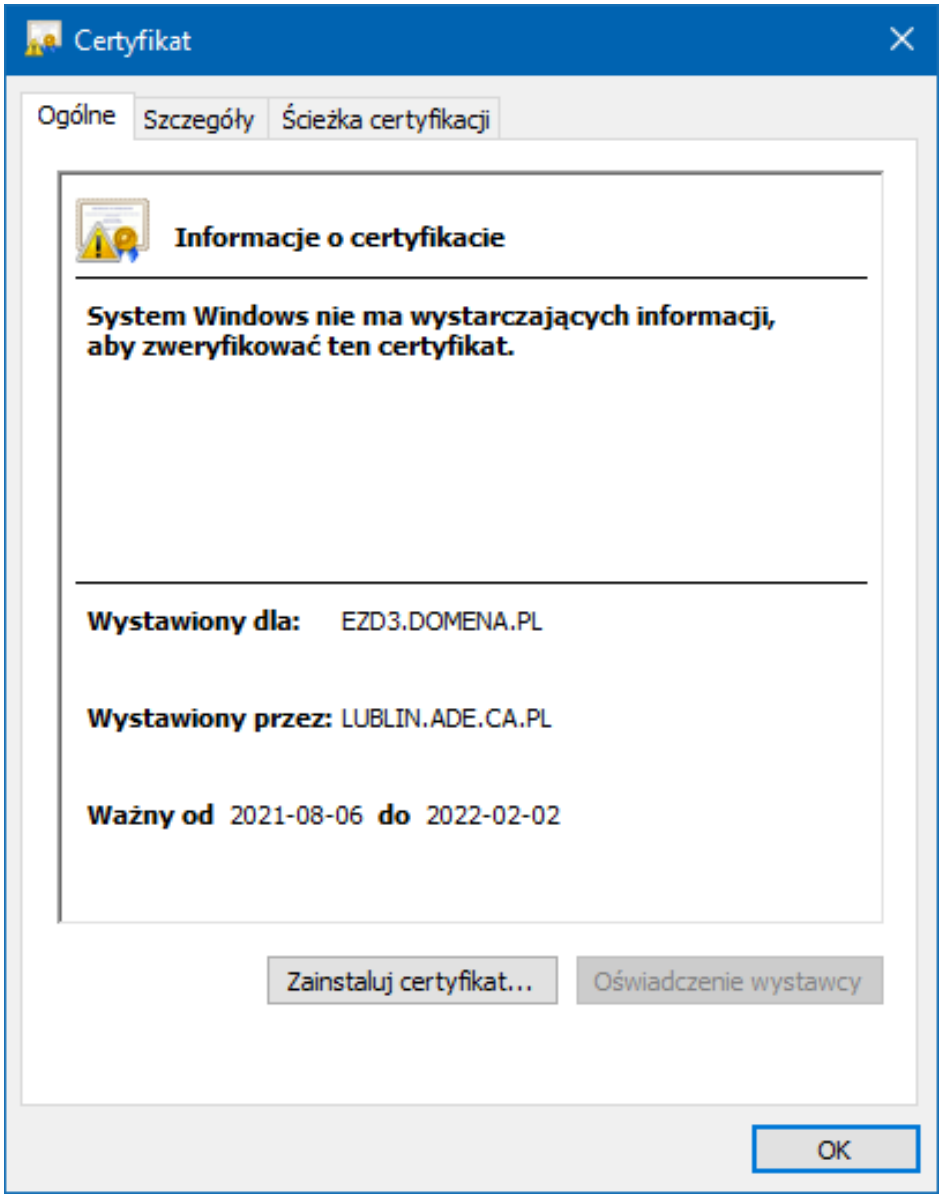
Weryfikacja certyfikatu i podpisów:

```
openssl verify -verbose -trusted CA.crt ed_2048.crt
openssl verify -check_ss_sig -trusted CA.crt ed_2048.crt
```

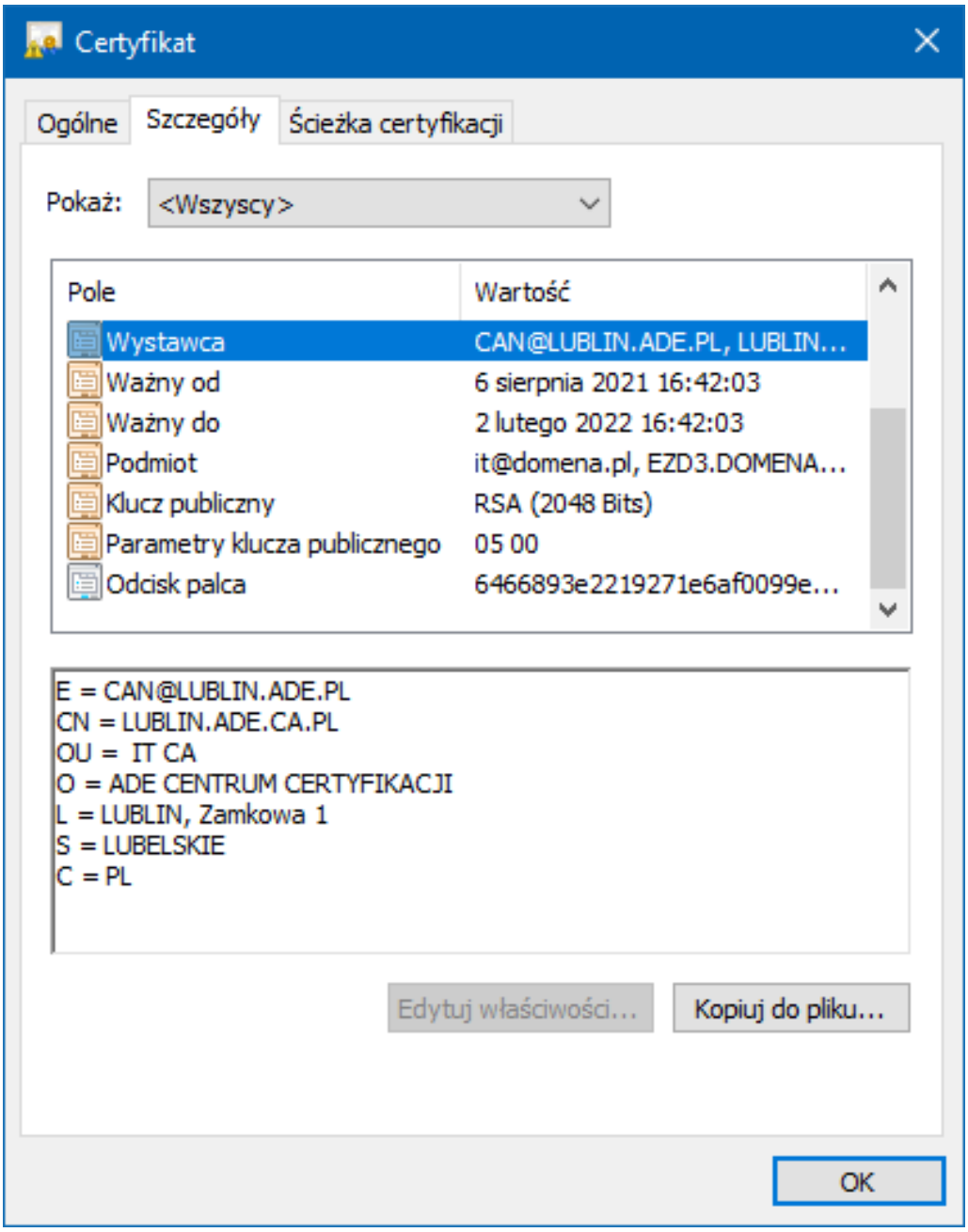
Te dwa polecenia wyświetlają sumy kontrolne md5 certyfikatu i klucza; sumy kontrolne można porównać sprawdzić zgodność certyfikatu i klucza:

```
openssl x509 -noout -modulus -in ed_2048.crt | openssl md5
openssl rsa -noout -modulus -in ed_2048_prv.key | openssl md5
```

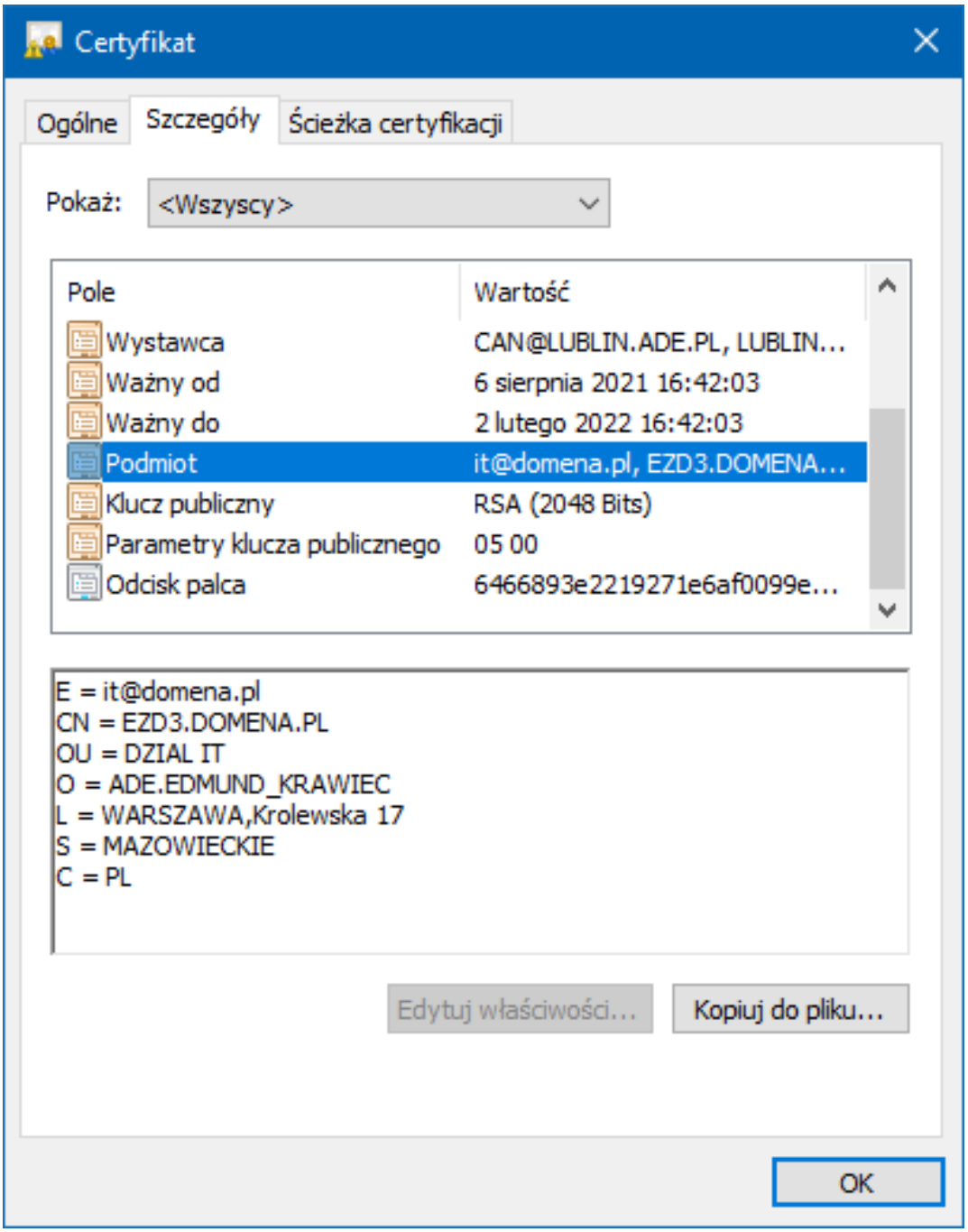
Poniżej informacje uzyskane po otworzeniu certyfikatu pod systemem Windows:



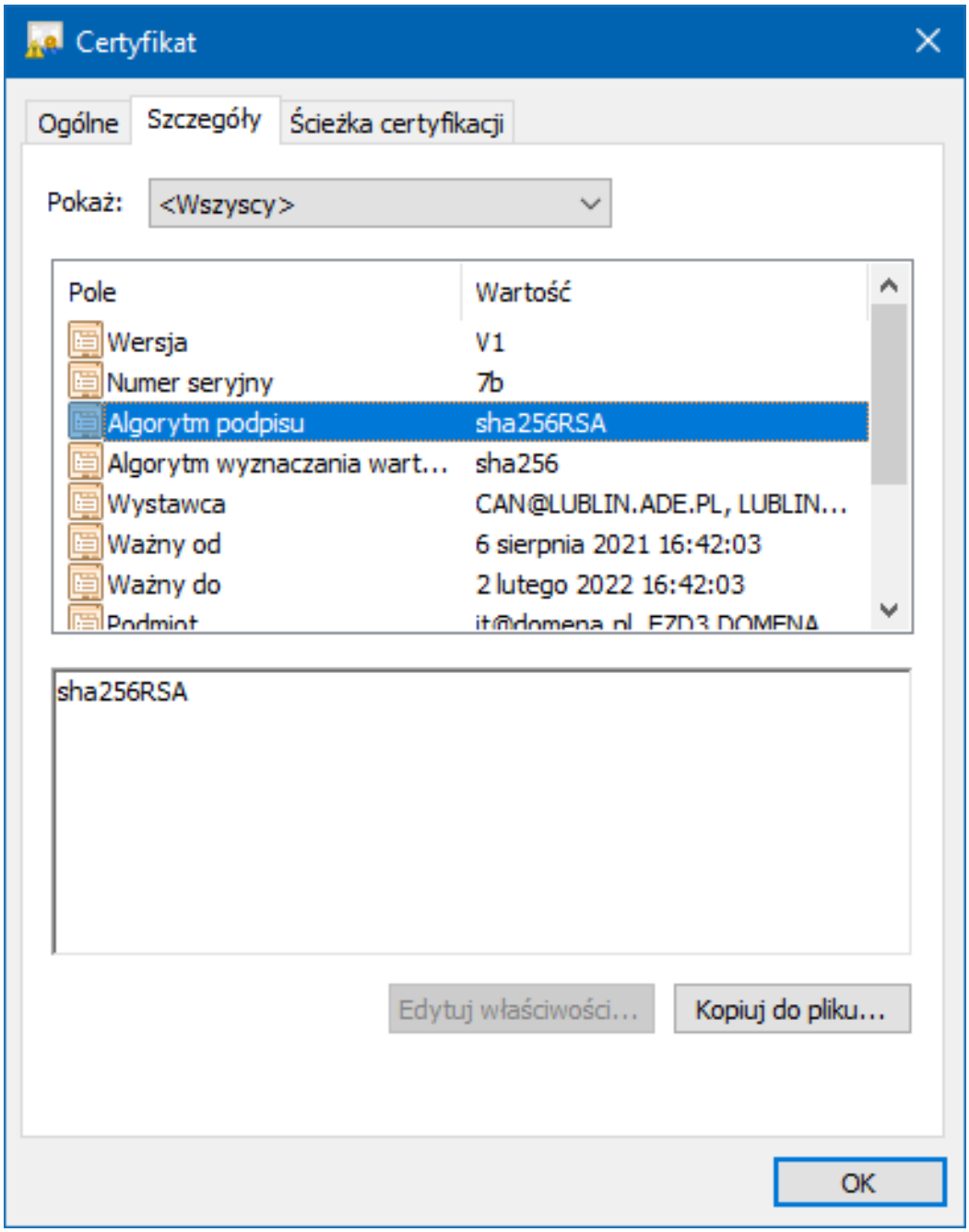
Informacje o wystawcy certyfikatu:



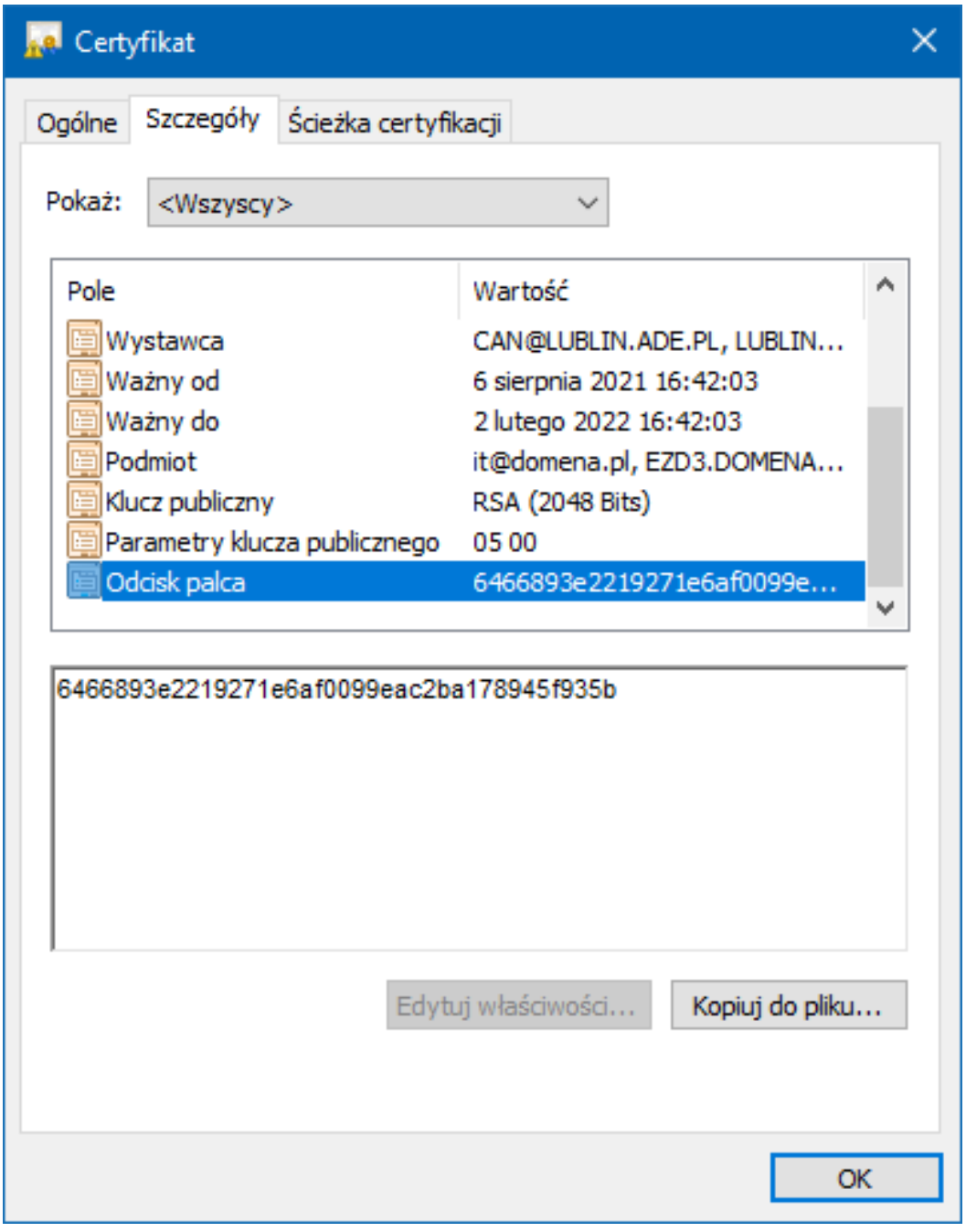
Informacje o podmiocie, dla którego został wystawiony certyfikat, na podstawie danych zawartych w pliku żądania certyfikatu:



Informacje o użytym algorytmie podpisu:



Informacje o odcisku palca certyfikatu:



Generowanie przez urząd certyfikacji (Centrum Certyfikacji) certyfikatu X.509 dla podmiotu z wykorzystaniem pliku żądania wydania certyfikatu CSR , dostarczonego przez podmiot.

```
openssl x509 -req -in ed_2048.csr -CA CA.crt -CAkey CA.key -
set_serial 123 -out ed_2048.crt -days 180
```

Weryfikacja certyfikatu X.509 podmiotu wytworzonego przez urząd certyfikacji (Centrum Certyfikacji) – zwróć uwagę na informacje o urzędzie podpisującym, dacie ważności itp.):

```
openssl x509 -in ed_2048.crt -text -noout
```

Weryfikacja certyfikatu, podpisów:

```
openssl verify -verbose -trusted CA.crt ed_2048.crt
```

Dwa polecenia wyświetlające sumy kontrolne md5 certyfikatu i klucza – sumy kontrolne możesz porównać, aby sprawdzić zgodność certyfikatu i klucza:

```
openssl x509 -noout -modulus -in .\ed_2048.crt | openssl md5
openssl rsa -noout -modulus -in .\ed_2048_prv.key | openssl md5
```

```
PS C:\Users\andrz> openssl x509 -req -in ed_2048.csr -CA CA.crt -CAkey CA.key -set_serial 123 -out ed_2048.crt -days 180
Signature ok
subject=C = PL, ST = MAZOWIECKIE, L = "WARSZAWA,Krolewska 17", O = ADE.EDMUND_KRAWIEC, OU = DZIAL IT, CN = EZD3.DOMENA.PL, emailAddress = it@domena.pl
Getting CA Private Key
Enter pass phrase for CA.key:
PS C:\Users\andrz> openssl x509 -in ed_2048.crt -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 123 (0x7b)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = PL, ST = LUBELSKIE, L = "LUBLIN, Zamkowa 1", O = ADE CENTRUM CERTYFIKACJI, OU = " IT CA", CN = LUBLIN.ADE.CA.PL, emailAddress = CAN@LUBLIN.ADE.PL
        Validity
            Not Before: Aug 16 14:08:27 2021 GMT
            Not After : Feb 12 14:08:27 2022 GMT
        Subject: C = PL, ST = MAZOWIECKIE, L = "WARSZAWA,Krolewska 17", O = ADE.EDMUND_KRAWIEC, OU = DZIAL IT, CN = EZD3.DOMENA.PL, emailAddress = it@domena.pl
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a4:8d:60:6c:5d:4d:fb:c2:82:19:6a:4c:3d:f7:
                    13:a3:11:8d:e4:f8:b5:80:e4:d7:38:10:6a:0a:1f:
                    63:10:9e:71:87:82:c9:82:db:d5:b5:5b:26:bd:4d:
                    81:f7:93:60:31:90:49:11:aa:9b:73:85:ce:a7:95:
                    aa:d8:b4:82:18:e2:f0:a1:e2:18:0b:a7:5a:9a:2d:
                    73:e4:b3:c0:f1:05:c4:7f:ab:16:15:4c:d0:d9:90:
                    fe:35:5c:be:48:ad:6e:5c:63:fc:e4:eb:38:80:48:
                    14:b4:52:c6:bd:51:1c:11:63:c4:bc:d7:8c:ff:66:
                    e0:ca:a5:65:0e:2e:d7:3d:e6:62:e4:3b:f1:ff:27:
                    ec:cc:92:9c:b6:27:30:73:b3:2b:b4:3f:00:95:6c:
                    be:96:68:30:48:68:1c:d3:0b:4d:bc:7c:32:7e:d7:
                    d9:ea:ef:b2:d0:88:3b:a5:64:00:c8:a0:11:a1:a4:
                    00:e2:55:74:62:9f:02:e2:d9:5d:df:fa:36:12:d0:
                    03:f4:57:da:79:f4:69:80:b4:45:62:1e:7f:33:a0:
                    6e:f3:8e:23:c5:74:a9:4d:b7:0e:fc:7c:50:12:89:
                    cd:b0:83:5a:a0:a9:d3:71:1f:ca:ae:9d:a8:d9:c9:
                    e3:7f:5c:2a:02:7c:5c:ff:1d:00:e5:8f:9a:9a:04:
                    48:59
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         12:67:f7:3e:0a:80:69:a0:ec:c6:b9:c0:45:24:f8:28:04:ae:
         35:93:3d:19:38:fd:d4:fc:7b:78:f3:7c:94:54:1c:08:1b:74:
         14:d3:f7:3d:17:62:ef:f5:3c:f5:2b:90:19:5a:97:c1:09:71:
         4d:13:ad:2d:10:44:e8:0a:80:57:d6:1b:5c:76:c5:5c:a6:dd:
         9f:73:20:d3:42:15:3a:15:9e:8f:2a:5f:01:ef:dc:7a:58:4c:
         34:6f:a4:f4:6e:a1:55:9b:0d:92:08:cb:19:fc:7f:21:81:54:
         96:f1:bf:86:3a:9a:54:ae:44:14:6a:8e:26:c0:23:52:4d:3b:
         2a:38:20:78:b2:6b:ed:3e:30:bc:ed:91:ec:41:6b:a5:d4:f3:
         e0:92:23:40:82:53:61:f0:81:9f:cd:1d:47:a5:0b:18:8e:41:
         0b:3c:af:b3:01:10:1f:36:e2:85:f4:c8:c9:d8:5b:c8:5d:21:
         7d:7f:c4:e3:a3:da:1e:d9:b9:6b:22:5a:43:00:27:31:94:3c:
         f6:9d:76:ce:9b:73:be:88:02:eb:df:08:76:10:08:a2:99:99:
         79:01:42:0b:54:f8:34:44:41:60:ba:84:96:ec:4a:99:50:b1:
         36:1c:85:c3:a7:97:81:f1:9e:53:a5:d9:32:a2:d8:03:ea:ee:
         1d:bc:62:ef
PS C:\Users\andrz> openssl x509 -noout -modulus -in .\ed_2048.crt | openssl md5
(stdin)= dba179cd4c7a6e850c0ceb7d7cefeccd
PS C:\Users\andrz> openssl rsa -noout -modulus -in .\ed_2048_prv.key | openssl md5
(stdin)= dba179cd4c7a6e850c0ceb7d7cefeccd
PS C:\Users\andrz>
```

3.8. Certyfikat kwalifikowany

Certyfikat umożliwiający dostęp do zasobów skrzynki powinien spełniać następujące parametry:

- **algorytmy podpisu:**
  - RSA – długość klucza zgodnie z polityką Urzędu Certyfikacji zalecane co najmniej 2048 bitów
  - ECDSA z użyciem P-256
  - ECDSA z użyciem P-384
  - ECDSA z użyciem P-521
- **użycie klucza:** digital signature
- **ulepszone użycia klucza:** niewymagane
- **wartość atrybutu „Subject”:** pole powinno zawierać dane umożliwiające jednoznaczną identyfikację podmiotu, który jest właścicielem skrzynki (np. jeden z identyfikatorów NIP, REGON, nazwę, adres).

Informacje dodatkowe

1. Certyfikat może być wydany przez polski lub zagraniczny urząd certyfikacji. Ważne, aby spełniał powyższe parametry.

2. Dopuszczalne jest użycie kwalifikowanej pieczęci elektronicznej i zaawansowanej pieczęci elektronicznej potwierdzonej kwalifikowanym certyfikatem.

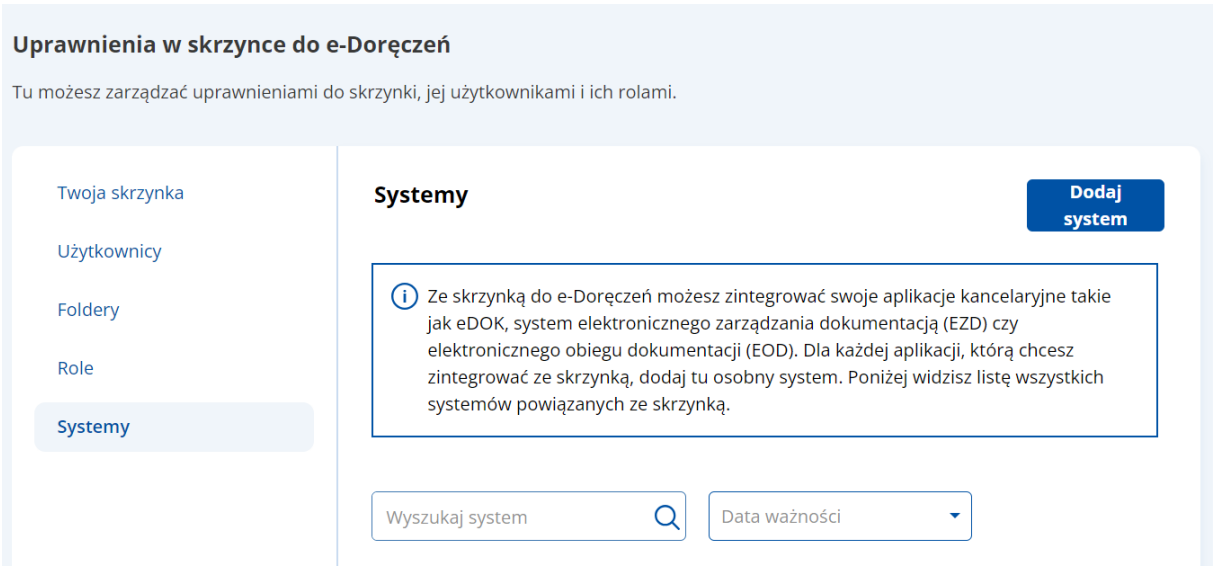
3. Aby jednoznacznie zidentyfikować podmiot, można wpisać identyfikator do atrybutu organizationIdentifier (OID = 2.5.4.97) na przykład: 2.4.5.97 = VATPL-XXX.

4. Certyfikat służy do podpisania tokena JWT zgodnie z opisem w „Instrukcji integracji dla podmiotów i integratorów EZD”. W tym kontekście nie jest używany certyfikat SSL (bez względu na to, czy użyto wildcard, czy nie).

4. Rejestracja systemu

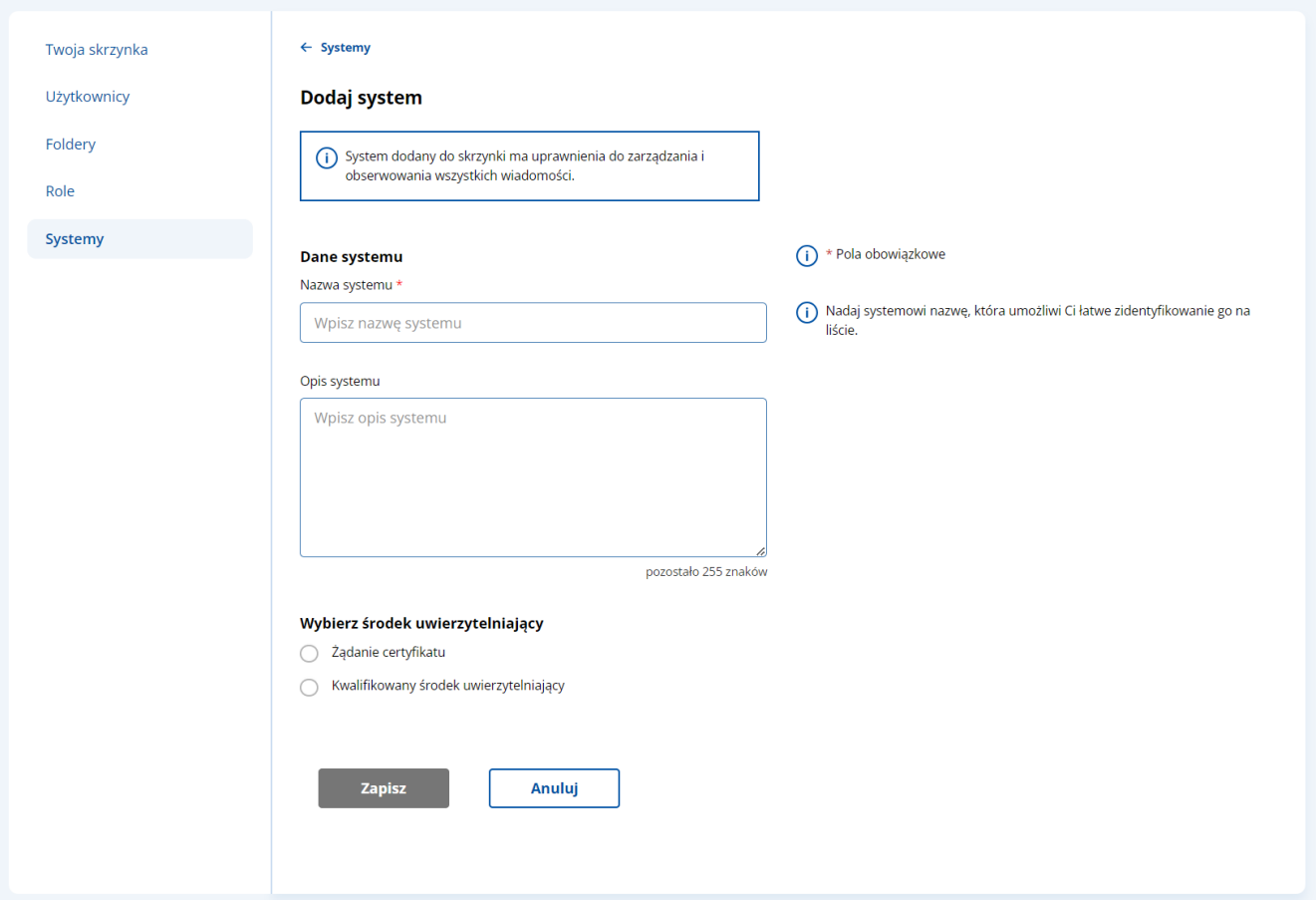
4.1. Dodanie systemu

Zaloguj się do skrzynki do e-Doręczeń w roli w właściciela lub administratora skrzynki. Przejdź do skrzynki, otwórz moduł **Uprawnienia**, a następnie zakładkę **Systemy**:

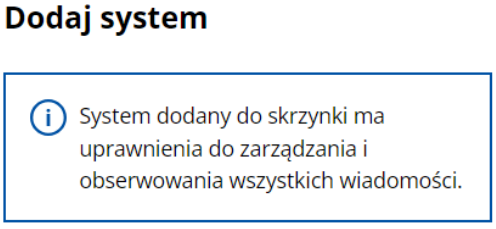


Następnie kliknij przycisk **Dodaj system**.

Tak wygląda ekran **Dodaj system**:



Na tej podstronie jest informacja o tym, że dodawany system ma uprawnienia do obserwowania wszystkich wiadomości i zarządzania nimi.



Wypełnij wymagane pole:

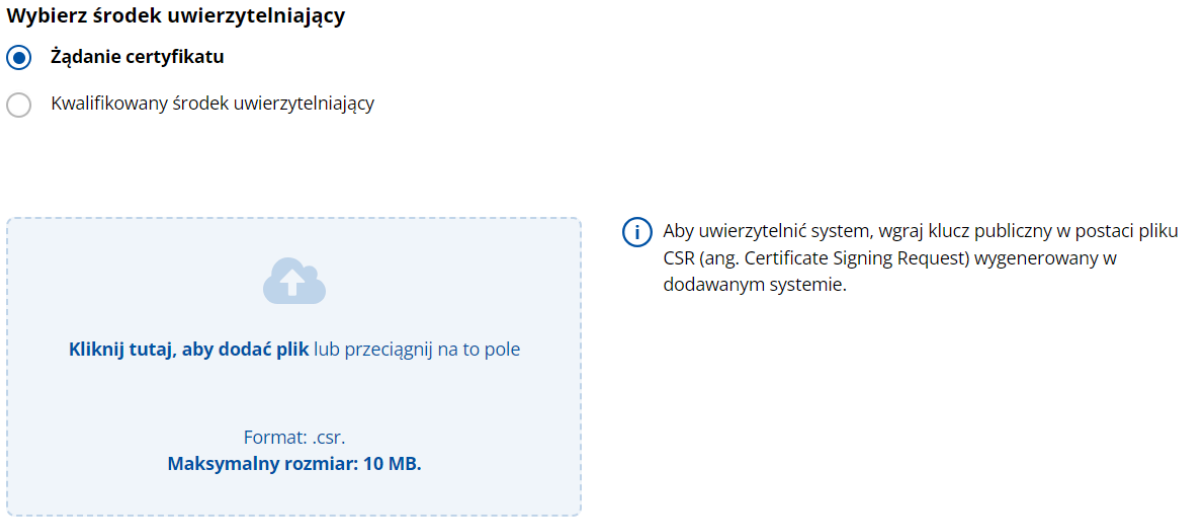
- **Nazwa systemu –** umożliwi łatwe zidentyfikowanie go na liście.

Dodatkowo możesz wypełnić pole niewymagane:

- **Opis systemu** – maksymalnie 255 znaków.

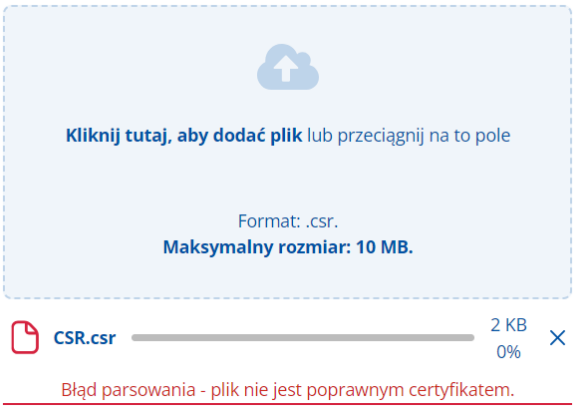
Następnie wybierz środek uwierzytelniający:

- **Żądanie certyfikatu**



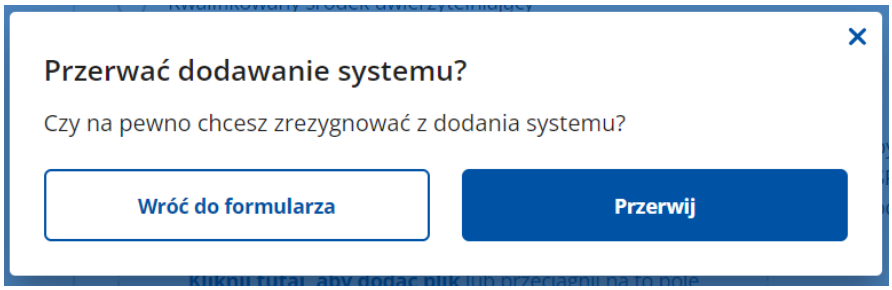
W polu dodaj pliku CSR. Nastąpi walidacja wgranego pliku. Gdy się powiedzie, zobaczysz następujący komunikat:

Jeśli plik żądania certyfikatu CSR będzie niepoprawny, wyświetli się komunikat błędu:



Możesz anulować rozpoczęty proces przyciskiem **Anuluj** na dole strony formularza:

Wtedy wyświetli następujący komunikat:

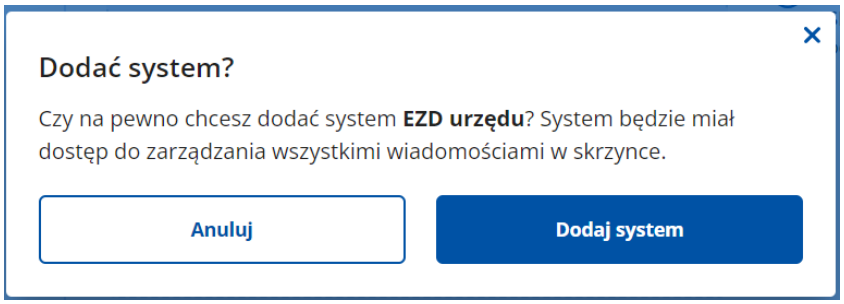


Jeśli wybierzesz przycisku **Przerwij**, powrócisz do podstrony **Systemy**.

Jeśli klikniesz **Wróć do formularza**, cofniesz się do jego edycji bez utraty dotychczas wprowadzonych informacji i możesz kontynuować dodawanie systemu.

Gdy walidacja pliku CSR będzie pomyślna, możesz kliknąć przycisk **Zapisz** na dole podstrony, aby zweryfikować certyfikat i dodać integrowany system do skrzynki.

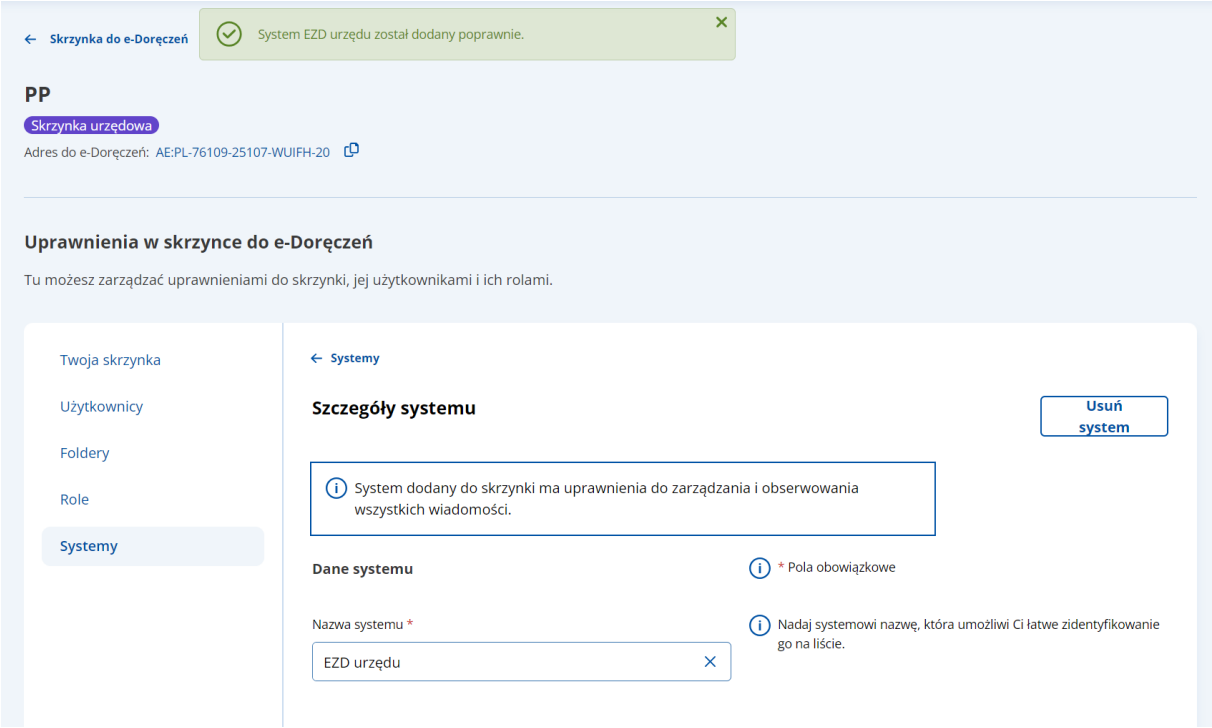
Wtedy wyświetli się następujące okno:



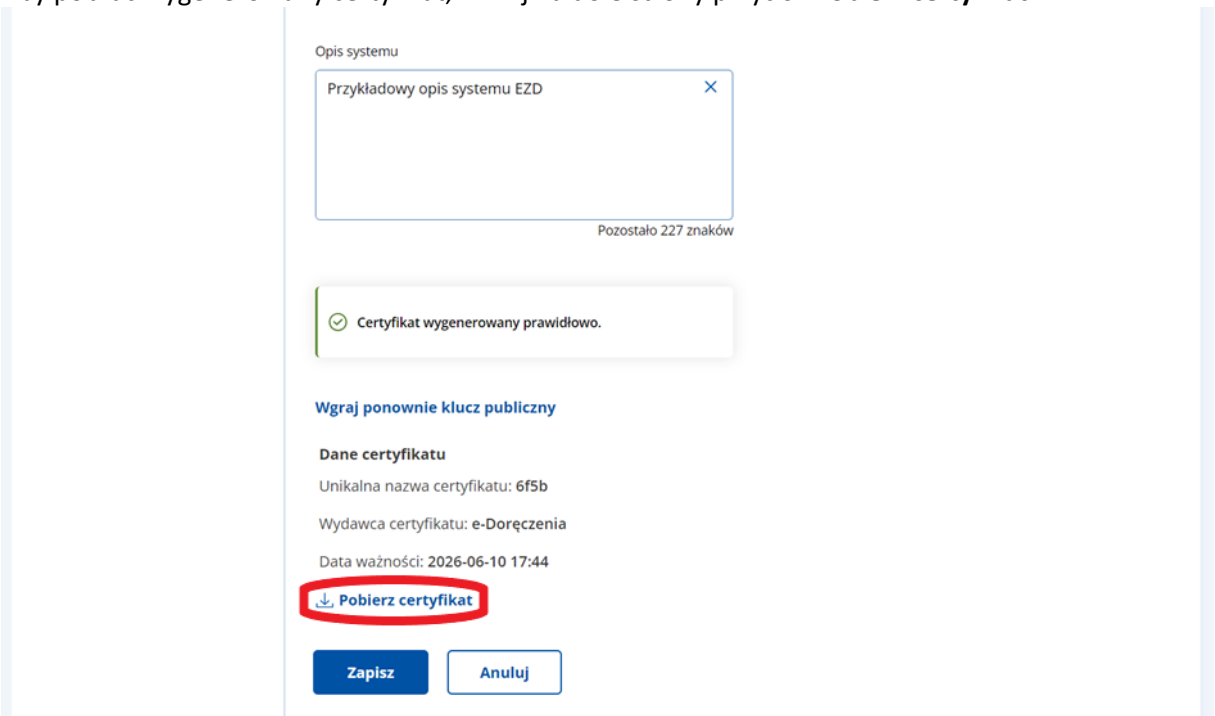
Gdy klikniesz przycisk **Dodaj system**, nastąpi weryfikacja certyfikatu i dodanie integrowanego systemu do skrzynki**.**

Jeżeli weryfikacja certyfikatu się nie powiedzie, otrzymasz również komunikat błędu. Wtedy ponownie wygeneruj plik CSR (rozdział 3).

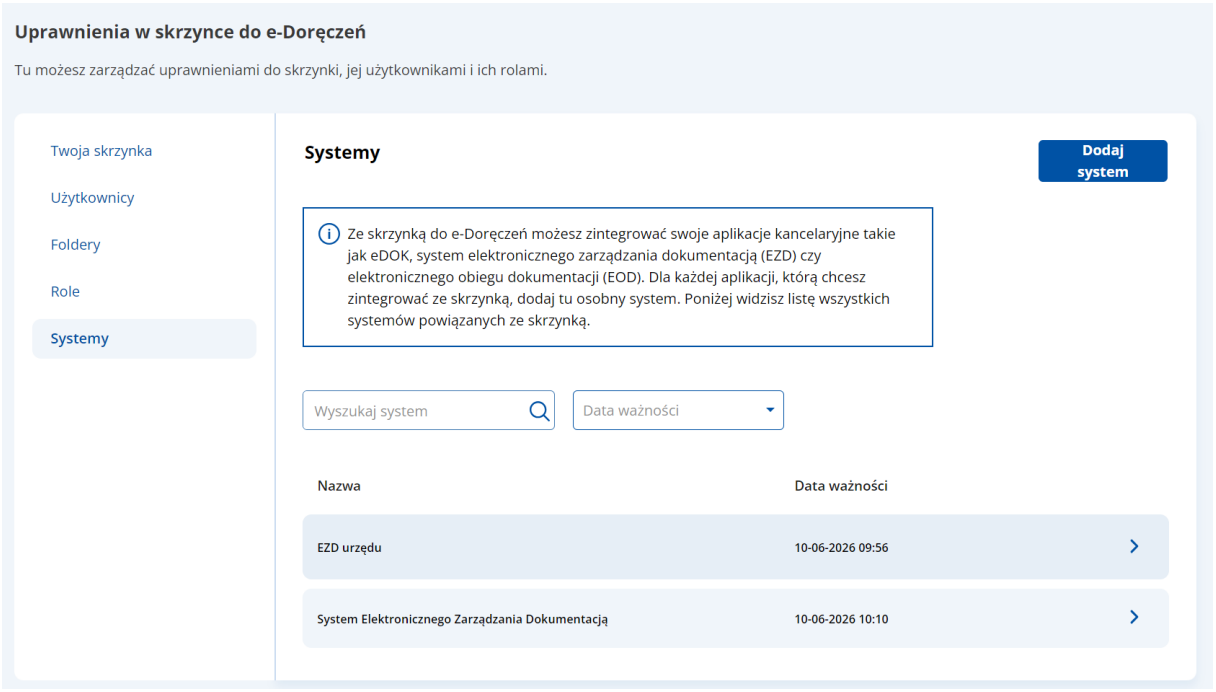
Jeśli weryfikacja przebiegnie pomyślne wyświetli się komunikat o poprawnym dodaniu systemu, a dane certyfikatu będą zamieszczone na stronie **Szczegóły systemu**:



Aby pobrać wygenerowany certyfikat, kliknij na dole strony przycisk **Pobierz certyfikat**:

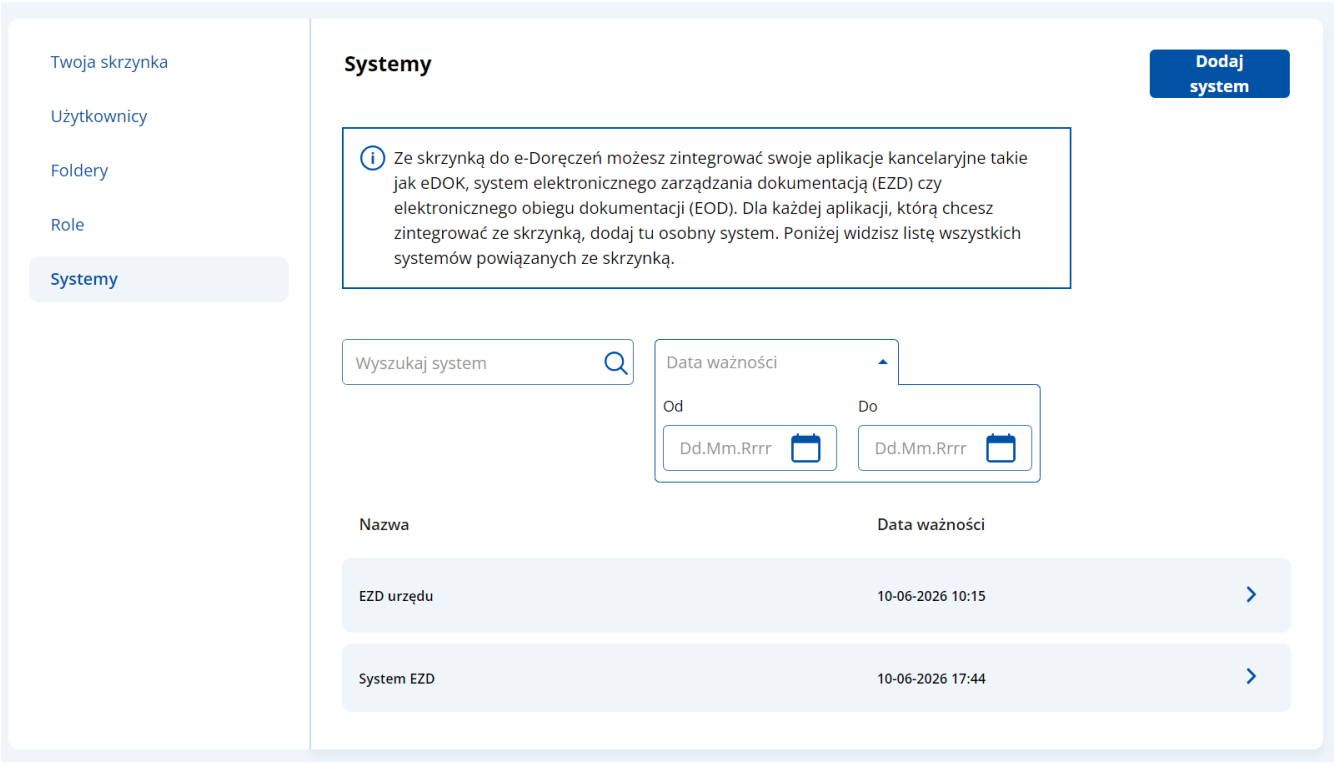


Następnie możesz wrócić na listę dodanych do skrzynki systemów, gdy klikniesz przycisk **Systemy** w menu bocznym lub na górze strony. Nowo dodany system będzie na liście:



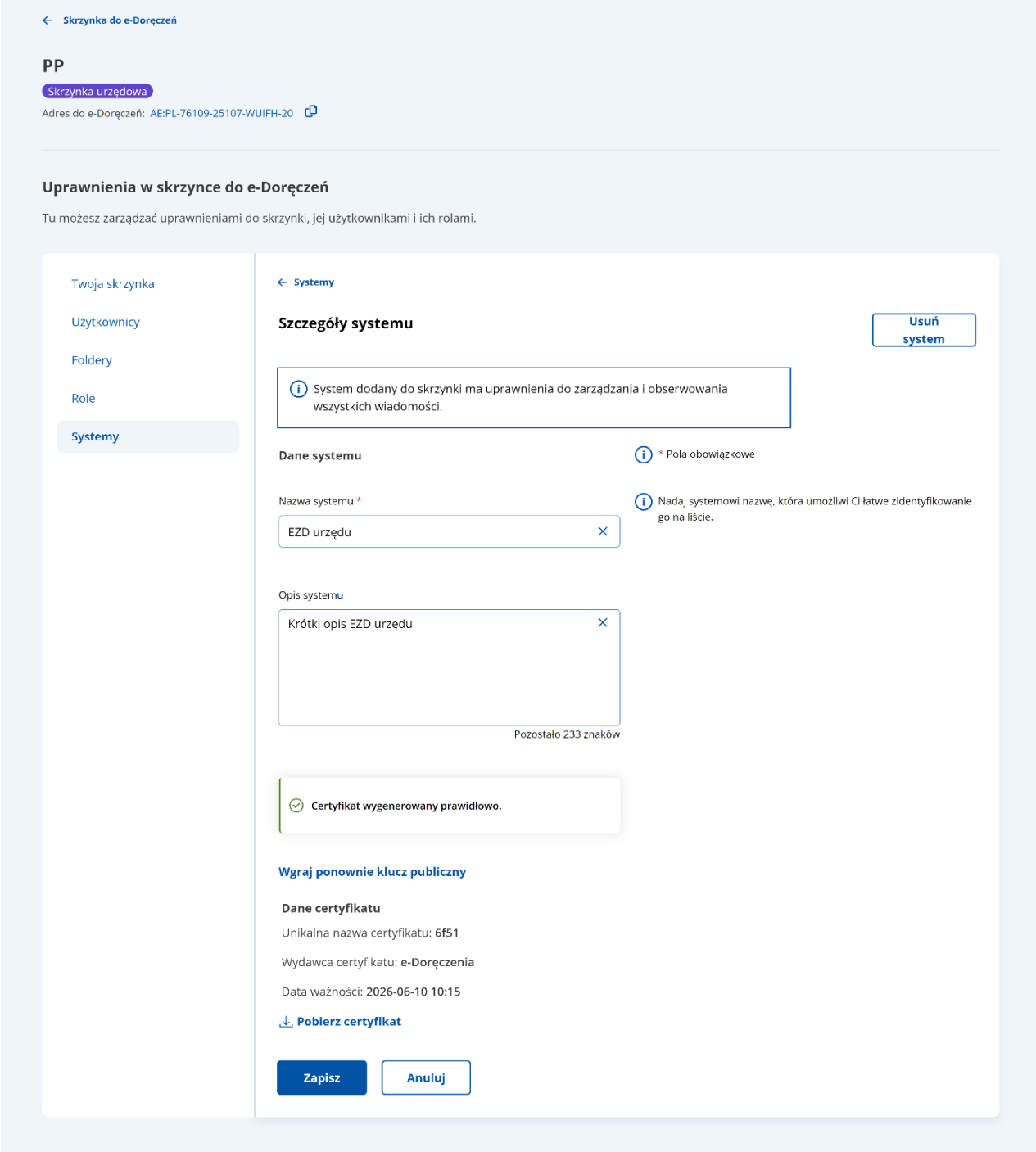
4.2. Wyszukiwanie dodanego systemu

Dodane systemy możesz przeszukiwać według nazwy lub daty ich ważności na podstronie **Systemy**:



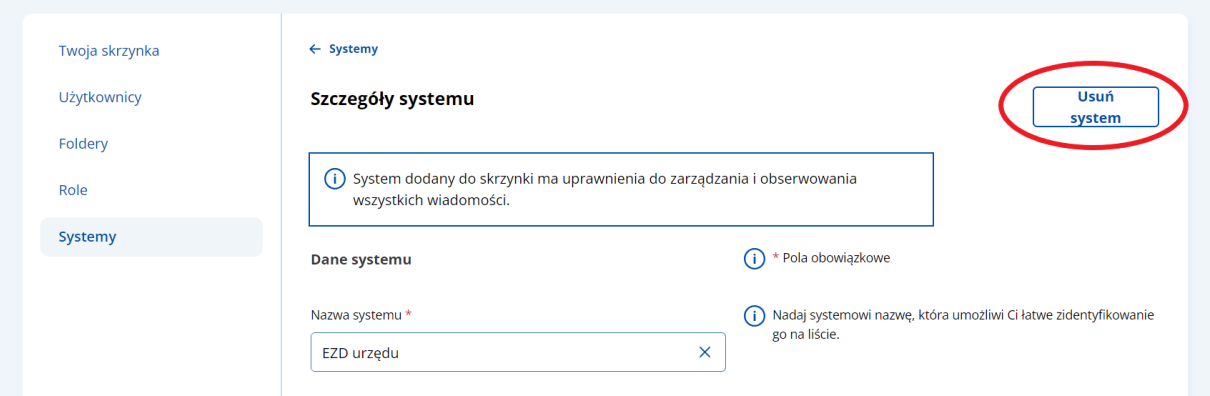
4.3. Edycja danych dodanego systemu

Gdy na liście systemów klikniesz jeden z systemów, przejdziesz do podstrony **Szczegóły systemu**, która umożliwia wprowadzenie zmian, ponowne wgranie pliku CSR, pobranie certyfikatu i usunięcie systemu z listy systemów dodanych do tej skrzynki:

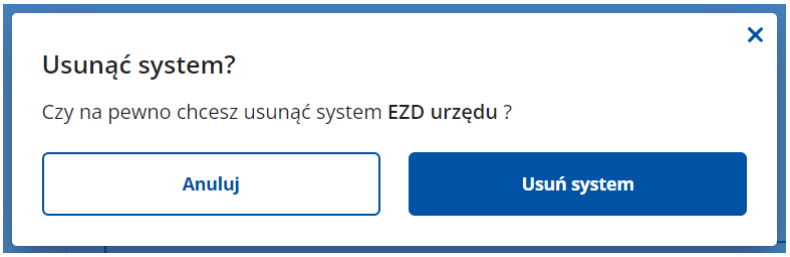


4.4. Usunięcie wybranego systemu

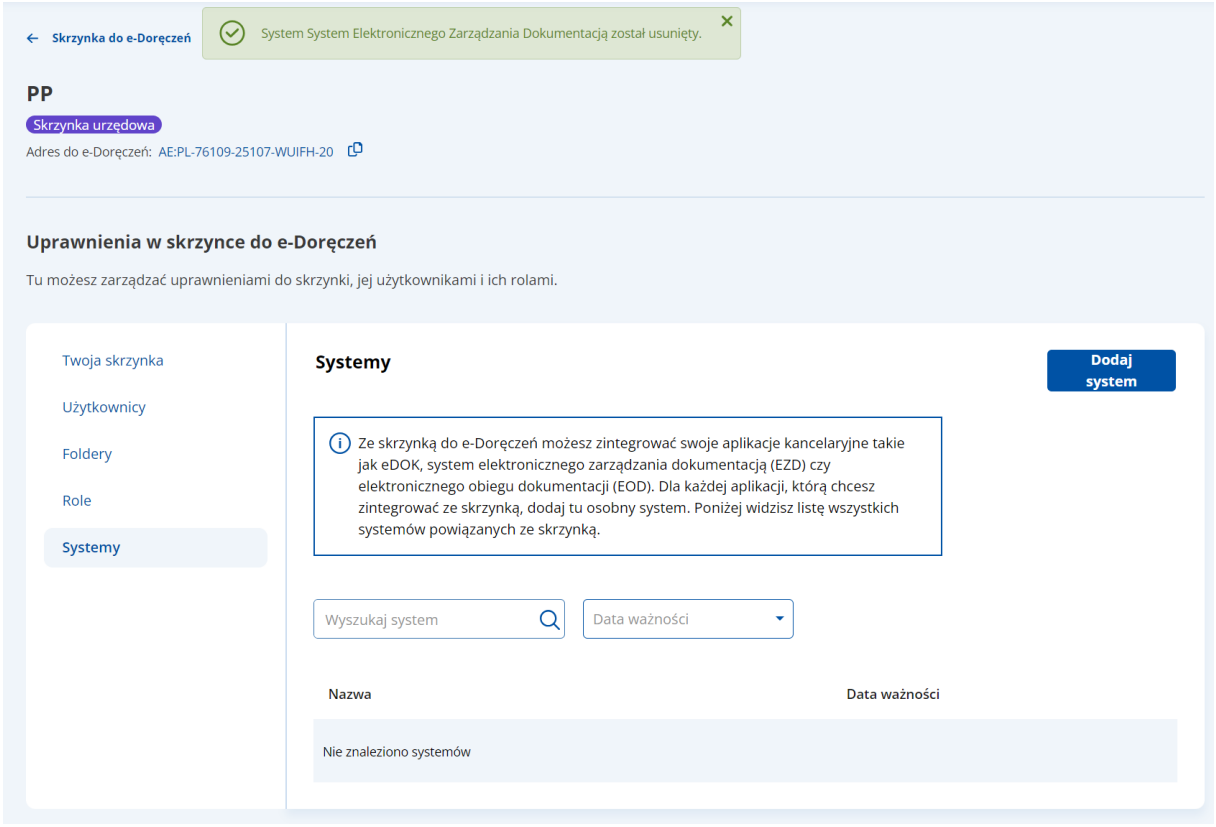
Aby usunąć system, kliknij go na liście, aby wejść w **Szczegóły systemu**. Następnie kliknij przycisk **Usuń system**:



Zostaniesz poproszony, aby potwierdzić usunięcie systemu:



Gdy potwierdzisz to przyciskiem **Usuń system**, integrowany system zostanie usunięty z listy zewnętrznych systemów zintegrowanych ze skrzynką. Wrócisz do podstrony **Systemy** z listą dodanych systemów i otrzymasz komunikat o usunięciu systemu:



W oknie **Usunąć system?** Możesz wybrać przycisk **Anuluj**, a wtedy wrócisz do podstrony **Szczegóły systemu**, która umożliwia dalszą edycję i modyfikację danych (rozdział 4.3).