**E-DORĘCZENIA ‒ INSTRUKCJA REJESTRACJI SYSTEMU ZEWNĘTRZNEGO**

**WERSJA 1.1**

Spis treści

[1. Wstęp 3](#_Toc79483813)

[2. Początek pracy 3](#_Toc79483814)

[3. Generowanie kluczy 4](#_Toc79483815)

[3.1. Generowanie klucza prywatnego 4](#_Toc79483816)

[3.2. Generowanie klucza publicznego 4](#_Toc79483817)

[3.3. Generowanie pliku żądania certyfikatu (Certificate Signing Request) 5](#_Toc79483818)

[3.4. Weryfikacja klucza prywatnego 7](#_Toc79483819)

[3.5. Weryfikacja poprawności wygenerowanego pliku CSR 8](#_Toc79483820)

[3.6. Wersje skrócone generowania pliku żądania wydania certyfikatu (CSR) 9](#_Toc79483821)

[3.6.1. UNIX 10](#_Toc79483822)

[3.6.2. LINUX 10](#_Toc79483823)

[3.6.3. WINDOWS 11](#_Toc79483824)

[3.7. Certyfikat klucza publicznego X.509 12](#_Toc79483825)

[4. Rejestracja systemu 18](#_Toc79483826)

[4.1. Dodanie systemu 18](#_Toc79483827)

[4.2. Wyszukiwanie dodanego systemu 23](#_Toc79483828)

[4.3. Edycja danych dodanego systemu 24](#_Toc79483829)

[4.4. Usunięcie wybranego systemu 25](#_Toc79483830)

# Wstęp

Skrzynkę e-Doręczeń możesz obsługiwać nie tylko za pomocą webowego interfejsu ale również za pomocą Twoich własnych systemów, na przykład systemu EZD czyli Elektronicznego Zarządzania Dokumentacją. Dla potrzeb niniejszej instrukcji wszystkie Twoje systemy będziemy nazywać systemami zewnętrznymi. System, któremu udzielisz dostępu do skrzynki może mieć uprawnienia do obserwowania i zarządzania wszystkimi Twoimi wiadomościami. W celu udzielenia dostępu do skrzynki dla Twojego systemu niezbędne jest wygenerowanie pliku CSR, który należy załączyć w procesie rejestracji. Po zweryfikowaniu przekazanego pliku CSR, system e-Doręczeń wygeneruje certyfikat X.509 i udostępni go do pobrania. Pobrany certyfikat należy zapisać w folderze, w którym znajduje się wygenerowany wcześniej plik CSR oraz certyfikat publiczny i prywatny rejestrowanego systemu.

Ostatnim krokiem jest dodanie nowego systemu uprawnionego do dostępu do Twojej skrzynki. Wszystkie powyższe kroki są szczegółowo opisane w kolejnych rozdziałach.

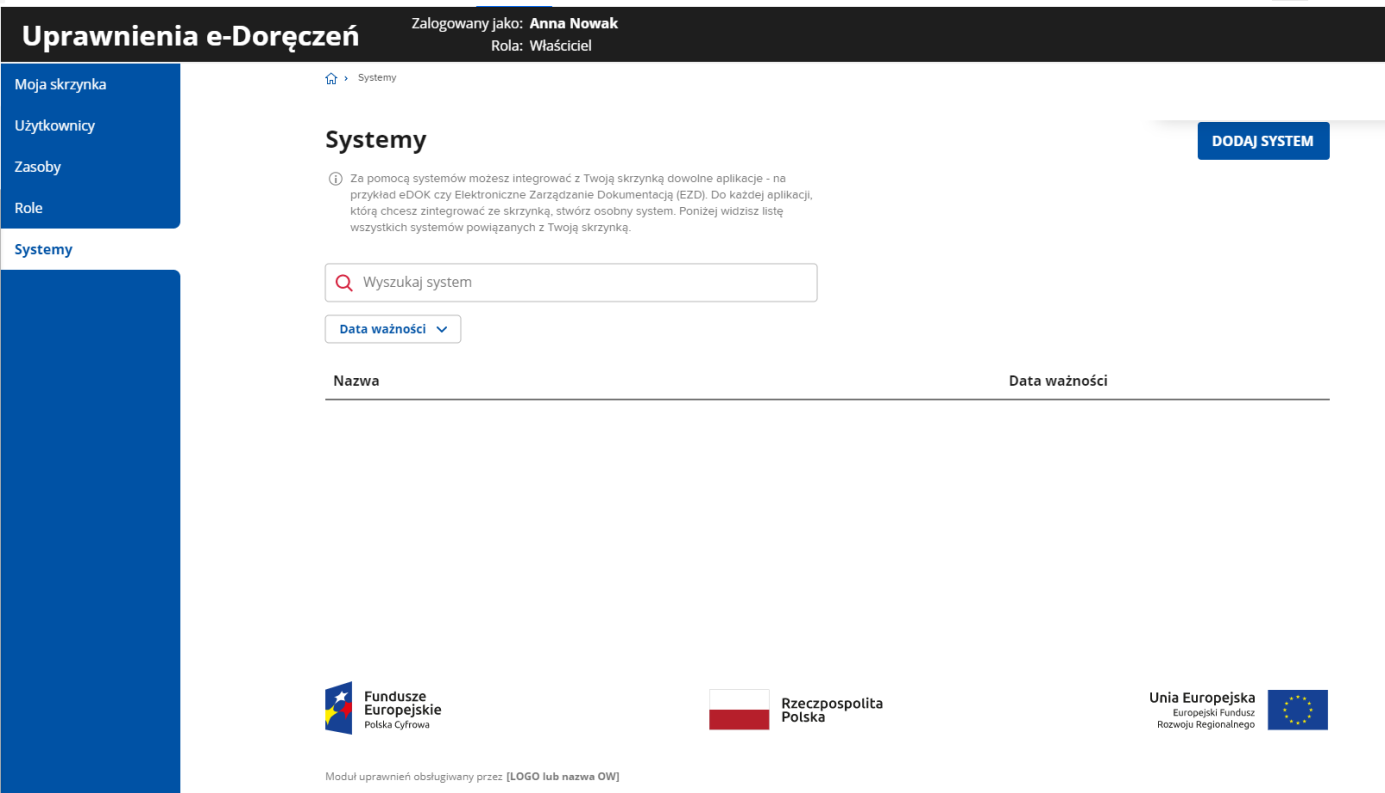
# Początek pracy

W celu rejestracji integrowanego systemu zewnętrznego ze skrzynką e-Doręczeń na środowisku testowym lub produkcyjnym użytkownik musi być zalogowany jako właściciel skrzynki.

**UWAGA:** Przeprowadzanie procesu rejestracji systemu zewnętrznego może dokonać tylko użytkownik pełniący role właściciela skrzynki.

Przed rozpoczęciem właściwego procesu rejestracyjnego niezbędne jest wygenerowanie pliku CSR. CSR (Certificate Signing Request) to żądanie podpisania certyfikatu niezbędne do utworzenia certyfikatu X.509. Plik ten generuje administrator serwera, na którym położony jest zewnętrzy system integrowany ze skrzynką e-Doręczeń.

Przed rejestracją integrowanego systemu, a po zalogowaniu do własnej skrzynki użytkownikowi ukaże się poniższy widok:



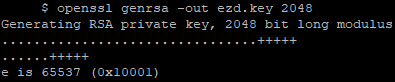
# Generowanie kluczy

Klucze prywatne i publiczne można tworzyć na wiele sposobów, ale jednym z najpopularniejszych jest narzędzie OpenSSL (oprogramowanie open source). Jest ono dostępne we wszystkich wiodących systemach operacyjnych i oferuje prosty interfejs wiersza polecenia służący do generowania kluczy.

## Generowanie klucza prywatnego

**Aby utworzyć klucz prywatny**, który będzie używany z certyfikatem, przy wykorzystaniu pakietu openSSL, należy wpisać poniższe polecenie w oknie terminala:

openssl genrsa –out ezd.key 2048



**UWAGA:** Wygenerowany klucz prywatny należy zachować w bezpiecznym miejscu i uniemożliwić dostęp do niego osobom trzecim. Należy również wykonać kopię bezpieczeństwa tego pliku, jest on niezbędny do późniejszego używania certyfikatu. Powtórne wygenerowanie identycznego klucza prywatnego nie jest możliwe, zatem jego utrata automatycznie uniemożliwia korzystanie z certyfikatu.

## Generowanie klucza publicznego

Do utworzenia **klucza publicznego**na podstawie wcześniej wygenerowanego klucza prywatnego, służy następujące polecenie:

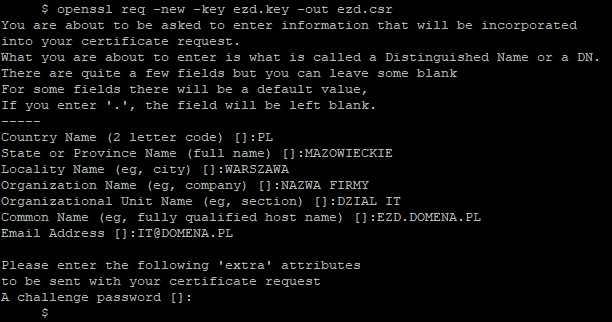
openssl rsa –in ezd.key –pubout –out ezd\_public.key

zrzut ekranu z konsolą.

## Generowanie pliku żądania podpisania certyfikatu (Certificate Signing Request)

Aby utworzyć **plik żądania podpisania certyfikatu (CSR)**na podstawie wcześniej wygenerowanego klucza prywatnego, należy użyć polecenia:

openssl req –new –key ezd.key –out ezd.csr

****

W trakcie tworzenia pliku CSR, należy podać następujące informacje:

1. **Country Name (C)** ‒ należy podać dwuliterowy kod kraju [PL].
2. **State or Province Name (ST)** ‒ należy podać nazwę województwa, w którym mieści się siedziba firmy [Wojewodztwo].
3. **Locality Name (L)** ‒ należy podać nazwę miejscowości, w której mieści się siedziba firmy [Miejscowosc].
4. **Organization Name (O)** ‒ należy podać pełną i dokładną nazwę firmy, musi się ona zgadzać z nazwą przedstawioną w dokumentach rejestrowych, czyli w rejestrze CEIDG lub KRS [Nazwa Firmy].
5. **Organizational Unit Name (OU)** ‒ pole nieobowiązkowe, opcjonalnie można podać nazwę działu firmy odpowiedzialnego za wdrożenie certyfikatu [Nazwa Dzialu IT].
6. **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].
7. **Email Address [E]** ‒ pole nieobowiązkowe.
8. Po przejściu przez tę procedurę pojawią się jeszcze dwa dodatkowe pytania (extra attributes). Pola te należy pozostawić puste i zatwierdzić klawiszem Enter:

**A challenge password** ‒ należy pominąć i zatwierdzić klawiszem Enter.

**An optional company name** *‒* należy pominąć i zatwierdzić klawiszem Enter.

**UWAGA:** Podczas udzielania odpowiedzi na pytania NIE NALEŻY używać polskich znaków.

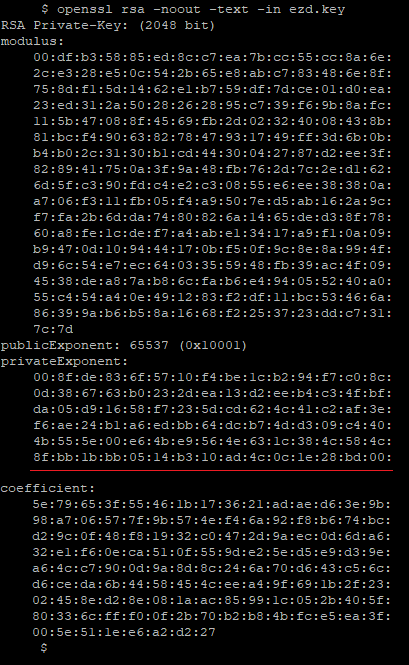
Plik CSR jest plikiem tekstowym, na przykład o takiej zawartości:



## Weryfikacja klucza prywatnego

Aby zweryfikować poprawność pliku, który zawiera klucz prywatny, należy wydać następujące polecenie:

openssl rsa –noout –text –in ezd.key



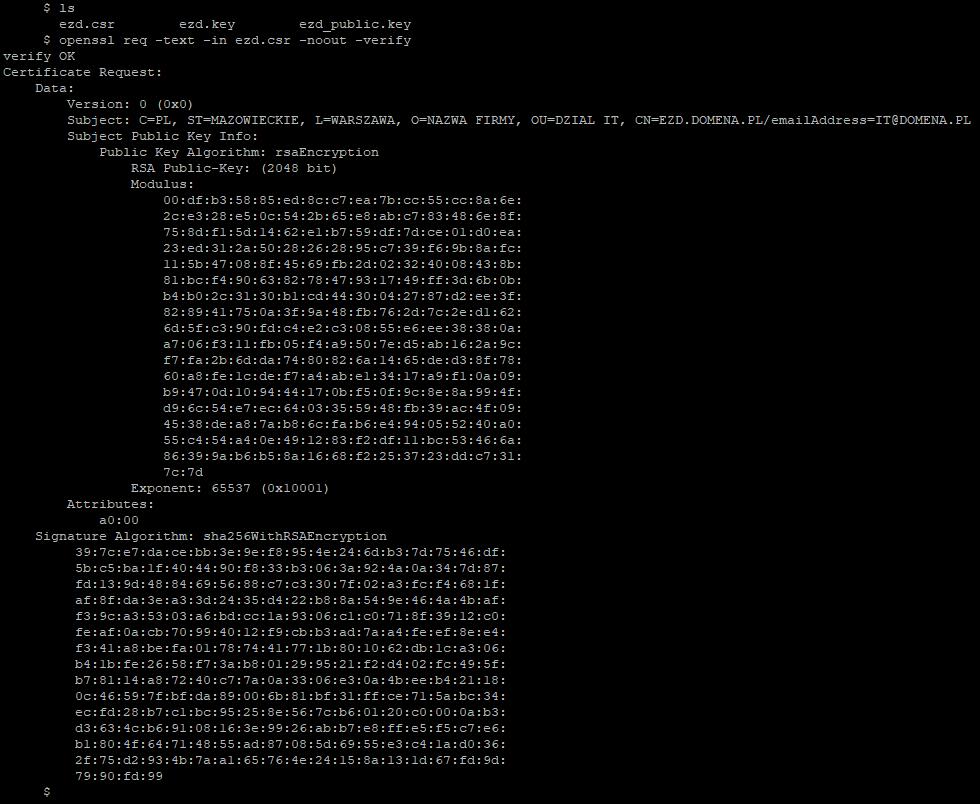
## Weryfikacja poprawności wygenerowanego pliku CSR

Gdy wydasz w konsoli polecenie ls , zobaczysz wszystkie otrzymane dotychczas pliki:

* ezd.key - plik klucza prywatnego
* ezd\_public.key - plik klucza publicznego
* ezd.csr - plik **żądania certyfikatu**

Gdy wydasz polecenie openssl req –text –in ezd.csr –noout –verify,sprawdzisz poprawność pliku CSR.

Na poniższym przykładzie weryfikacja przebiegła prawidłowo.

Dodatkowo widać wszystkie atrybuty wprowadzone podczas tworzenia pliku CSR i informację o kluczu publicznym razem z sygnaturą algorytmu.

Poprawność pliku CSR zostanie sprawdzona podczas rejestracji integrowanego systemu. Proces opisany został w rozdziale 4.1.

## Wersje skrócone generowania pliku 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, musi się ona zgadzać z nazwą przedstawioną w dokumentach rejestrowych, czyli w rejestrze CEIDG lub KRS [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 podaj nazwę domeny w postaci [\*.domena.pl].

**Email Address [E]** ‒ pole nieobowiązkowe.

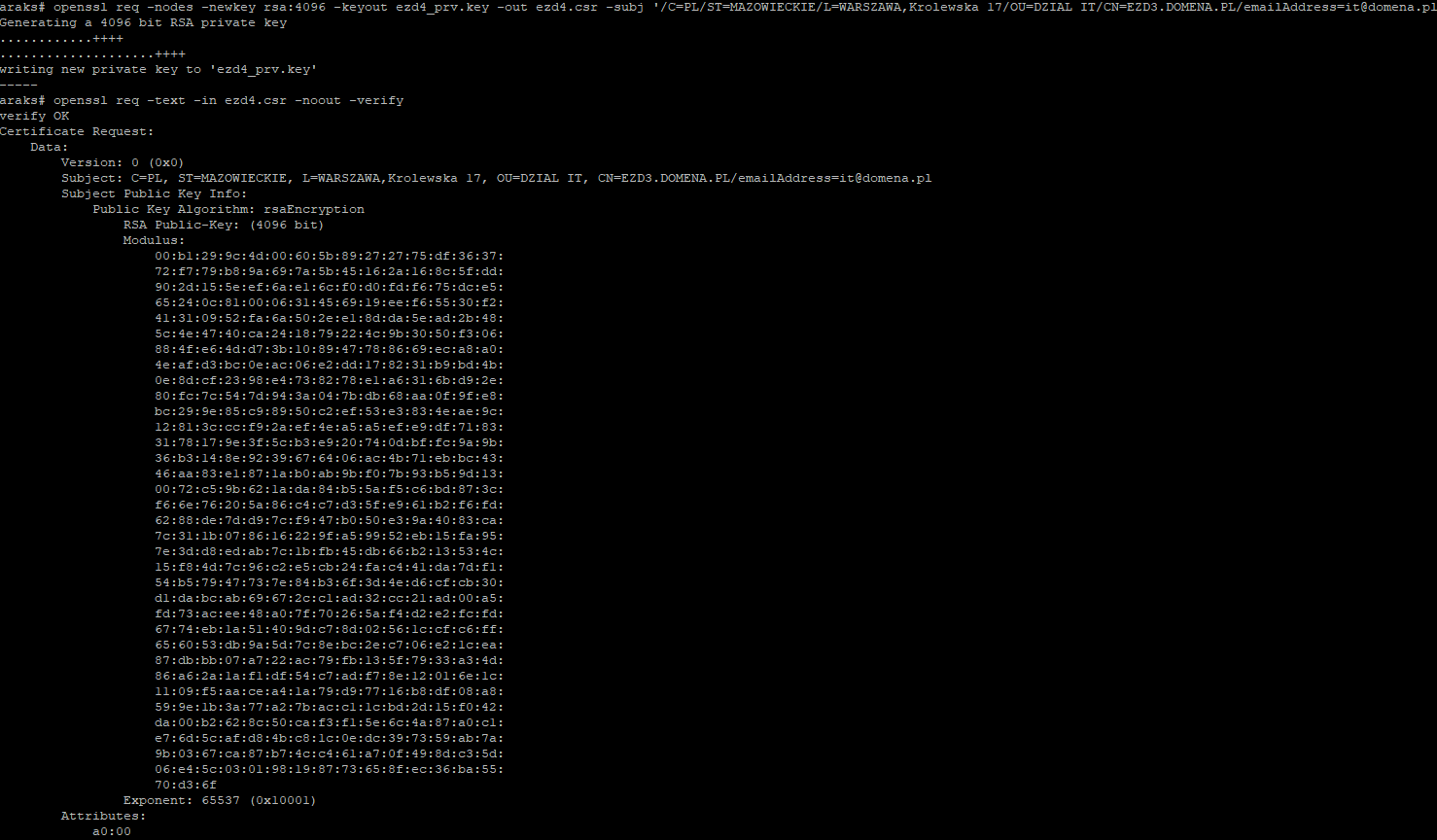
1. Instrukcja utworzenia pliku CSR:

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

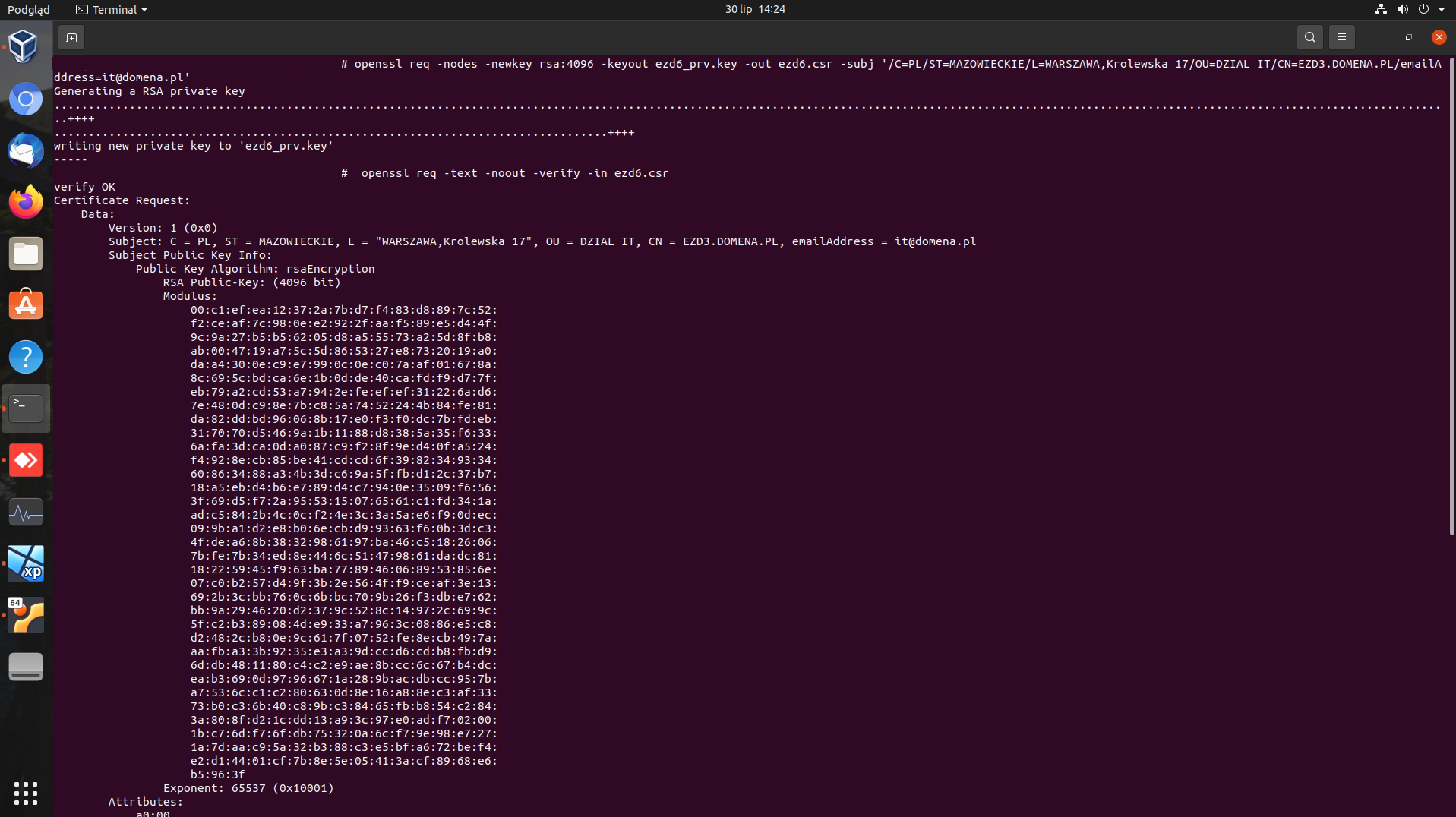
1. Instrukcja weryfikacji utworzonego pliku CSR:

openssl req –text –in ed\_2048.csr –noout -verify

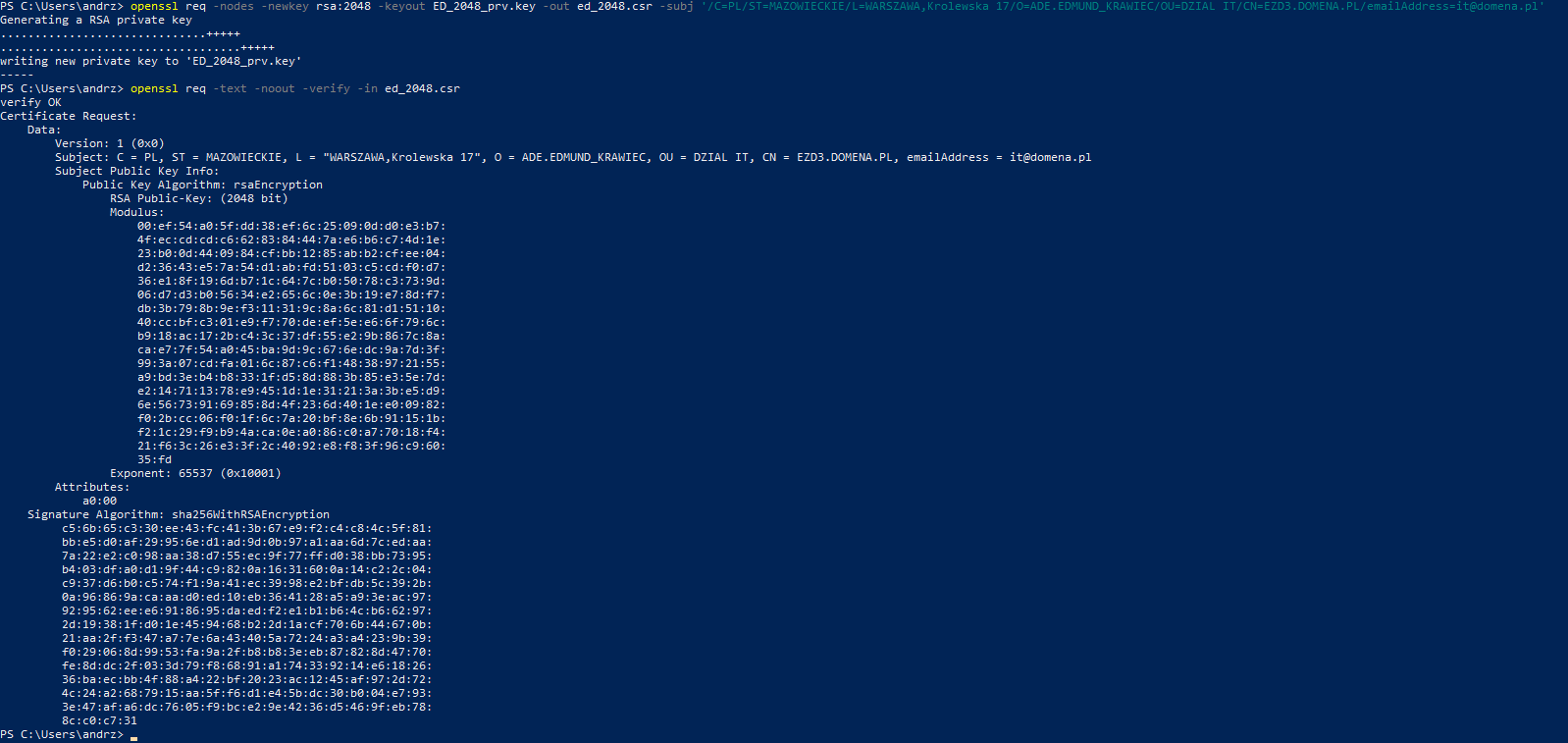
## UNIX



## LINUX



## WINDOWS



## 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, podpisów

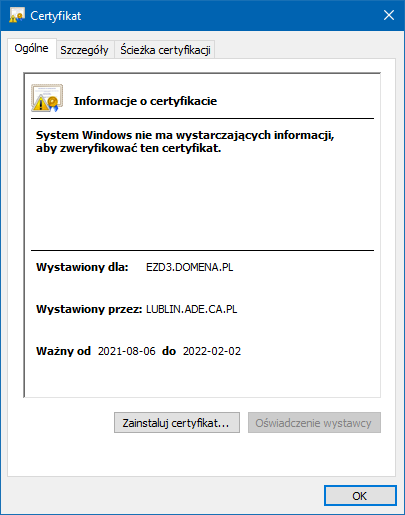
openssl verify -verbose -trusted CA.crt ed\_2048.crt

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, aby sprawdzić zgodności certyfikatu i klucza.

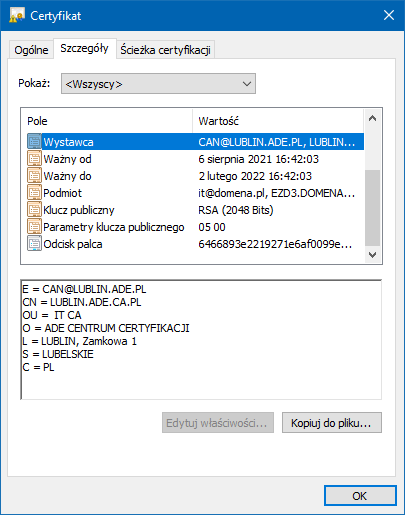
openssl x509 -noout -modulus -in ed\_2048.crt | openssl md5

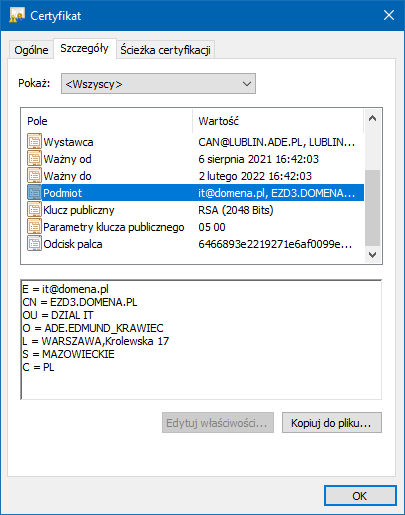
openssl rsa -noout -modulus -in ed\_2048\_prv.key | openssl md5

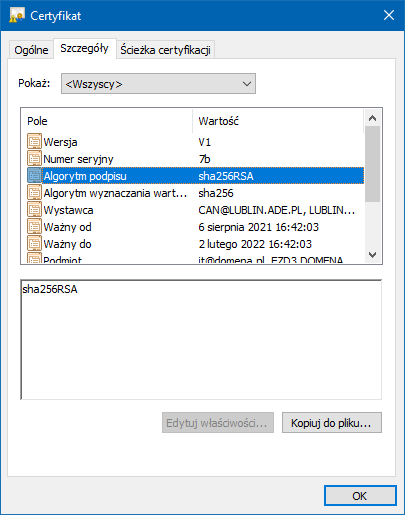
Poniżej informacje uzyskane po otworzeniu certyfikatu w systemie Windows.

Informacje o wystawcy certyfikatu:

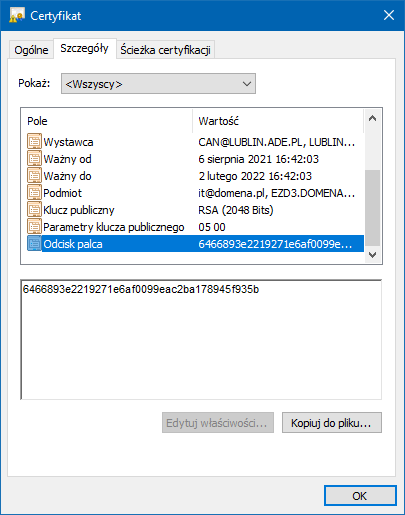
Informacje o podmiocie, dla którego został wystawiony certyfikat, na podstawie danych zawartych w pliku żądania certyfikatu:



Informacje o algorytmie podpisu:

I

Informacje o odcisku palca certyfikatu:



* Generowanie przez urząd certyfikacji (Centrum Certyfikacji) certyfikatu x509 dla podmiotu z wykorzystaniem pliku 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 x509 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

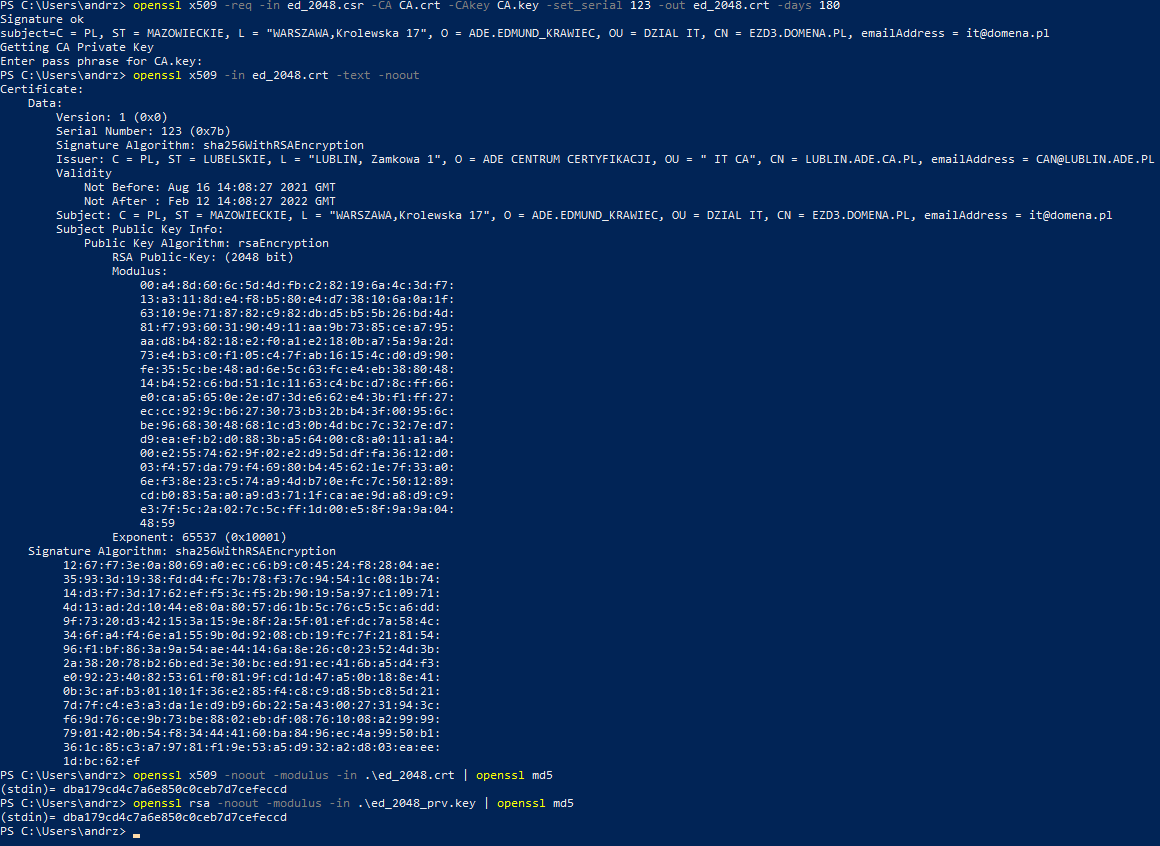
* Weryfikacja certyfikatu, podpisów:

openssl verify -verbose -trusted CA.crt ed\_2048.crt

* Poniżej dwa polecenia, które wyświetlają sumy kontrolne md5 certyfikatu i klucza. Sumy kontrolne można porównać, aby sprawdzić zgodność certyfikatu i klucza.

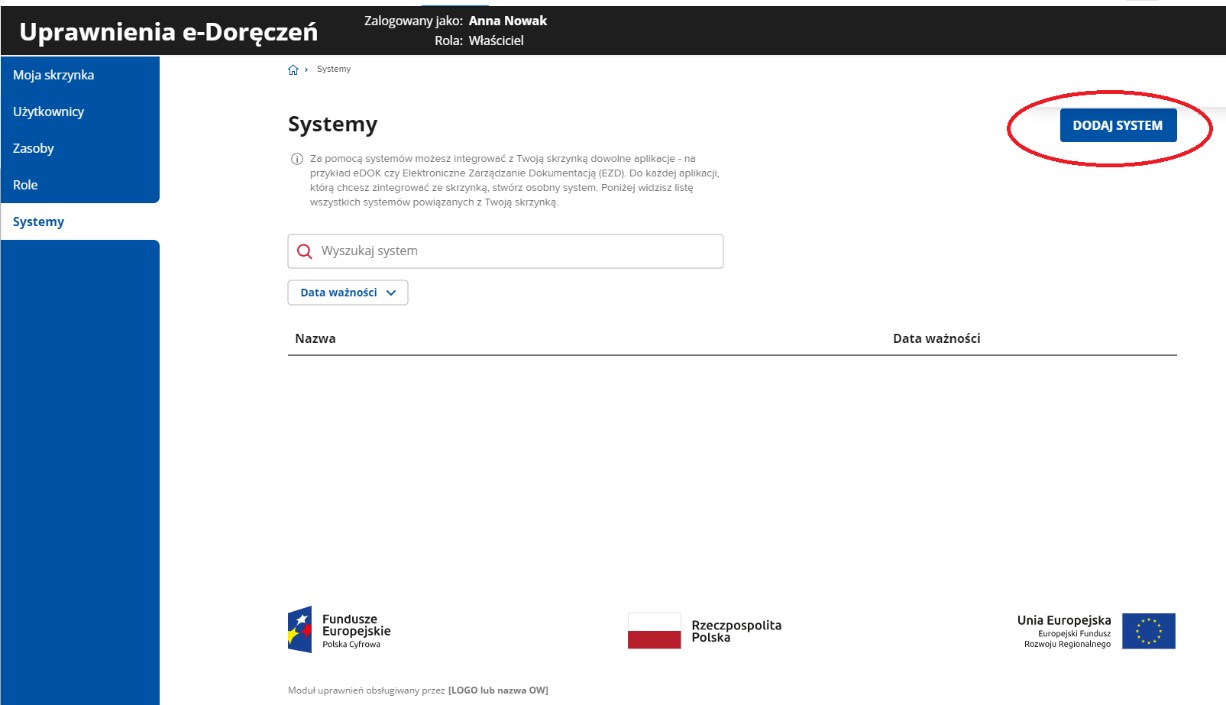
openssl x509 -noout -modulus -in .\ed\_2048.crt | openssl md5

openssl rsa -noout -modulus -in .\ed\_2048\_prv.key | openssl md5

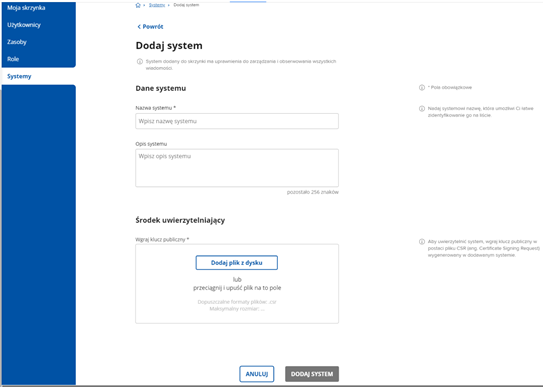


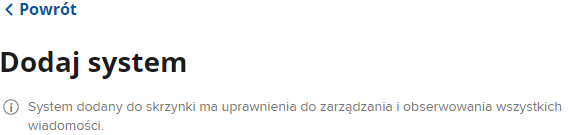
# Rejestracja systemu

## Dodawanie systemu

Rejestrację integrowanego systemu rozpocznij od zalogowania się do systemu e-Doręczeń w roli w właściciela skrzynki. Otworzy się strona z widokiem zakładki Systemy.

Następnie naciśnij przycisk Dodaj system w prawym górnym rogu ekranu. Przejedziesz do strony Dodaj system.



Zobaczysz informację, że system dodawany do skrzynki ma uprawnienia do zarządzania i obserwowania wszystkich wiadomości.

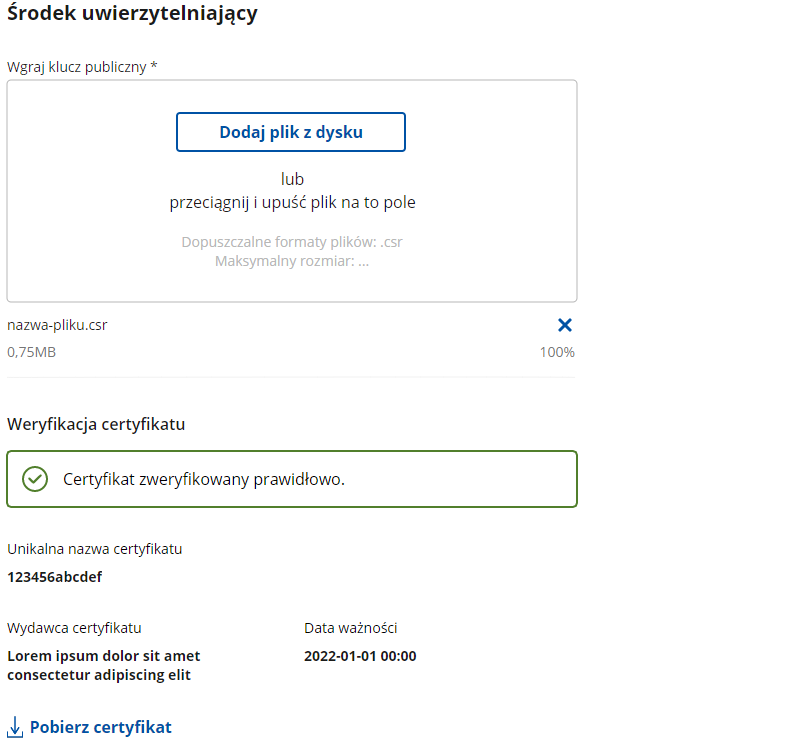
Wprowadź wymagane informacje:

* **Nazwę systemu**, która umożliwi łatwe zidentyfikowanie go na liście;
* **Wgraj Klucz publiczny**, jako środek uwierzytelniający ‒ wgraj klucz publiczny w postaci pliku CSR wygenerowany w dodawanym systemie (opis przygotowania pliku znajduje się w rozdziale 3 instrukcji).

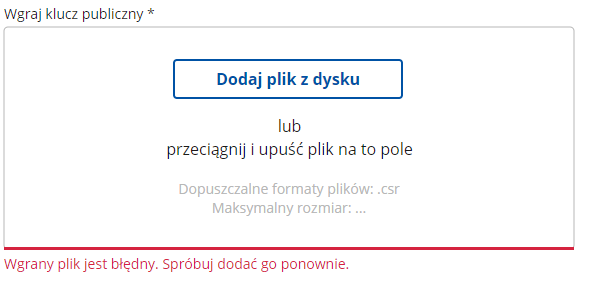
Dodatkowo w polu Opis systemu możesz wprowadzić krótki opis systemu, maksymalnie 256 znaków.

Pliku CSR jest weryfikowany – dostaniesz informację o tym, czy proces weryfikacji przebiegł prawidłowo.

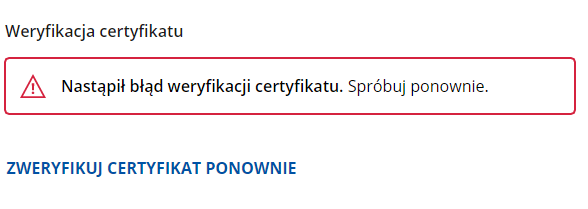
Jeśli tak, system tworzy certyfikat X.509. Kliknij Pobierz certyfikat, aby go pobrać.



Jeśli nie, zobaczysz komunikat o tym, że plik jest błędny.



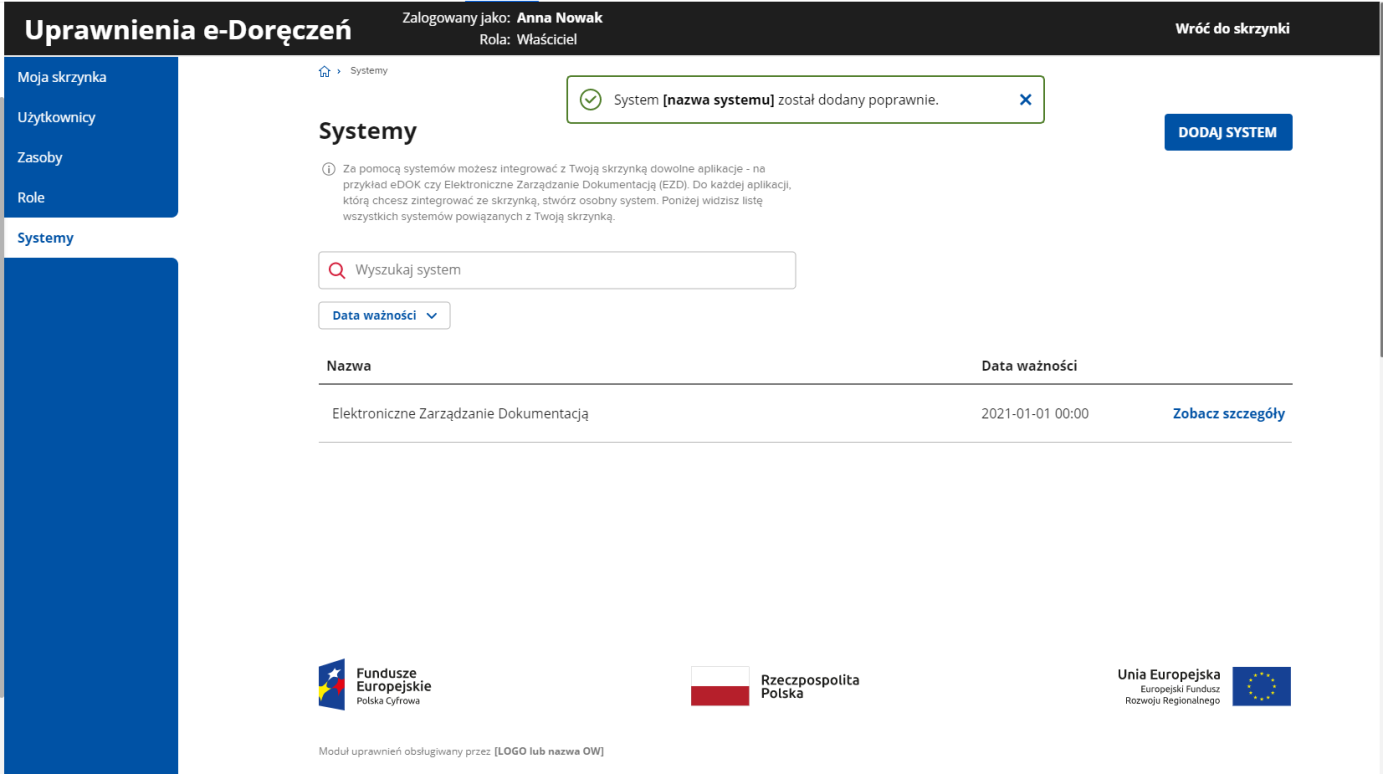
Jeśli wystąpi błąd podczas weryfikacji, również zobaczysz komunikat na ten temat.



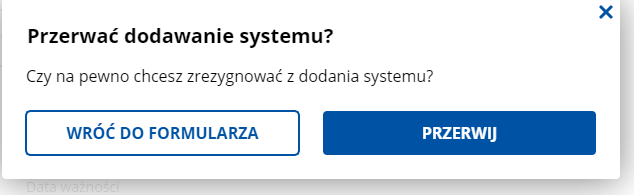
Po prawidłowym przejściu weryfikacji możesz dodać integrowany system do własnej skrzynki za pomocą przycisku: Dodaj system, któryznajduje się na dole strony, lub możesz anulować proces przyciskiem Anuluj.



Jeśli klikniesz przycisk Dodaj system, dodasz system do listy już zintegrowanych systemów zewnętrznych i wrócisz do zakładki Systemy,w której jest lista dodanych systemów. Zobaczysz też komunikat o poprawnym dodaniu systemu.



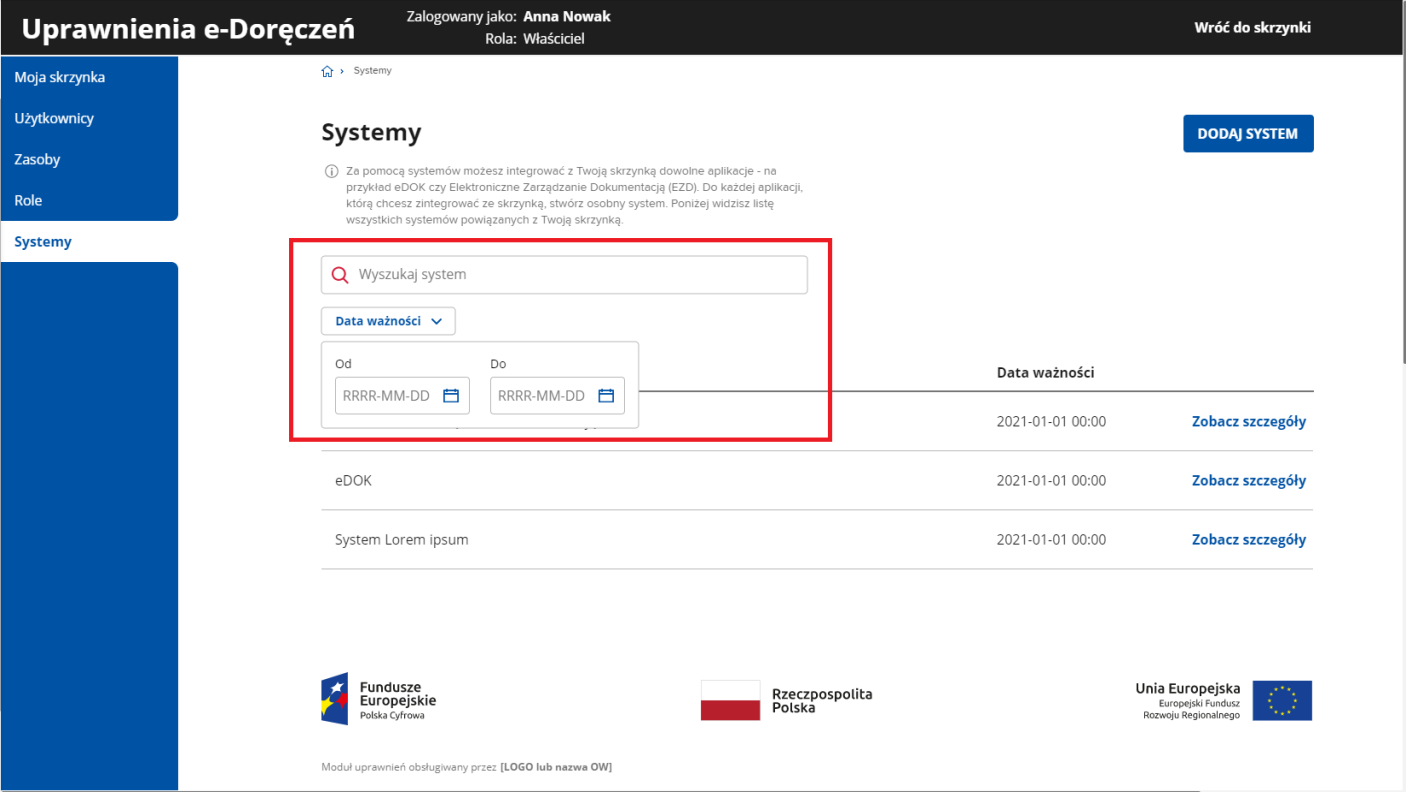
Po naciśnięciu przycisku Anuluj wyświetli się pytanie, czy chcesz przerwać dodawanie systemu.



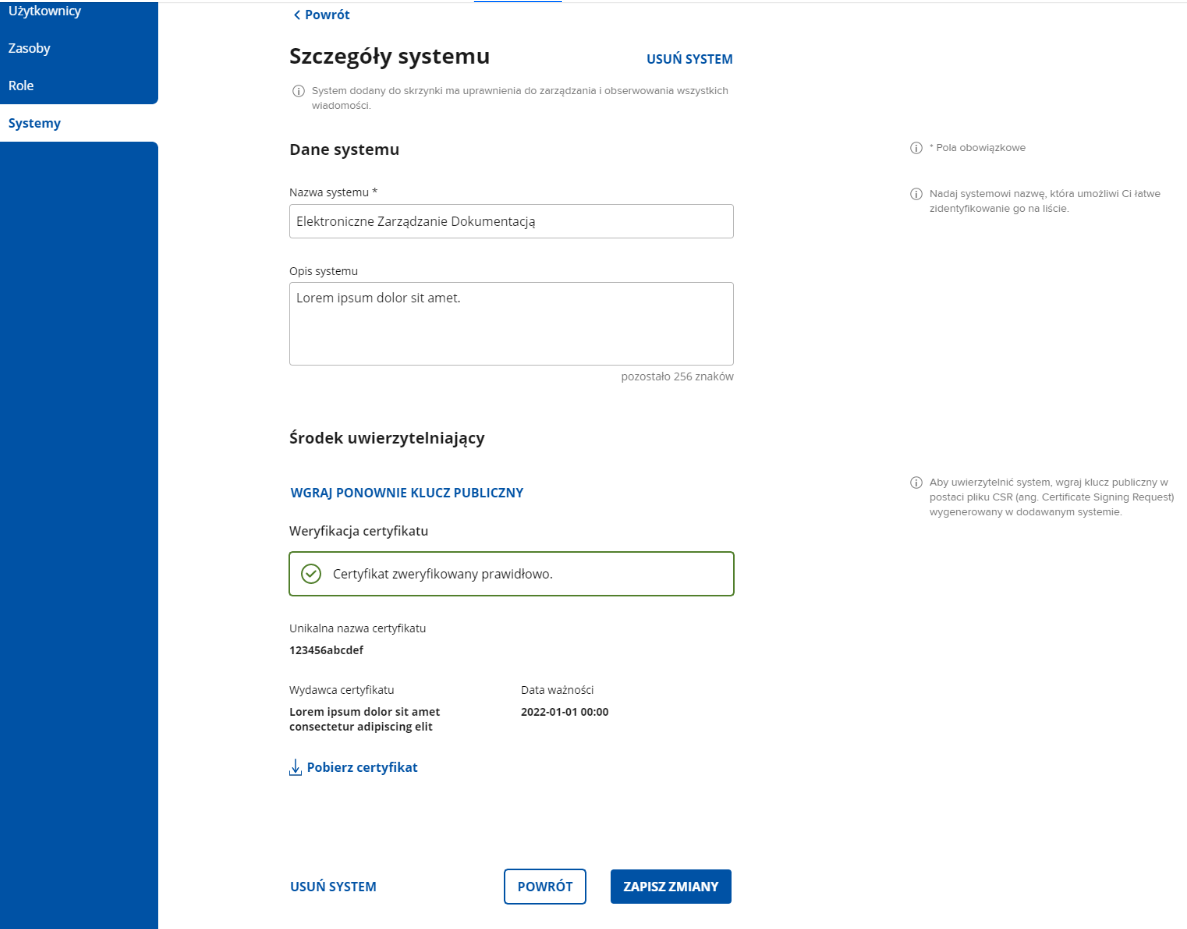
Jeśli klikniesz Wróć do formularza, cofniesz się do ekranu edycji.

Jeśli klikniesz Przerwij proces zostanie przerwany i wrócisz do strony Systemy**,** na której jest informacja o już dodanych systemach.

## Wyszukiwanie dodanego systemu

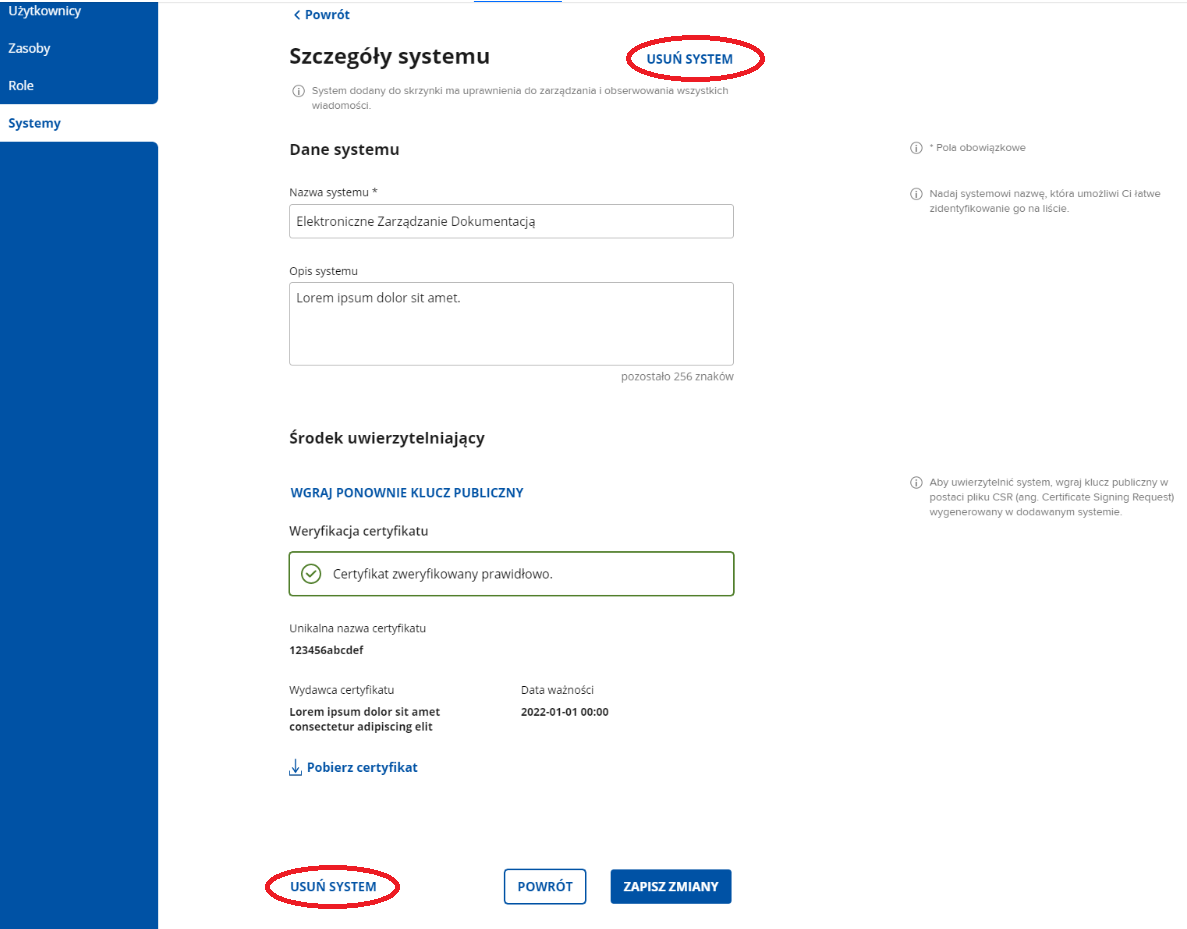
Aby wyszukać system, wejdź w zakładkę Systemy. Dodanych systemów możesz szukać po ich nazwach lub/i po dacie ich ważności (podaj zakres dat).

## Edycja danych dodanego systemu

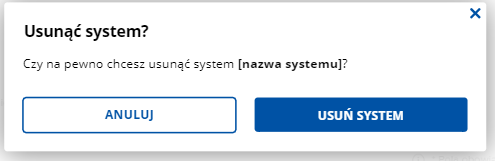
Gdy klikniesz przycisk Zobacz szczegóły, który znajduje się obok każdego systemu na liście z prawej strony, przejdziesz do formularza. Możesz w nim wprowadzić zmiany, ponownie wgrać plik CSR, pobrać certyfikat oraz usunąć system z listy.

## Usunięcie wybranego systemu

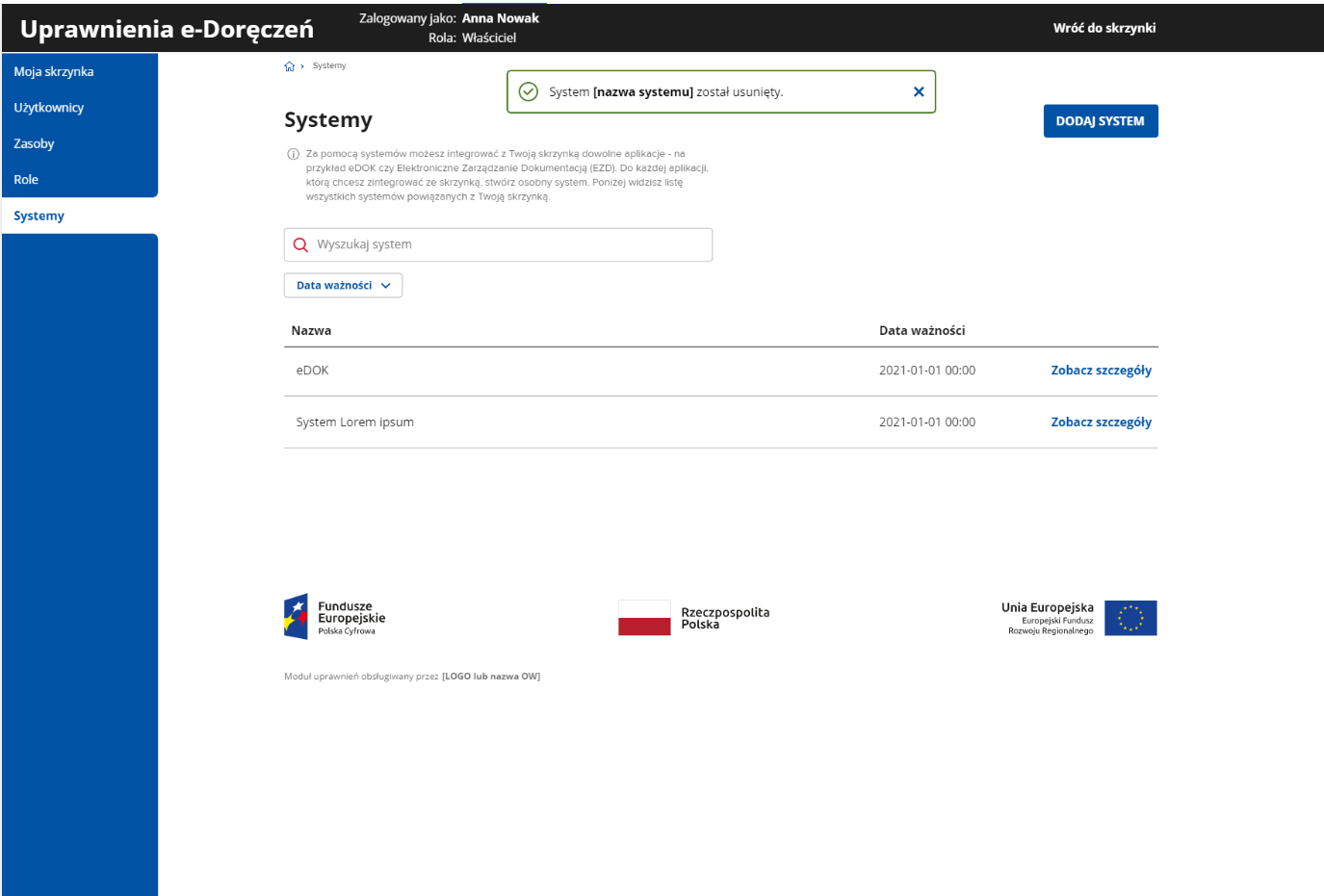
Aby usunąć konkretny system z listy, kliknij przycisk Zobacz szczegóły. Przejdziesz do formularza, w którym na górze po prawej stronie lub na dole po lewej znajdują się przyciski Usuń system.



Gdy klikniesz Usuń system, pojawi się ekran z prośbą o potwierdzenie. Potwierdź usunięcie przyciskiem Usuń system.



System zostanie usunięty z listy zintegrowanych systemów zewnętrznych i nastąpi powrót do strony Systemy.



Jeśli klikniesz Anuluj, wrócisz do formularza, w którym możesz dalej edytować informacje (rozdział 4.3).