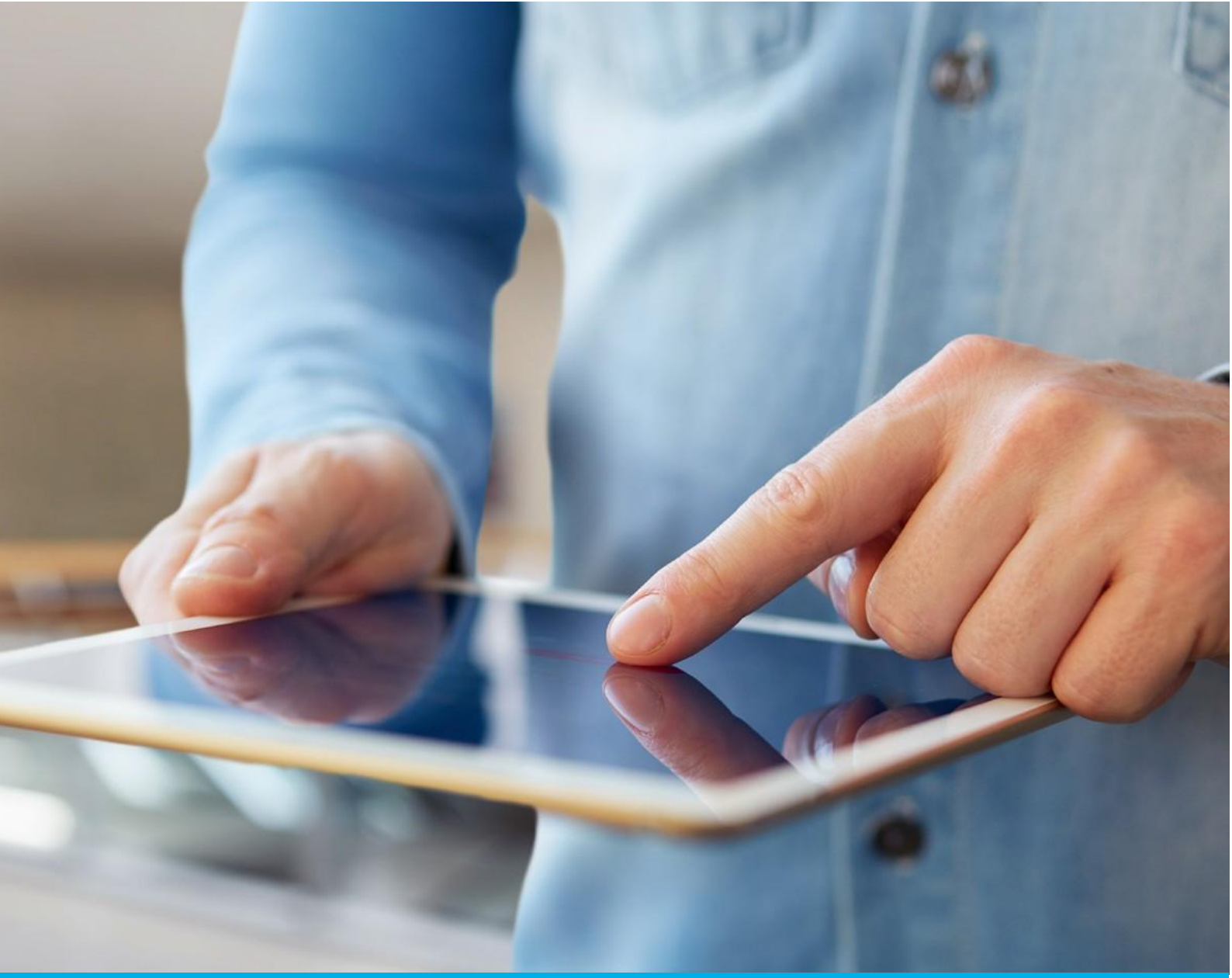


Instrukcja generowania plików CSR i PFX w OpenSSL

Wer. 1.3

asseco

Certum by asseco

Spis treści

certum.pl
infolinia@certum.pl

1. Uruchomienie narzędzia OpenSSL

Instrukcja przedstawia proces generowania CSR z wykorzystaniem narzędzia OpenSSL.

Uwaga: Zachowaj wygenerowany plik klucza prywatnego, ponieważ będzie on niezbędny do instalacji certyfikatu po jego wydaniu. Utwórz folder w znanym Ci miejscu na dysku i to w nim zapisuj wygenerowane pliki.

Instrukcja powstała z wykorzystaniem pakietu instalacyjnego dla OpenSSL, zainstalowanego w środowisku Windows. Krok instalacji OpenSSL może się różnić w zależności od systemu operacyjnego, jednak polecenia OpenSSL służące do wygenerowania CSR są uniwersalne. Niektóre systemy operacyjne posiadają OpenSSL domyślnie zainstalowany w systemie.

Pobieranie OpenSSL

Pobierz narzędzie OpenSSL w jednej z dystrybucji oferującej narzędzie w formie instalatora np. z https://slproweb.com/products/Win32OpenSSL.html. Wybierz odpowiedni plik instalacyjny, zgodny z system operacyjnym, na których przeprowadzisz proces. Lista innych serwisów hostujących instalatory OpenSSL jest umieszczona pod adresem: https://wiki.openssl.org/index.php/Binaries.

Uwaga: Zalecamy korzystanie z rekomendowanych przez zespół OpenSSL pakietów instalacyjnych. Produkty rekomendowane deweloperów OpenSSL posiadają w opisie poniższy komentarz: [Recommended for users by the creators of OpenSSL].

Instalacja OpenSSL i przygotowanie do pracy

- Uruchom pobrany pakiet instalacyjny OpenSSL
- Przejdź przez kreator instalacji. W razie potrzeby, zmień domyślne opcje wyboru
- Zakończ instalację
- Utwórz w znanym Ci miejscu na dysku folder, w którym przechowasz CSR i klucz prywatny.

Uruchomienie OpenSSL

Przejdź do folderu, w którym zainstalowany został program. W przypadku systemu Windows wartość domyślna to zwykle: C:\Program Files\OpenSSL . Uruchom plik *start.bat*.

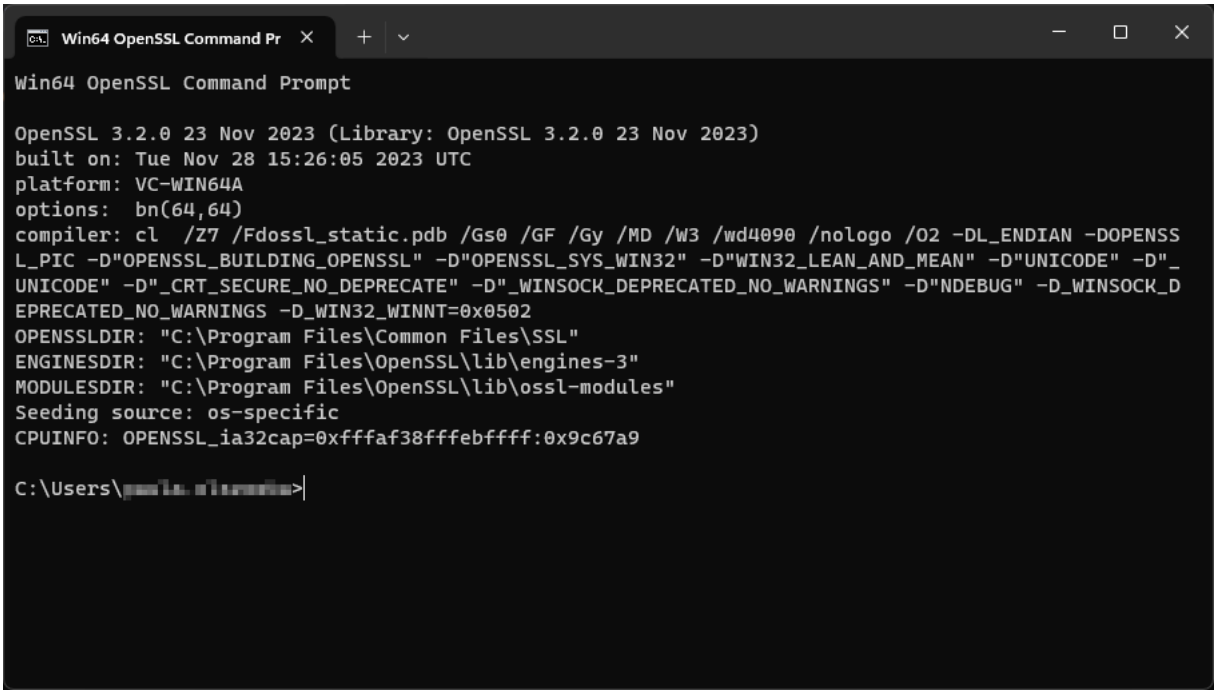
Alternatywnie, możesz uruchomić wiersz poleceń, a następnie przejść do folderu z OpenSSL poleceniem:

```
cd "ścieżka do aplikacji OpenSSL"
```

przykład:

```
cd "C:\Program Files\OpenSSL\bin".
```

Wynikowo, powinieneś mieć uruchomiony terminal z wierszem poleceń, w którym będziesz mógł wykonać komendy OpenSSL.



2. Generowanie pliku CSR i klucza prywatnego

Generacja CSR dla kluczy RSA

a) W konsoli OpenSSL użyj poniższego polecenia i zatwierdź jego wykonanie przyciskiem **Enter**:

```
openssl req -new -newkey rsa:3072 -sha256 -nodes -keyout kluczprywatny.key -out CSR.csr
```

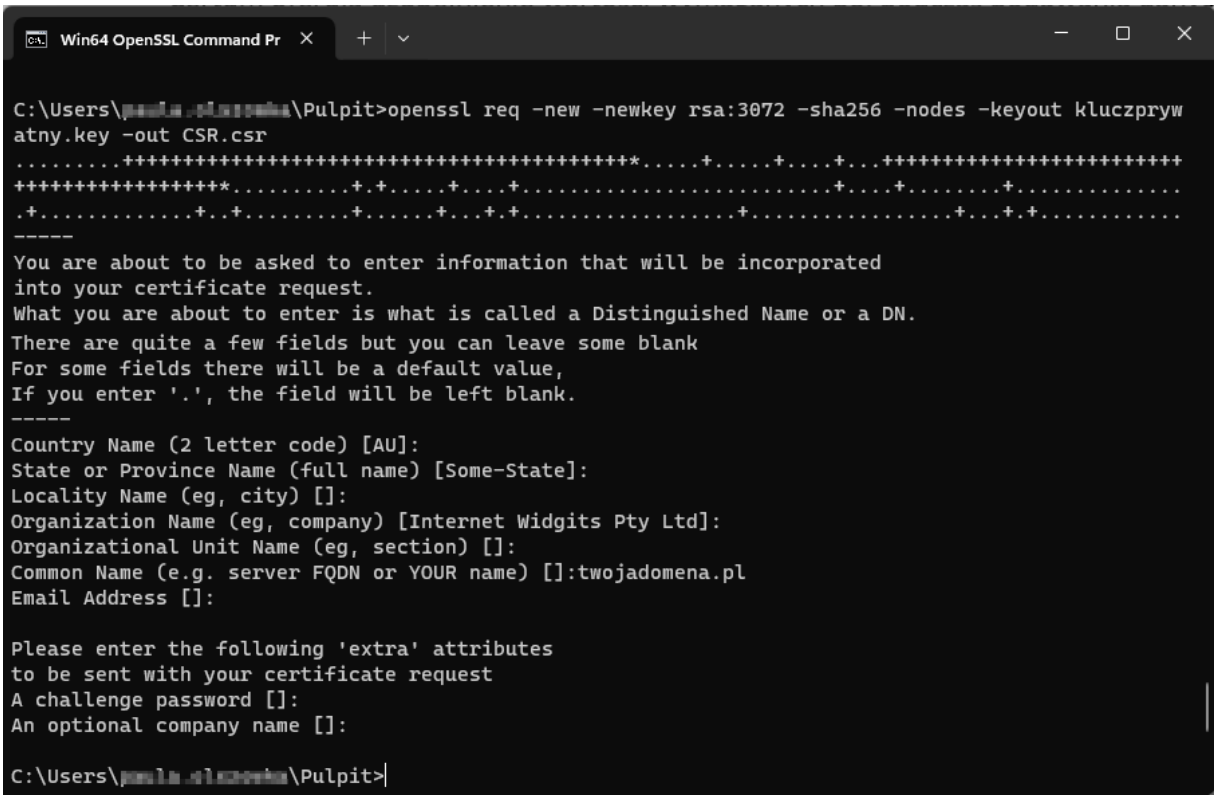
gdzie:

- **3072** – to długość klucza. Jeśli potrzebujesz, możesz użyć innej wartości jak 2048 lub 4096 bit
- **kluczprywatny**.key – to klucz prywatny. Możesz w poleceniu nadać mu inną nazwę. Zachowaj ten plik, ponieważ będzie on niezbędny do zainstalowania wydanego certyfikatu
- **CSR**.csr – to plik CSR. Możesz w poleceniu nadać mu inną nazwę. Użyjesz go do podania danych do aktywacji certyfikatu

b) Gdy konsola zapyta o wartości pól do umieszczenia w CSR, podaj przynajmniej wartość *Common name*. Niewymagane wartości możesz pominąć klikając przyciskiem **Enter**. Systemy

Certum oferują uzupełnienie wartości wymaganych pól podczas podawania danych do certyfikatu i nie ma potrzeby podawać ich w CSR

c) Po wprowadzeniu lub pominięciu wszystkich wymaganych pól , w folderze w którym uruchomiono OpenSSL zostaną wygenerowane 2 pliki: CSR oraz klucz prywatny o podanych w poleceniu nazwach. Możesz je skopiować do utworzonego wcześniej do tego celu folderu.



Aby użyć wygenerowanego CSR do podania danych do aktywacji certyfikatu, otwórz plik **CSR.**csr w edytorze tekstu np. programie Notatnik i skopiuj jego treść.

Generacja CSR dla kluczy ECC

Jeśli chcesz wygenerować CSR na kluczach ECC, co jest wymagane np. dla certyfikatu Krajowy Węzeł Tożsamości, wykonaj następujące kroki:

a) W konsoli OpenSSL użyj poniższego polecenia do wygenerowania pliku konfiguracyjnego dla ECC i zatwierdź jego wykonanie przyciskiem **Enter**:

```
openssl genpkey -genparam -algorithm ec -pkeyopt ec_paramgen_curve:P-256 -
out ECC.pem
```

gdzie:

- **P-256** – to długość klucza. Jeśli potrzebujesz, możesz użyć innej wartości jak P-384
- **ECC**.pem – to plik konfiguracyjny do generacji CSR i klucza prywatnego w algorytmie EC. Możesz w poleceniu nadać mu inną nazwę

b) W konsoli OpenSSL użyj poniższego polecenia i zatwierdź jego wykonanie przyciskiem **Enter**:

```
openssl req -newkey ec:ECC.pem -keyout kluczprywatny.key -out CSR.csr
```


certum.pl
infolinia@certum.pl

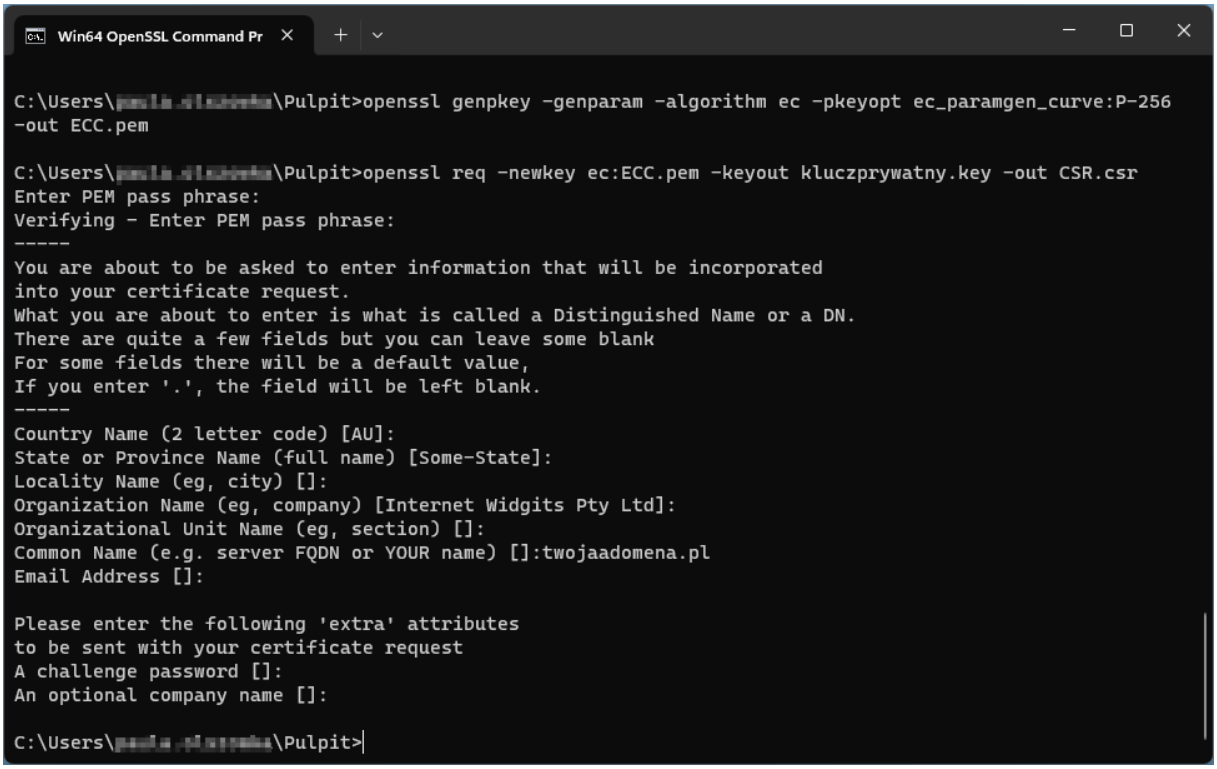
gdzie:

- **kluczprywatny**.key – to klucz prywatny. Możesz w poleceniu nadać mu inną nazwę. Zachowaj ten plik, ponieważ będzie on niezbędny do zainstalowania wydanego certyfikatu
- **CSR**.csr – to plik CSR. Możesz w poleceniu nadać mu inną nazwę. Użyjesz go do podania danych do aktywacji certyfikatu.

c) Nadaj hasło dla pliku klucza prywatnego. Zapisz je, ponieważ będzie potrzebne do instalacji wydanego certyfikatu. Wprowadzane hasło jest niewidoczne i należy je podać dwukrotnie

d) Gdy konsola zapyta o wartości pól do umieszczenia w CSR, podaj przynajmniej wartość *Common name*. Niewymagane wartości możesz pominąć klikając przyciskiem **Enter**. Systemy Certum oferują uzupełnienie wartości wymaganych pól podczas podawania danych do certyfikatu i nie ma potrzeby podawać ich w CSR

e) Po wprowadzeniu lub pominięciu wszystkich wymaganych pól , w folderze w którym uruchomiono OpenSSL zostaną wygenerowane 2 pliki: CSR oraz klucz prywatny o podanych w poleceniu nazwach. Możesz je skopiować do utworzonego wcześniej do tego celu folderu.



Aby użyć wygenerowanego CSR do podania danych do aktywacji certyfikatu, otwórz plik **CSR**.csr w edytorze tekstu np. w programie Notatnik i skopiuj jego treść.

3. Generowanie certyfikatu w pliku .pfx

Plik .pfx służy do zainstalowania certyfikatu. Możesz go wygenerować po wydaniu certyfikatu.

W tym celu, po wydaniu certyfikatu, pobierz plik certyfikatu w kodowaniu PEM i wykonaj kroki opisane poniżej. Wydany certyfikat możesz pobrać z wiadomości e-mail o utworzeniu certyfikatu lub z widoku **Szczegóły certyfikatu** z **Twojego konta** w zakładce **Produkty bezpieczeństwa** w sklepie Certum, w dogodnym kodowaniu **PEM**.

W widoku **Szczegółów certyfikatu** możesz również pobrać certyfikaty pośrednie dla Twojego certyfikatu.

a) Umieść pobrany plik certyfikatu w folderze z kluczem prywatnym
b) Używając konsoli OpenSSL, wykonaj następujące polecenie:

```
openssl pkcs12 -export -out certyfikat.pfx -inkey kluczprywatny.key -in
cert.pem
```

Wartości pogrubione oznaczają:

- **certyfikat**.pfx – nazwa, pod którą zostanie zapisany plik .pfx
- **kluczprywatny**.key – nazwa pliku klucza prywatnego, wygenerowanego wraz z CSR
- **cert**.pem – nazwa pliku wydanego certyfikatu.

c) Po wpisaniu komendy zostaniesz poproszony o nadanie hasła do pliku .pfx. Późniejsze podanie tego hasła będzie niezbędne do instalacji certyfikatu.

Po wykonaniu żądania zostanie utworzony plik .pfx pod wskazaną nazwą, w tym samym folderze co klucz prywatny i certyfikat.