Instrukcja –

Generacja CSR

Generowanie pliku CSR z pomocą narzędzia OpenSSL

wersja 1.2

Certum
by asseco

Spis treści

1. Zawartość instrukcji

Instrukcja służy do wygenerowania pliku CSR (plik żądania o certyfikat) koniecznego do zakupu i wydania certyfikatów:

- SSL,
- E-mail ID,
- Code Signing,
- Krajowy Węzeł.

Instrukcja przedstawiania proces generowanie CSR narzędziem OpenSSL, który jest najczęściej używaną na świecie implementacją protokołu Transport Layer Security (TLS). Użytkownicy na całym świecie korzystają z tego narzędzia celem, mi.in, utworzenia żądania podpisania certyfikatu (CSR). Te krok zostanie omówiony w niniejszej instrukcji.

Rekomendacja: Pamiętaj, aby nigdy nie usuwać plików certyfikatu po prawidłowym wykonaniu żądania! Trzymaj wszystkie pliki w jednym miejscu.

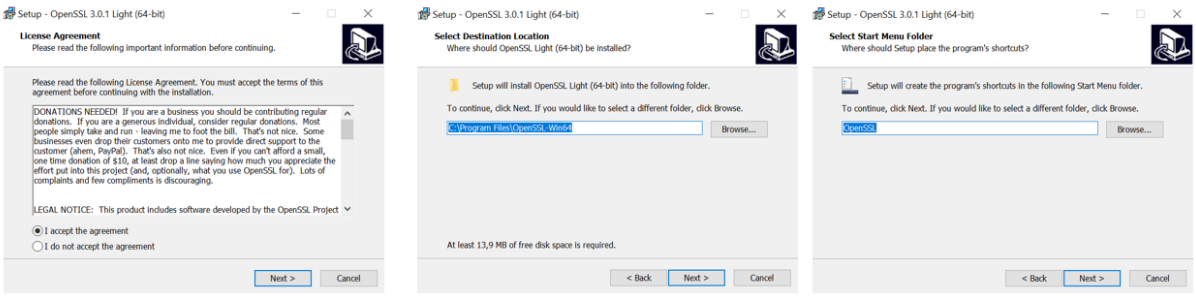
2. Instalacja narzędzia OpenSSL

a) Pobierz narzędzie OpenSSL z poziomu https://slproweb.com/products/Win32OpenSSL.html. Wybierz odpowiedni plik instalacyjny, zgodny z system operacyjnym, na których przeprowadzisz proces.

Uwaga: Zalecamy korzystanie z rekomendowanych plików przez zespół OpenSSL. Produkty rekomendowane i utworzone przez deweloperów OpenSSL posiadają w opisie poniższy komentarz: (Recommended for users by the creators of open SSL]

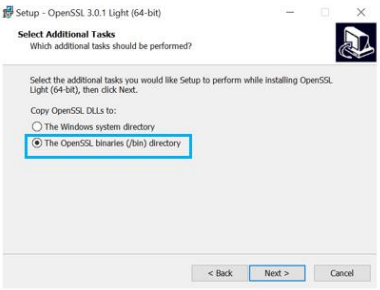
b) Zainstaluj oprogramowanie zgodnie z poniższymi krokami:

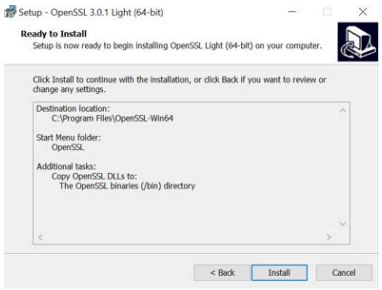
- Zaakceptuj warunki
- Wybierz miejsce zapisu (Rekomendujemy pozostawanie wartości domyślnej)
- Wybierz nazwę folderu (Rekomendujemy pozostawanie wartości domyślnej)



- Wybierz sposób uruchamiania programu (Rekomendujemy The OpenSSL binaries)
- Zainstaluj program, klikając polecenie Install

- Jeśli chcesz przekazać donacje, zaznacz wybraną opcję. Kliknij Finish celem zakończenia instalacji.





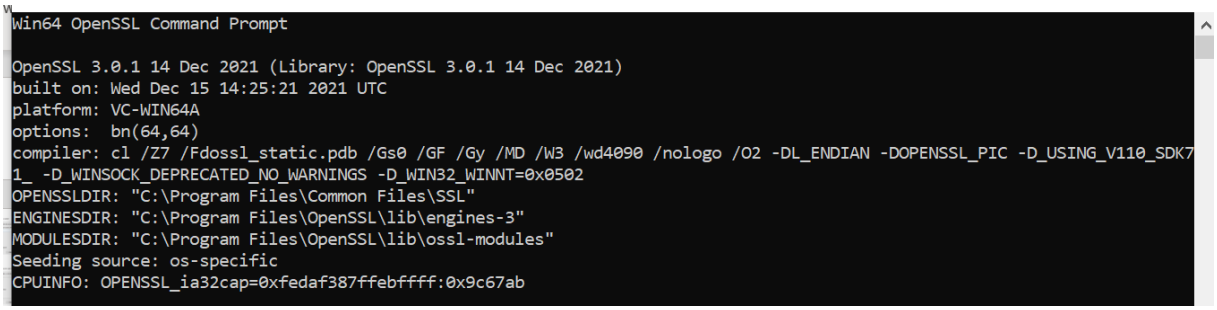
3. Uruchomienie OpenSSL

a) Przejdź do folderu, w którym zainstalowany został program. Wartość domyślna to: C:\Program Files\OpenSSL

b) Uruchom plik .bat start.bat

bin	01.02.2022 12:40	Folder plików	
acknowledgements.txt	15.12.2021 09:30	Dokument tekstowy	1 KB
authors.txt	15.12.2021 09:30	Dokument tekstowy	2 KB
c_rehash.pl	15.12.2021 09:30	Plik PL	7 KB
changes.txt	15.12.2021 09:30	Dokument tekstowy	721 KB
faq.txt	15.12.2021 09:30	Dokument tekstowy	1 KB
libcrypto-3-x64.dll	15.12.2021 09:30	Rozszerzenie aplikacji	5 006 KB
libssl-3-x64.dll	15.12.2021 09:30	Rozszerzenie aplikacji	754 KB
license.txt	15.12.2021 09:30	Dokument tekstowy	11 KB
news.txt	15.12.2021 09:30	Dokument tekstowy	70 KB
readme.txt	15.12.2021 09:30	Dokument tekstowy	7 KB
start.bat	15.12.2021 09:30	Plik wsadowy Windo...	1 KB
unins000.dat	01.02.2022 12:40	Plik DAT	12 KB
unins000.exe	01.02.2022 12:34	Aplikacja	714 KB

c) Po uruchomieniu pliku, pokaże się konsola, na której zaczniesz generować swój plik csr. Plik CSR zostanie wygenerowany za pomocą komend, które zostaną przedstawione w następnym rozdziale. Jeśli chcesz możesz je skopiować bez konieczności edycji.



4. Tworzenie pliku CSR

4.1 Tworzenie plików na RSA

Po otworzeniu się konsoli, będziesz musiał wpisać odpowiednie polecenia. Polecania różnią się w zależności o typu certyfikatu czy klucza certyfikatu. (Polecenia można wkleić za pomocą kombinacji CTRL+V). Jeśli się pomylisz, będziesz mógł ponownie wprowadzić poprawne polecenie, a konsola powiadomi cię o typie błędu). Po wpisaniu komendy, zawsze kliknij Enter.

a) Wpisz następujące polecenie i kliknij Enter

openssl req -new -newkey rsa:***3072*** –sha256 -nodes -keyout ***kluczprywatny***.key -out ***kluczpubliczny***.csr

```
C:\Users\anna.sikorska>openssl req -new -newkey rsa:3072 -sha256 -nodes -keyout kluczprywatny.key -out kluczpubliczny.csr
```

Uwaga: wartości zapisane kursywą można modyfikować.

3072 – wartość określa długość klucza. Można użyć 2048, 4096.

kluczprywatny i kluczpubliczny – pod tą nazwą zostaną zapisane pliki certyfikatów, możesz je dowolnie modyfikować, lub użyć tych wartości.

b) Po wpisaniu polecenia, zostaniesz poproszony o kolejne dane, które należy wypełnić w zależności od typu certyfikatu.

```
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) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:certum.pl
```

UWAGA: Dla certyfikatu Commercial DV uzupełnij tylko pole CN, w którym podasz domenę, którą chcesz zabezpieczyć, np. www.certum.pl Dla certyfikatu typu Wildcard, przed domenę podaj *certum.pl

Pola które poprzedzają CN, pomiń klikając Enter

Opis pozostałych pól.

UWAGA: Pola te są potrzebne do certyfikatów typu OV i EV

Nazwa kraju: Użyj dwuliterowego kodu bez interpunkcji dla kraju, na przykład: PL.

Stan lub prowincja: Wymień pełną nazwę województwa, stanu lub prowincji, na przykład: zachodniopomorskie czy Brandenburg, Texas itp.

Miejscowość lub Miasto: Wpisz miasto, np. Szczecin, New York, Berlin. Nie skracaj nazwy miasta.

Firma: Wpisz pełną i poprawną nazwę firmy.

Jednostka organizacyjna: Wpisz jednostkę organizacyjną

CN: nazwa domeny, np. certum.pl

Uwaga: podczas generowania CSR nie należy wprowadzać adresu e-mail, hasła zabezpieczającego ani opcjonalnej nazwy firmy. Pomiń te kroki klikając ENTER.

a) Po wpisaniu dodatkowych pól, zostaniesz poproszony o dodatkowe atrybuty związane z hasłem. Pozostaw je puste, klikając enter.

Please enter the following 'extra' attributes

to be sent with your certificate request

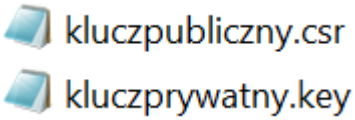
A challenge password []:

An optional company name []:

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

b) Będziesz wiedział, że zakończyłeś generowanie CSR, kiedy pojawi się Twoja nazwa użytkownika. Po wpisaniu komendy zostanie utworzona para kluczy publiczny .csr /prywatny .key. Oba klucze zostaną zapisane lokalnie na komputerze, w twoim folderze. Do wydania certyfikatu, będzie potrzeby plik publiczny certyfikatu z formatem .csr

c) Pliki zostaną domyślnie zapisane w folderze użytkownika: C:\Users\anna.sikorska



d) Pełna żądanie w postaci tekstowej (na niebiesko wpisano komendy, wprowadzone ręcznie zgodnie z instrukcją)

C:\Users\anna.sikorska>**openssl req -new -newkey rsa:3072 -sha256 -nodes -keyout kluczprywatny.key -out kluczpubliczny.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) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:certum.pl
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
C:\Users\anna.sikorska>
```

4.1 Tworzenie plików na ECC

Jeśli chcesz wygenerować pliki certyfikatu na kluczach ECC, co jest koniecznie np. dla certyfikatu Krajowy Węzeł, wykonaj następujące kroki:

a) uruchom generowanie pliku pem, z którego następnie zostaną wyeksportowane pliki .CRT oraz .KEY. Generowanie uruchamiamy z poziomu konsoli OpenSSL za pomocą następnego żądania”

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

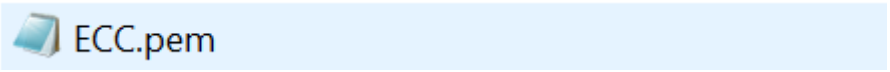
Wartość pogrubioną I pochyloną można edytować.

P-256 - to długość klucza, można zastosować również: P-384

ECC - pod tą nazwą zostanie utworzony plik .pem. Możesz ją dowolnie zmienić, jak i również skorzystaj z domyślnej. Pamiętaj, że będzie ona konieczna do drugiego żądania.

```
C:\Users\anna.sikorska>openssl genpkey -genparam -algorithm ec -pkeyopt ec_paramgen_curve:P-256 -out ECC.pem
```

Po przetworzeniu żądania w folderze użytkownika zostanie wygenerowany plik .pem pod wskazaną nazwą.



b) uruchom polecenie które wyeksportuje z pliku .pem kolejne pliki certyfikatu .csr oraz .key

UWAGA: pamiętaj, aby użyć takiej samej nazwy pliku pem, jakiej użyłeś przy generowaniu pierwszego żądania

openssl req -newkey ec:ECC.pem -keyout **kluczprywatny**.key -out **kluczpubliczny**.csr

Wartość pogrubioną I pochyloną można edytować. Pod tą nazwa zostaną utworzony pliki .key i .csr

```
C:\Users\anna.sikorska>openssl req -newkey ec:ECC.pem -keyout kluczprywatny.key -out kluczpubliczny.csr
```

c) w następnym kroku zostaniesz poproszony o podanie hasła. W przypadku ECC, należy je podać. Pamiętaj, żeby wpisać hasło, które zapamiętasz, będzie ono konieczne do otwarcia pliku .key oraz utworzenia pliku .pfx

UWAGA: wpisywane hasło będzie niewidoczne!! Nie martw się, jeśli nic nie widzisz. Po kliknięciu Enter, hasło zostanie przetworzone i nadpisane.

d) W następnym kroku zostaniesz poproszony o powtórzenie hasła. Powtórz to dokładnie to samo hasło.

```
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

e) Uzupełnij dalsze pola, wpisując potrzebne dane do certyfikatu zgodnie z tabelą. UWAGA: jeśli generujesz CSR dla SSL Commercial uzupełnij tylko pole CN.

Nazwa kraju: Użyj dwuliterowego kodu bez interpunkcji dla kraju, na przykład: PL.

Stan lub prowincja: Wymień pełną nazwę województwa, stanu lub prowincji, na przykład: zachodniopomorskie czy Brandenburg, Texas itp.

Miejscowość lub Miasto: Wpisz miasto, np. Szczecin, New York, Berlin. Nie skracaj nazwy miasta.

Firma: Wpisz pełną i poprawną nazwę firmy.

Jednostka organizacyjna: Wpisz jednostkę organizacyjną

CN: nazwa domeny, np. certum.pl

Uwaga: podczas generowania CSR nie należy wprowadzać adresu e-mail, hasła zabezpieczającego ani opcjonalnej nazwy firmy. Pomiń te kroki klikając ENTER.

f) Po wykonaniu tych kroków zostaną utworzone trzy pliki. Wszystkie zostaną zapisane w folderze Użytkownika: C:\Users\anna.sikorska. Do Certum dostarcz kluczpubliczny.csr

ECC.pem

kluczprywatny.key

kluczpubliczny.csr

g) Pełne żądanie w formie tekstowej (na niebiesko polecenia wprowadzone ręcznie)

C:\Users\anna.sikorska>**openssl genpkey -genparam -algorithm ec -pkeyopt ec_paramgen_curve:P-256 -out ECC.pem**

C:\Users\anna.sikorska>**openssl req -newkey ec:ECC.pem -keyout kluczprywatny.key -out kluczpubliczny.csr**
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

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) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []: certum.pl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\Users\anna.sikorska>
```

5. Dostarczenie pliku CSR do Certum

Po zakończeniu procesu, nie zależnie od sposobu generowanie kluczy (ECC czy RSA), pliki zostaną automatycznie utworzone w folderze Użytkownika: C:\Users\anna.sikorska>

Do wydania certyfikatu potrzebny będzie publiczna cześć certyfikatu.

Plik należy otworzyć w programie Notatnik.

Aby to zrobić, kliknij w plik. Zostaniesz poproszony o wybranie programu, w jakim chcesz otworzyć plik. Wybierz program notatnik. Po dokonaniu wyboru otwórz ponownie plik. Skopiuj treść i wklej ją do formularza zamawiania.

6. Utworzenie pliku .pfx

Plik .pfx konieczny jest celem zainstalowania certyfikatu. Plik pfx tworzymy po utworzeniu i wydaniu certyfikatu.

a) Po wydaniu certyfikatu pobierz plik certyfikatu w formie binarnej lub tekstowej) , z poziomu zakładki Zarządzanie Certyfikatami

6.1 Tworzenie z pliku .cer

a) Użyj następującego polecenia:

openssl pkcs12 -export -out **certificate**.pfx -inkey **kluczprywatny**.key -in **1f1da808028adaae5d5ced0679e04657**.cer

Wartość pogrubione oznaczają:
certificate – nazwa pod którą zostanie utworzony plik .pfx
kluczprywatny – nazwa klucza prywatnego, wygenerowana wraz z kluczem publicznym (musi być dokładnie taka sama)
1f1da808028adaae5d5ced0679e04657 – nazwa pliku .cer pobranego ze sklepu Certum

```
C:\Users\anna.sikorska>openssl pkcs12 -export -out certificate.pfx -inkey kluczprywatny.key -in 1f1da808028adaae5d5ced0679e04657.cer
Enter pass phrase for kluczprywatny.key:
```

Po wpisaniu komendy zostaniesz poproszony o podanie hasła, jeśli używasz certyfikatu na kluczach ECC. W przypadku RSA nie jest to wymagane.

Po wykonaniu żądania zostanie utworzony plik .pfx pod wskazaną nazwa w tym samym folderze.

6.2 Tworzenie pliku z pliku .pem

openssl pkcs12 -export -inkey private-kluczprywatny.key -in certyfikat.pem -certfile **plikpośrednizestronycertum**.pem -out nazwapfx.pfx

kluczprywatny – nazwa pliku .key utworzona w poprzednim żądaniu

certyfikat – nazwa pliku .pem pobranego ze strony Certum (użyj ten samej nazwy)

plikpośrednizestronycertum – nazwa pliku .pem pobranego ze sklepu Certum (użyj dokładnie tej samej nazwy)

nazwapfx – nazwa pliku pfx, który próbujesz utworzyć

UWAGA: potrzebujesz pliku pośredniego, który również możesz pobrać ze sklepu Certum.

UWAGA: Jeśli chcesz zaszyfrować plik pfx dodaj do żądania atrybut -aes256

Dodatkowo jeśli chcesz zdekodować swój CSR, użyj następującego polecenia:

openssl req -newkey ec:ECC.pem -keyout **kluczprywatny**.key -out **kluczpubliczny**.csr -nodes

Email Address []:	Common Name (e.g. server FQDN or YOUR name) []:	Organization al Unit Name (eg, section) []:	Organization Name (eg, company) [Internet Widgits Pty Ltd]:	Locality Name (eg, city) []:	State or Province Name (full name) [Some-State]:	Country Name (2 letter code) [AU]:	
Zawsze puste	**Domena** -jedna z domen	x	x	x	x	x	SSL Commercial
Zawsze puste	**Domena** -jedna z domen zawartych w certyfikacie, dla	*tak*	**tak**	**tak**	**tak**	**Kraj**	SSL OV/EV
Zawsze puste	**Open Source Developer + zawsze imię i nazwisko**	*tak*	**Open Source Developer**	**tak**	**tak**	**Kraj**	Code Signing Open Source
Zawsze puste	**Zawsze imię i nazwisko**	*tak*	tak	tak	**tak**	**Kraj**	Code Signing Standard
Zawsze puste	**Nazwa firmy**	*tak*	**tak**	**tak**	**tak**	**Kraj**	Code Signing EV
Zawsze puste	**Adres e-mail**	x	x	x	x	x	E-mail ID Individual
Zawsze puste	**Imię i nazwisko lub nazwa organizacii.**	**tak**	**tak**	**tak**	**tak**	**Kraj**	E-mail ID Business
Zawsze puste	**Imię i nazwisko lub nazwa**	**tak**	**tak**	**tak**	**tak**	**Kraj**	Krajowy Węzeł