Krajowy Operator Chmury Medycznej sp z o.o.
ul. Branickiego 13 02-072 Warszawa
22 574 81 60
biuro@chmuradlazdrowia.pl

INSTRUKCJA PRZYGOTOWANIA

ŻĄDANIA PODPISANIA CERTYFIKATU (CSR) i KLUCZA PRYWATNEGO

Przeznaczenie dokumentu:

W dokumencie opisano procedurę przygotowania CSR i kluczy prywatnych, które zostaną wykorzystane do wygenerowania certyfikatów służących do uwierzytelniania oprogramowania podmiotu medycznego w usługach udostępnionych w Chmurze dla zdrowia.

Uzasadnienie:

Komunikacja z usługami udostępnionymi w Chmurze dla zdrowia wymaga posiadania dwóch certyfikatów.

1. Pierwszy certyfikat (TLS) wykorzystywany jest do identyfikacji tożsamości systemu podczas nawiązywania połączenia z serwerem (Mutual TLS authentication).
2. Drugi certyfikat (WSS) wykorzystywany jest do podpisywania komunikatów przekazywanych do serwera usługi (WS-Security).

System wykorzystuje certyfikaty dostarczane przez Certum. Każde konto klienta w Chmurze dla zdrowia zostanie powiązane z parą certyfikatów. Certyfikaty generuje Biuro Obsługi Klienta (BOK). W celu wygenerowania certyfikatów, klient powinien dostarczyć do BOK poprawne żądania podpisania certyfikatu (Certificate Signing Request - CSR). Żądania podpisania certyfikatu można wygenerować korzystając z narzędzia udostępnionego przez Certum.

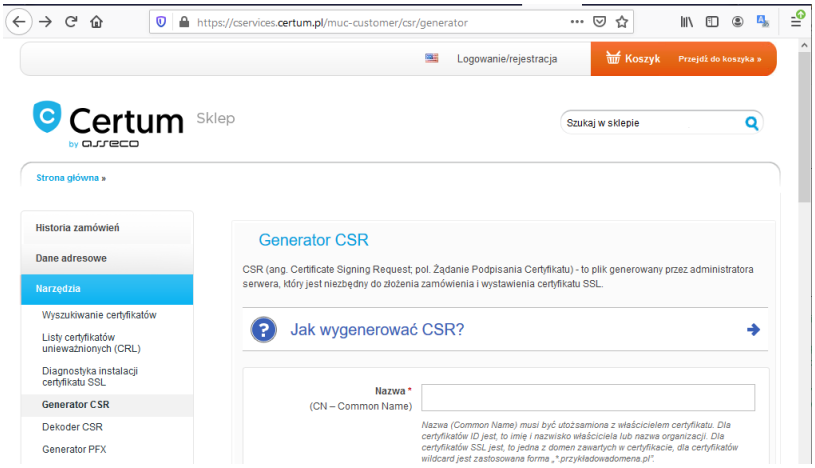
Wymagania wstępne:

Przeglądarka internetowa i dostęp do strony https://cservices.certum.pl/muc-customer/csr/generator. Na stronie dostępny jest generator CSR udostępniony przez wystawcę certyfikatów, Certum.

Dane podmiotu, dla którego mają być wygenerowane CSR i klucze prywatne.

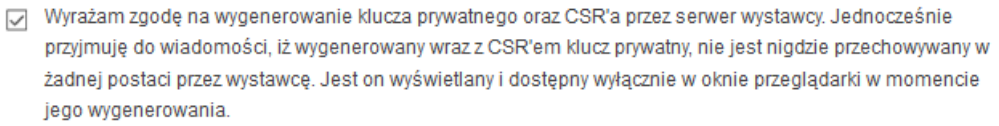
Krajowy Operator Chmury Medycznej sp z o.o.
ul. Branickiego 13 02-072 Warszawa
22 574 81 60
biuro@chmuradlazdrowia.pl

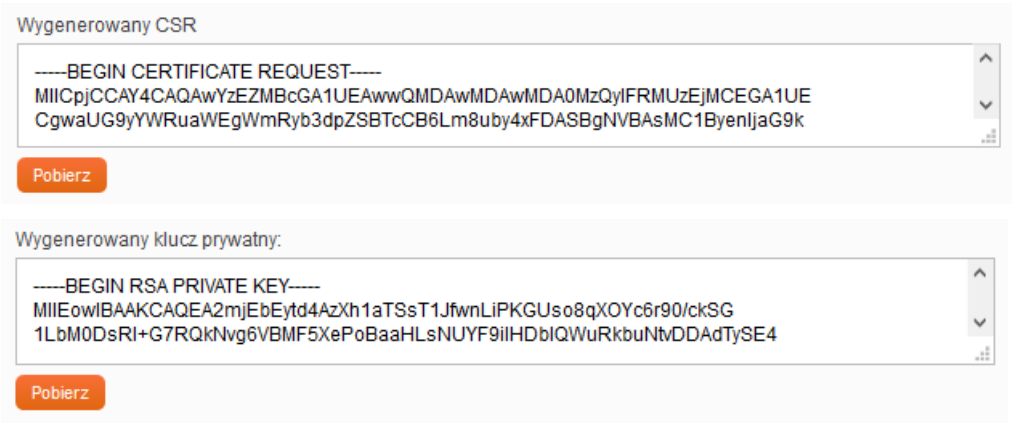
Kroki do wykonania:

Lp.	Nazwa kroku	Opis kroku
1	Wejście na stronę generatora CSR	1. W oknie przeglądarki wpisz adres: https://cservices.certum.pl/muc-customer/csr/generator Generator jest dostępny publicznie i nie wymaga podania żadnych danych uwierzytelniających.  2. Aplikacja wyświetli ekran umożliwiający wygenerowanie CSR i kluczy prywatnych.
2	Wprowadzenie danych podmiotu	1. Aplikacja prezentuje formularz umożliwiający wprowadzenie danych podmiotu. W celu wygenerowania CSR i kluczy prywatnych należy wprowadzić następujące dane (w polach wskazano przykładowe wartości). a. Nazwa (CN – Common Name) – Numer w rejestrze podmiotów wykonujących działalność leczniczą oraz ciąg znaków TLS lub WSS. (Numer będzie identyfikował dostarczony do BOK CSR. W ramach procedury generowania certyfikatu pracownik BOK zmodyfikuje wartość w tym polu, wpisując identyfikator klienta wygenerowany przez system. Ciąg znaków TLS lub WSS identyfikuje przeznaczenie CSR i klucza prywatnego.) **Nazwa *** (CN – Common Name) 000000004342 TLS b. Nazwa organizacji / Firmy (O – Organization Name) – Pełna nazwa podmiotu, dla którego będzie wydany certyfikat. **Nazwa Organizacji/Firmy** (O – Organization Name) Poradnia Zdrowie Sp z.o.o. c. Jednostka organizacyjna (OU – Organization Unit) – Nazwa jednostki organizacyjnej podmiotu, dla której będzie wydany certyfikat. **Jednostka organizacyjna** (OU – Organization Unit) Przychodnia d. Kraj (C – Country code) – Kod kraju, w którym zlokalizowany jest podmiot. **Kraj*** (C – Country code) Polska

Krajowy Operator Chmury Medycznej sp z o.o.
ul. Branickiego 13 02-072 Warszawa
22 574 81 60
biuro@chmuradlazdrowia.pl

<table>
<tr><td></td><td></td><td>2. Pozostawić domyślne parametry klucza:
a. Algorytm klucza – RSA.
b. Długość klucza – 2048.
c. Funkcja skrótu – SHA-256.
 

3. Pozostałe pola należy pozostawić niewypełnione.</td></tr>
<tr><td>3</td><td>Generowanie i zapis CSR oraz kluczy prywatnych</td><td>1. Przed wygenerowanie CSR i klucza prywatnego należy wyrazić zgodę na wygenerowanie tych danych przez serwer wystawcy, Certum.
 

2. Następnie należy nacisnąć przycisk „Generuj”.
3. System wygeneruje i udostępni CSR oraz klucz prywatny (poniżej przykładowe dane).
 

4. Wygenerowany CSR i klucz prywatny należy zapisać w osobnych plikach. W tym celu należy nacisnąć przycisk „Pobierz”.
5. Procedurę generowania CSR i klucza prywatnego należy wykonać dwa razy (dla klucza TLS i dla klucza WSS). Pliki z kluczami prywatnymi należy przechowywać w bezpiecznym miejscu.
6. Pliki CSR należy dostarczyć do Biura Obsługi Klienta (wysyłając wiadomość email na adres biuro@chmuradlazdrowia.pl). Na ich podstawie pracownik BOK wygeneruje certyfikaty TLS i WSS dla klienta.</td></tr>
</table>