

5.3. Certyfikaty

5.3.1. Wnioskuj o certyfikat

W MCU została udostępniona funkcjonalność wnioskowania o certyfikat KSeF.

Ważne!

Użyty środek uwierzytelnienia i zawarty w nim identyfikator decydują, na który identyfikator zostanie wydany certyfikat KSeF.

Aby złożyć wniosek o certyfikat KSeF z Menu głównego należy wybrać pozycję „Certyfikaty”, a następnie zakładkę „Wnioskuj o certyfikat”.

The screenshot shows a web application interface. On the left is a navigation menu with the following items: 'Uprawnienia', 'Certyfikaty', 'Wnioskuj o certyfikat', and 'Lista certyfikatów'. The 'Certyfikaty' and 'Wnioskuj o certyfikat' items are highlighted with a red box and an arrow. The main content area is titled 'Generowanie klucza i wniosku o wydanie certyfikatu' with a sub-header 'Wnioskuj o certyfikat'. It contains several form fields: 'Nazwa certyfikatu*' (with a help icon), a text input field, and a note 'Wpisz od 5 do 50 znaków' and 'Pole wymagane'. Below this is the 'Hasło*' section with a text input field and a list of requirements: 'Mus zawierać minimum:' (15 znaków, 1 wielką literę, 1 małą literę, 1 cyfrę, 1 znak specjalny) and 'Nie może zawierać:' (więcej niż 35 znaków, polskich znaków, innych znaków specjalnych). At the bottom is a 'Powtórz hasło*' section with another text input field.

Rysunek 79: Widok menu z pozycją „Certyfikaty”

MCU wyświetli formularz „Generowanie klucza i wniosku o wydanie certyfikatu”. Jest to pierwszy krok procesu składania wniosku o wydanie certyfikatu.

W tym kroku generowana jest para kluczy: publiczny i prywatny do certyfikatu.

Ważne!

Klucz publiczny jest dołączony do wniosku o wydanie certyfikatu. Klucz prywatny jest niezbędny do posługiwania się certyfikatem KSeF i jest przypisany do właściciela certyfikatu.

Klucz prywatny nie powinien być ujawniany i należy przechowywać go w bezpieczny sposób!

Uprawnienia
Certyfikaty
Wnioskuje o certyfikat
Lista certyfikatów

Generowanie klucza i wniosku o wydanie certyfikatu

Wnioskuje o certyfikat

Nazwa certyfikatu* 1
Pod nadaną przez Ciebie nazwą zapiszemy klucz prywatny oraz certyfikat

Wpisz nazwę certyfikatu

Wpisz od 5 do 50 znaków
Pole wymagane

Hasło* 2

Wpisz hasło

Musi zawierać minimum:

- 15 znaków
- 1 wielką literę
- 1 małą literę
- 1 cyfrę
- 1 znak specjalny: !@#%&*()-_+=

Nie może zawierać:

- więcej niż 35 znaków
- polskich znaków
- innych znaków specjalnych

Powtórz hasło* 3

Wpisz hasło

Generuj 4

Rysunek 80: Widok kroku 1 składania wniosku o wydanie certyfikatu

Pierwszym krokiem składania wniosku o wydanie certyfikatu jest uzupełnienie formularza.

W polu [1] „**Nazwa certyfikatu**” należy podać nazwę, pod którą zostanie zapisany klucz prywatny oraz certyfikat. Nazwa ta posłuży także do wyszukania certyfikatu na liście certyfikatów. System wykorzysta ją również do zapisu plików związanych z certyfikatem.

Nazwa certyfikatu powinna zawierać od 5 do 50 znaków. Może zawierać: litery bez polskich znaków, cyfry, spacje oraz znaki specjalne: myślnik (-) i podkreślenie (_).

W polu [2] „**Hasło**” należy zdefiniować hasło, które zabezpieczy klucz prywatny.

Hasło musi zawierać:

- od 15 do 32 znaków,
- wielką i małą literę bez polskich znaków diakrytycznych,
- cyfrę,
- jeden ze znaków specjalnych: !@#\$%^&*()-_+=

Hasło*

Hasło nie spełnia wszystkich wymagań

Musi zawierać minimum:

- ✗ 15 znaków
- ✗ 1 wielką literę
- ✓ 1 małą literę
- ✗ 1 cyfrę
- ✓ 1 znak specjalny: !@#\$%^&*()-_+=

Nie może zawierać:

- ✓ więcej niż 32 znaków
- ✓ polskich znaków
- ✓ innych znaków specjalnych

Rysunek 81: Komunikat o braku spełnienia wszystkich wymagań w zakresie hasła

Ważne!

Hasło należy zapamiętać lub zapisać i przechowywać w bezpiecznym miejscu ponieważ nie będzie można go zresetować.

W polu [3] „Powtórz hasło” należy wpisać powtórnie zdefiniowane w poprzednim polu hasło.

Po uzupełnieniu wszystkich danych użycie przycisku [4] „Generuj” spowoduje wygenerowanie pary kluczy: klucza publicznego i klucza prywatnego. Klucz prywatny zostanie automatycznie zapisany na urządzeniu Użytkownika pod nazwą własną zdefiniowaną w pierwszym polu dla certyfikatu w formie pliku z rozszerzeniem **.key**, np. moj_certyfikat.key.

Ważne!

Należy pamiętać, aby plik z kluczem prywatnym zapisać w bezpiecznym miejscu.



Przesłanie wniosku

Wniosku o certyfikat



Wygenerowano klucz prywatny


Wygenerowany klucz jest zapisany na Twoim urządzeniu pod nazwą Certyfikat_KSEF i zabezpieczony hasłem

Przeznaczenie certyfikatu* **1**

- Podpis linku do weryfikacji wystawcy
- Uwierzytelnienie w systemie KSeF

Certyfikat ważny od* **2**

Możesz zmienić datę, od której będzie ważny Twój certyfikat. Certyfikat będzie ważny przez 2 lata od podanej daty.

Wyślij wniosek o wydanie certyfikatu **3**

Rysunek 82: Widok kroku 2 składania wniosku o certyfikat

Drugim krokiem w składaniu wniosku o certyfikat jest ekran „Przesłanie wniosku”, w którym należy określić **[1] „Przeznaczenie certyfikatu”** oraz w polu **[2] „Certyfikat ważny od”** datę, od której będzie ważny certyfikat.

W części **[1] „Przeznaczenie certyfikatu”** Użytkownik wybiera jedną z dwóch dostępnych opcji:

- Podpis linku weryfikacyjnego wystawcy
- Uwierzytelnienie w systemie KSeF

W polu **[2] „Certyfikat ważny od”** system automatycznie ustawi aktualną datę. Certyfikat będzie ważny 2 lata od podanej daty. Istnieje możliwość zmiany daty początku ważności certyfikatu na przyszłą. Przy zmianie należy pamiętać o obowiązujących limitach w zakresie posiadanych certyfikatów.

Przy ponownym składaniu wniosku o certyfikat zaleca się podawanie daty początku ważności, jako dnia następnego po dacie wygaśnięcia posiadanego certyfikatu.

Użycie przycisku **[3] „Wyślij wniosek o wydanie certyfikatu”** uruchamia proces wydawania certyfikatu KSeF.

Wnioskuje o certyfikat

W realizacji

Twoje żądanie jest w trakcie przetwarzania. Operacja może potrwać kilka minut.



Rysunek 83: Widok "W realizacji" po uruchomieniu procesu wydawania certyfikatu

System wyświetli ekran realizacji procesu, który może potrwać kilka minut.

Istnieje możliwość użycia przycisku „Odśwież” służącego do ponownego załadowania aktualnie otwartej strony i aktualizacji jej zawartości, aby sprawdzić czy certyfikat KSeF został już wydany.

Wnioskuje o certyfikat

Zakończono pomyślnie

Twój certyfikat został wydany. Zadbaj o jego poufność i bezpieczeństwo.

Certyfikat wraz z kluczem prywatnym może zostać użyty do wystawiania faktur w trybie offline. W celu wygenerowania certyfikatu do uwierzytelnienia w KSeF ponownie wygeneruj klucz prywatny oraz zawnioskuj o certyfikat.



Rysunek 84: Widok pomyślnego zakończenia procesu wydawania certyfikatu

Po poprawnym wydaniu certyfikatu system wyświetli informacje o pomyślnym zakończeniu procesu. Z poziomu tego ekranu można zapisać wydany certyfikat na dysku wybierając przycisk [1] **Pobierz certyfikat** lub przejść do listy certyfikatów wybierając przycisk [2] **Przejdź do listy certyfikatów**.

Przycisk [1] „**Pobierz certyfikat**” umożliwi pobranie i zapisanie certyfikatu na dysku urządzenia pod nazwą własną zdefiniowaną w pierwszym kroku formularza w formie pliku w formacie PEM z rozszerzeniem **.crt**, np. **moj_certyfikat.crt**.

W przypadku wystąpienia problemu z wydaniem certyfikatu System wyświetli komunikat błędu z informacją, że certyfikat KSeF nie został wydany.