



Certyfikaty KSeF

Poradnik do Modułu Certyfikatów i Uprawnień – definicja, opis
i przebieg procesu wnioskowania

btla

Krajowy System
e-Faktur

Co to jest Certyfikat KSeF?

Certyfikat KSeF stanowi **cyfrowe narzędzie kryptograficzne**, które potwierdza tożsamość osoby fizycznej lub podmiotu gospodarczego.

Dokument ten jest wydawany przez Centrum Certyfikacji działające w ramach Ministerstwa Finansów. Certyfikaty te zawierają szczegółowe dane osobowe wnioskującego lub informacje identyfikujące dany podmiot gospodarczy.

Z uwagi na wrażliwy charakter danych osobowych, o certyfikat zawierający dane konkretnej osoby fizycznej może wystąpić wyłącznie ta osoba. **Tylko osoba, której dane dotyczą, może pobrać certyfikat i następnie wykorzystywać go w systemie KSeF.** Ta zasada zapewnia najwyższy poziom bezpieczeństwa i chroni przed nieuprawnionym dostępem do systemu.

Okres ważności certyfikatu

Certyfikat KSeF zachowuje ważność przez maksymalnie **2 lata** od daty wskazanej we wniosku o jego wydanie

Data początkowa

Jeśli we wniosku nie zostanie określona data początkowa ważności, certyfikat będzie ważny od momentu jego wydania przez system

Automatyczne wygaśnięcie

Po upływie okresu ważności certyfikat automatycznie wygasa i konieczne jest złożenie wniosku o nowy

Co to jest Certyfikat KSeF?

Certyfikat KSeF będzie stanowił jedną z dostępnych metod uwierzytelnienia się w systemie. Jest to narzędzie, które stanie się dostępne dopiero po uprzednim uwierzytelnieniu się w KSeF przy użyciu profilu zaufanego, podpisu kwalifikowanego lub pieczęci kwalifikowanej. Ta dwuetapowa procedura zapewnia dodatkowy poziom bezpieczeństwa.

Zastosowanie w trybach szczególnych

Certyfikat KSeF będzie **niezbędny do oznaczenia faktury** specjalnym kodem umożliwiającym potwierdzenie tożsamości wystawcy. Dotyczy to wystawiania faktur w następujących trybach szczególnych:

- Tryb offline24 (tymczasowy brak połączenia)
- Tryb offline przy niedostępności systemu
- Tryb awaryjny KSeF

Termin wdrożenia

Uwierzytelnienie za pomocą certyfikatu KSeF oraz jego wykorzystanie przy wystawianiu faktur w trybach szczególnych będzie **możliwe od 1 lutego 2026 roku**.

To kluczowa data dla wszystkich przedsiębiorców planujących korzystać z tej funkcjonalności.

Co to jest Certyfikat KSeF?

O wydanie certyfikatu będzie można występować w **Module Certyfikatów i Uprawnień (MCU)** już od 1 listopada 2025 roku. Moduł MCU zostanie udostępniony w domenie systemu KSeF i będzie dostępny dla wszystkich uprawnionych użytkowników po zalogowaniu się do systemu.

01

Osoby fizyczne zgłoszone w ZAW-FA

Osoby fizyczne, które zostały zgłoszone w zawiadomieniu ZAW-FA, będą mogły złożyć wniosek bez dodatkowych warunków

02

Osoby z uprawnieniami właścicielskimi

Osoby fizyczne posiadające uprawnienia właścicielskie w systemie KSeF mają automatyczny dostęp do funkcji wnioskowania

03

Podatnicy niebędący osobą fizyczną

Podmioty prawne posiadające uprawnienia właścicielskie i posługujące się pieczęcią elektroniczną do uwierzytelnienia w KSeF

04

Osoby z nadanymi uprawnieniami

Osoby lub podmioty, którym uprawnienia zostały nadane w MCU po 1 listopada 2025 roku

Wymienione kategorie użytkowników będą mogły składać wnioski o certyfikat KSeF **bez spełniania jakichkolwiek dodatkowych wymagań czy warunków**. System automatycznie zweryfikuje uprawnienia na podstawie danych zawartych w profilu użytkownika.

Co to jest Certyfikat KSeF?

Integracja z narzędziami komercyjnymi

Certyfikat będzie można wykorzystywać w profesjonalnych narzędziach komercyjnych do wystawiania e-Faktur, które są zintegrowane z API KSeF 2.0. Dzięki temu przedsiębiorcy korzystający z systemów księgowych będą mogli płynnie uwierzytelniać się za pomocą certyfikatu.

Ważne ograniczenie: Nie będzie możliwości uwierzytelnienia się certyfikatem w bezpłatnych narzędziach oferowanych przez Ministerstwo Finansów, takich jak Aplikacja Podatnika KSeF.

Dwa rodzaje certyfikatów

Certyfikat KSeF - uwierzytelnienie Przeznaczony będzie wyłącznie do uwierzytelniania się w systemie KSeF jako jedna z dostępnych metod logowania.

Certyfikat KSeF - offline Wymagany będzie do oznaczenia faktury kodem umożliwiającym potwierdzenie tożsamości wystawcy przy wystawianiu faktur w trybie offline.

Certyfikat do uwierzytelnienia

Uniwersalne narzędzie dostępu do systemu KSeF

Certyfikat typu 1 został zaprojektowany jako **uniwersalne narzędzie do uwierzytelniania się w systemie KSeF**. Stanowi on jedną z wielu dopuszczalnych metod logowania, która może być stosowana zamiennie z innymi metodami uwierzytelnienia dostępnymi w systemie.

Sesja interaktywna

Uwierzytelnienie certyfikatem KSeF będzie możliwe podczas pracy interaktywnej z systemem, gdy użytkownik bezpośrednio korzysta z interfejsu aplikacji

Sesja wsadowa

Certyfikat może być również wykorzystywany w sesjach wsadowych, gdzie następuje automatyczne przetwarzanie dużych ilości faktur

Mechanizm uprawnień

Po zalogowaniu się certyfikatem KSeF system automatycznie uwzględnia uprawnienia powiązane z identyfikatorem podatkowym (NIP lub PESEL) użytkownika. Dzięki temu użytkownik ma dostęp do wszystkich funkcji, do których został upoważniony.

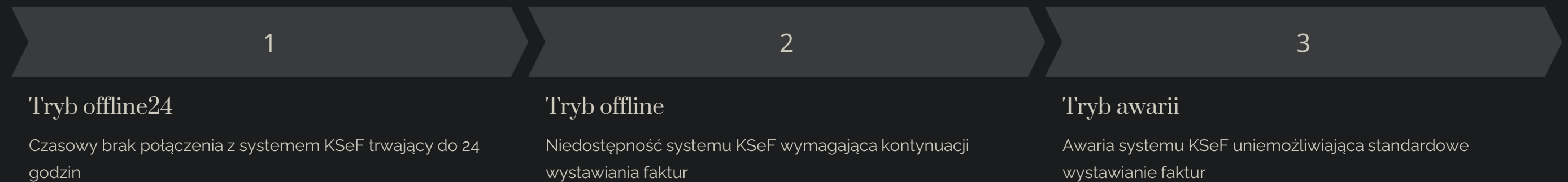
Powiązanie identyfikatorów

System inteligentnie rozpoznaje powiązanie między identyfikatorami NIP i PESEL tej samej osoby, co umożliwia płynne korzystanie z certyfikatu niezależnie od tego, który identyfikator został użyty przy jego wydaniu.

Certyfikat offline

Zabezpieczenie faktur w trybach awaryjnych

Certyfikat typu 2 pełni specjalistyczną rolę w systemie KSeF. Jest przeznaczony do **oznaczenia faktury specjalnym kodem umożliwiającym potwierdzenie tożsamości wystawcy** przy wystawianiu dokumentów w sytuacjach nadzwyczajnych. Dotyczy to następujących trybów pracy:



Interpretacja potwierdzenia tożsamości

Przez potwierdzenie tożsamości wystawcy należy rozumieć:

- **Potwierdzenie tożsamości osoby** – jeśli certyfikat był wydany na osobę fizyczną i zawiera jej dane osobowe
- **Identyfikację konkretnego podmiotu** – na przykład spółki, jeśli certyfikat był wydany na podmiot inny niż osoba fizyczna, taki jak spółka z ograniczoną odpowiedzialnością czy spółka akcyjna

Certyfikat KSeF

Kluczowe informacje o certyfikatach

Osobne generowanie certyfikatów

Certyfikaty KSeF obu typów (typu 1 - uwierzytelnienie oraz typu 2 - offline) będą generowane całkowicie osobno. System nie przewiduje możliwości wygenerowania jednego uniwersalnego certyfikatu KSeF, który obejmowałby jednocześnie oba zastosowania.

Oznacza to, że jeśli przedsiębiorca potrzebuje korzystać zarówno z funkcji uwierzytelnienia, jak i z możliwości wystawiania faktur w trybie offline, musi wystąpić o dwa odrębne certyfikaty - każdy przeznaczony do innego celu.

Mechanizm rozróżnienia

Dla ułatwienia identyfikacji i rozróżnienia certyfikatów przez użytkowników, certyfikaty obu typów będą posiadały w atrybucie **CN (commonName)** odpowiedni dopisek:

- „uwierzytelnienie” - dla certyfikatów typu 1
- „offline” - dla certyfikatów typu 2

Ten wyraźny sposób oznaczenia zapewnia, że użytkownik zawsze będzie wiedział, z jakim typem certyfikatu ma do czynienia i do jakiego celu może go wykorzystać.

Certyfikat KSeF

Limity dotyczące certyfikatów KSeF

System KSeF wprowadza precyzyjne limity liczby certyfikatów, które może posiadać jeden użytkownik lub podmiot. Limity te zostały ustalone w celu zapewnienia bezpieczeństwa systemu oraz racjonalnego zarządzania certyfikatami.

Osoby z numerem PESEL

Osoba fizyczna postępująca się **wyłącznie numerem PESEL** może posiadać:

- Co najwyżej **2 aktywne certyfikaty** w danym momencie
- Dodatkowo **2 nowe certyfikaty** oczekujące na użycie po wygaśnięciu obecnie aktywnych

To ograniczenie ma zastosowanie do osób, które nie prowadzą działalności gospodarczej i nie posiadają przypisanego numeru NIP.

Osoby fizyczne z numerem NIP

Osoba fizyczna postępująca się **identyfikatorem NIP** (prowadząca działalność gospodarczą) może uzyskać:

- Co najwyżej **100 certyfikatów** wydanych na podstawie danych kwalifikowanego certyfikatu podpisu elektronicznego
- Dodatkowo **100 nowych certyfikatów** do wykorzystania po wygaśnięciu aktualnie obowiązujących

Ten wyższy limit uwzględnia potrzeby przedsiębiorców prowadzących rozbudowaną działalność gospodarczą.

Certyfikat KSeF

Limity dotyczące certyfikatów KSeF - kontynuacja

Firmy (identyfikator NIP)

Podmiot gospodarczy identyfikowany numerem NIP, taki jak spółka z ograniczoną odpowiedzialnością, spółka akcyjna czy inna forma prawna, może posiadać:

- Co najwyżej **100 certyfikatów** wydanych na podstawie danych kwalifikowanego certyfikatu pieczęci elektronicznej
- Dodatkowo **100 nowych certyfikatów** przeznaczonych do użycia po wygaśnięciu obecnie aktywnych

Pieczęć elektroniczna jest odpowiednikiem podpisu elektronicznego dla podmiotów innych niż osoby fizyczne.

Podmioty bez NIP/PESEL

Podmioty zagraniczne lub inne jednostki, które uwierzytelniają się za pomocą certyfikatu niezawierającego identyfikatora NIP ani PESEL, mogą uzyskać:

- Co najwyżej **2 aktywne certyfikaty** w tym samym czasie
- Dodatkowo **2 nowe certyfikaty** do użycia po wygaśnięciu obecnie obowiązującego certyfikatu

Ten limit jest analogiczny do limitu dla osób fizycznych postępujących się wyłącznie numerem PESEL.

Określone limity certyfikatów zapewniają równowagę między elastycznością użytkowania systemu a **zachowaniem najwyższych standardów bezpieczeństwa**. Przedsiębiorcy mogą planować zarządzanie certyfikatami z odpowiednim wyprzedzeniem, dbając o ciągłość dostępu do systemu KSeF.

Wydanie certyfikatu KSeF w MCU

Rozpoczęcie procesu wnioskowania

Aby złożyć wniosek o certyfikat KSeF w Module Certyfikatów i Uprawnień, należy najpierw **zalogować się do MCU** przy użyciu dostępnej metody uwierzytelnienia (profil zaufany, podpis kwalifikowany lub pieczęć kwalifikowana).

Po zalogowaniu należy z menu głównego wybrać pozycję „Certyfikaty”, a następnie przejść do podzakładki „Wnioskuj o certyfikat”.

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

W tym kluczowym kroku następuje generowanie **pary kluczy kryptograficznych**: klucza publicznego oraz klucza prywatnego. Te dwa elementy stanowią podstawę bezpieczeństwa certyfikatu i umożliwiają późniejsze uwierzytelnienie w systemie.

The screenshot shows the MCU interface. On the left, a sidebar menu under 'Uprawnienia' has 'Certyfikaty' selected, with a sub-item 'Wnioskuj o certyfikat' highlighted by a red box and an arrow. The main area is titled 'Generowanie klucza i wniosku o wydanie certyfikatu' with a progress indicator '1 z 2'. Below the title is a form with three main sections: 1. 'Nazwa certyfikatu' with a text input field and a note 'Pod nadaną przez Ciebie nazwą zapiszemy klucz prywatny oraz certyfikat'. 2. 'Hasło' with a text input field and an eye icon. 3. A list of password requirements: 'Musi 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). There is also a 'Powtórz hasło' section with another text input field and eye icon.

Uprawnienia

Certyfikaty

Wnioskuj o certyfikat

Lista certyfikatów

1 z 2

Generowanie klucza i wniosku o wydanie certyfikatu

Wnioskuj o certyfikat

Nazwa certyfikatu * ⓘ

Pod nadaną przez Ciebie nazwą zapiszemy klucz prywatny oraz certyfikat

Wpisz nazwę certyfikatu

Wpisz od 5 do 50 znaków

Pole wymagane

Hasło *

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 *

Wpisz hasło

Wydanie certyfikatu KSeF w MCU

Moduł Certyfikatów i Uprawnień (MCU)

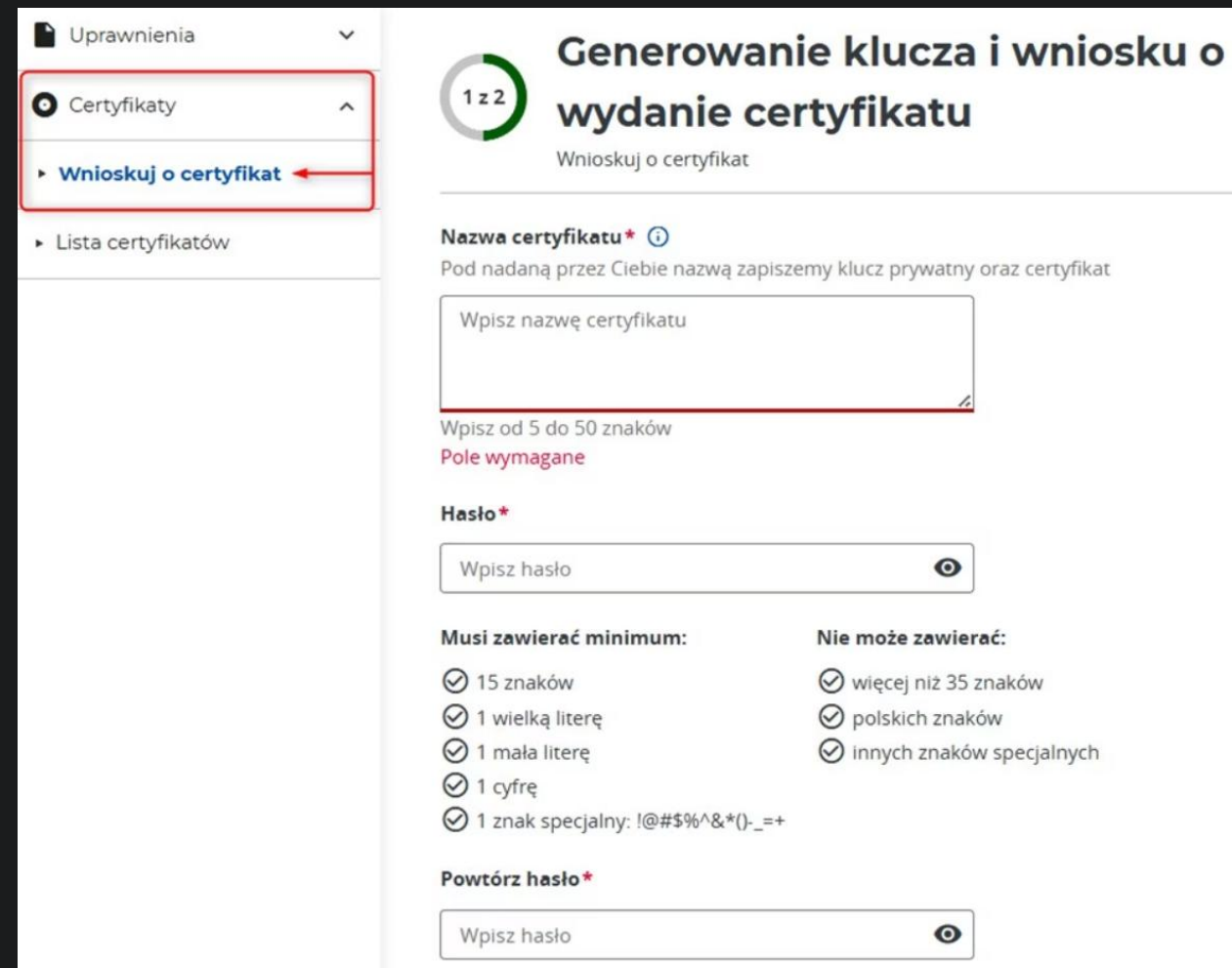
Kluczowa informacja o kluczach kryptograficznych

Klucz publiczny jest automatycznie dołączany do składanego wniosku o wydanie certyfikatu KSeF. Ten klucz może być udostępniany i służy do weryfikacji tożsamości użytkownika w systemie.

Klucz prywatny jest absolutnie niezbędny do posługiwania się certyfikatem KSeF. Jest on przypisany wyłącznie do właściciela certyfikatu i stanowi podstawę bezpieczeństwa całego mechanizmu uwierzytelnienia.

Klucz prywatny nie powinien być ujawniany!

Należy przechowywać go w maksymalnie bezpiecznym miejscu. Utrata klucza prywatnego oznacza całkowitą utratę możliwości korzystania z certyfikatu, a jego ujawnienie osobom trzecim może prowadzić do poważnych naruszeń bezpieczeństwa. System nie oferuje możliwości odzyskania utraconego klucza prywatnego - w przypadku jego zgubienia konieczne będzie wygenerowanie całkowicie nowego certyfikatu.



The screenshot shows the 'Uprawnienia' (Permissions) menu on the left, with 'Certyfikaty' (Certificates) selected. A red box highlights the 'Wnioskuj o certyfikat' (Apply for certificate) option. The main panel is titled 'Generowanie klucza i wniosku o wydanie certyfikatu' (Generating key and application for certificate issuance) and shows a progress indicator '1 z 2'. The form includes fields for 'Nazwa certyfikatu' (Certificate name) and 'Hasło' (Password), both marked as required. The 'Nazwa certyfikatu' field has a hint: 'Pod nadaną przez Ciebie nazwą zapiszemy klucz prywatny oraz certyfikat' (Under the name you give, we will save the private key and the certificate). The 'Hasło' field has a hint: 'Wpisz od 5 do 50 znaków' (Enter from 5 to 50 characters). Below the fields, there are two columns of requirements: 'Musi zawierać minimum:' (Must contain at least:) and 'Nie może zawierać:' (Must not contain:). The 'Musi zawierać minimum:' column lists: 15 znaków (15 characters), 1 wielką literę (1 uppercase letter), 1 małą literę (1 lowercase letter), 1 cyfrę (1 digit), and 1 znak specjalny: !@#\$%^&*()-_+= (1 special character: !@#\$%^&*()-_+=). The 'Nie może zawierać:' column lists: więcej niż 35 znaków (more than 35 characters), polskich znaków (Polish characters), and innych znaków specjalnych (other special characters). At the bottom, there is a 'Powtórz hasło' (Repeat password) field.

Uprawnienia

Certyfikaty

Wnioskuj o certyfikat

Lista certyfikatów

Generowanie klucza i wniosku o wydanie certyfikatu

Wnioskuj o certyfikat

1 z 2

Nazwa certyfikatu * ⓘ

Pod nadaną przez Ciebie nazwą zapiszemy klucz prywatny oraz certyfikat

Wpisz nazwę certyfikatu

Wpisz od 5 do 50 znaków

Pole wymagane

Hasło *

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 *

Wpisz hasło

Wydanie certyfikatu KSeF w MCU

Definiowanie nazwy certyfikatu

W polu oznaczonym jako **[1] Nazwa certyfikatu** użytkownik musi podać nazwę, pod którą zostanie zapisany zarówno klucz prywatny, jak i sam certyfikat. Ta nazwa pełni kilka istotnych funkcji w systemie:

- Służy do **identyfikacji certyfikatu** na liście wszystkich certyfikatów użytkownika
- System wykorzysta ją do **automatycznego zapisu plików** związanych z certyfikatem na urządzeniu użytkownika
- Ułatwia późniejsze **wyszukiwanie konkretnego certyfikatu** wśród wielu dokumentów

Wymagania formalne nazwy

Nazwa certyfikatu musi spełniać określone kryteria techniczne:

1. Długość: od **5 do 50 znaków**
2. Dopuszczalne znaki: litery polskiego alfabetu (bez znaków diakrytycznych), cyfry (0-9), spacje
3. Znaki specjalne: myślnik (-) oraz podkreślenie (_)

Przykładowe prawidłowe nazwy: „Certyfikat_Firmy_2025”, „Moj pierwszy certyfikat”, „Cert-Uwierzytelnienie-01”

Wydanie certyfikatu KSeF w MCU

Tworzenie hasła zabezpieczającego

W polu oznaczonym jako **[2] Hasło** należy zdefiniować silne hasło, które będzie zabezpieczało klucz prywatny przed nieuprawnionym dostępem. To hasło stanowi dodatkową warstwę ochrony certyfikatu.

Wymagania dotyczące hasła

Hasło musi spełniać następujące rygorystyczne kryteria bezpieczeństwa:

- **Długość:** od 15 do 32 znaków
- **Wielka litera:** co najmniej jedna wielka litera alfabetu łacińskiego (A-Z) bez polskich znaków diakrytycznych
- **Mała litera:** co najmniej jedna mała litera alfabetu łacińskiego (a-z) bez polskich znaków diakrytycznych
- **Cyfra:** co najmniej jedna cyfra (0-9)
- **Znak specjalny:** co najmniej jeden ze znaków: !@#\$%^&*()-_+=

Przykład prawidłowego hasła: „Moje#Haslo2025_KSeF!”

The screenshot displays the 'Generowanie klucza i wniosku o wydanie certyfikatu' (Key generation and certificate request) screen. A sidebar on the left contains navigation links: 'Uprawnienia', 'Certyfikaty', 'Wniosek o certyfikat', and 'Lista certyfikatów'. The main area shows a form for 'Nazwa certyfikatu*' (Certificate name*) with a red error indicator '1'. Below the form, a modal window titled 'Hasło* 2' (Password* 2) is open, showing password requirements. The modal includes a 'Wpisz hasło' (Enter password) field with a toggle for visibility. The requirements are listed in two columns: 'Musi zawierać minimum:' (Must contain at least:) and 'Nie może zawierać:' (Must not contain:). The 'Musi zawierać minimum:' column lists: 15 znaków (15 characters), 1 wielką literę (1 uppercase letter), 1 małą literę (1 lowercase letter), 1 cyfrę (1 digit), and 1 znak specjalny: !@#\$%^&*()-_+= (1 special character). The 'Nie może zawierać:' column lists: więcej niż 32 znaków (more than 32 characters), polskich znaków (Polish characters), and innych znaków specjalnych (other special characters). The modal also has a 'Wpisz hasło' field and a 'Generuj' (Generate) button with a red error indicator '4'.

WAŻNE: System nie przewiduje możliwości resetowania zapomnianego hasła. W przypadku utraty hasła jedynym rozwiązaniem będzie wygenerowanie całkowicie nowego certyfikatu z nowym hasłem.

Wydanie certyfikatu KSeF w MCU

Potwierdzenie hasła

Po zdefiniowaniu hasła w polu [2], należy je **zapamiętać lub zapisać w bezpiecznym miejscu**. Jest to absolutnie kluczowe, ponieważ system nie oferuje funkcji resetowania zapomnianego hasła.

Zalecane metody bezpiecznego przechowywania hasła:

- Menedżer haseł (np. KeePass, LastPass, 1Password)
- Zaszyfrowany plik na zabezpieczonym nośniku
- Sejf lub inna fizyczna skrytka (dla zapisanego hasła)

Nigdy nie należy przechowywać hasła w postaci niezabezpieczonej, takiej jak zwykły plik tekstowy czy notatka w telefonie.

Pole potwierdzenia

W polu oznaczonym jako [3] **Powtórz hasło** należy wpisać ponownie dokładnie to samo hasło, które zostało zdefiniowane w poprzednim polu [2].

Ten mechanizm **weryfikacji podwójnej** zabezpiecza przed przypadkowymi błędami podczas wpisywania hasła. System porówna obie wersje i dopiero po ich zgodności pozwoli na kontynuację procesu generowania certyfikatu.

Jeśli hasła nie będą identyczne, system wyświetli komunikat o błędzie i poprosi o ponowne wprowadzenie danych.

Uprawnienia

Certyfikaty

Wnioskuje o certyfikat

Lista certyfikatów

1 z 2

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:

Nie może zawierać:

15 znaków

1 wielką literę

1 małą literę

1 cyfrę

1 znak specjalny: !@#\$%^&*()_+=

więcej niż 32 znaków

polskich znaków

innych znaków specjalnych

Powtórz hasło* 3

Wpisz hasło

Generuj 4

Wydanie certyfikatu KSeF w MCU

Generowanie pary kluczy

Po prawidłowym uzupełnieniu wszystkich trzech pól (nazwa certyfikatu, hasło oraz powtórzenie hasła), należy użyć przycisku oznaczonego jako **[4] Generuj**. Ta czynność uruchomi proces generowania pary kluczy kryptograficznych.

Co się dzieje po kliknięciu „Generuj”?

System automatycznie wygeneruje:

1. **Klucz publiczny** - zostanie dołączony do wniosku o wydanie certyfikatu
2. **Klucz prywatny** - zostanie automatycznie zapisany na urządzeniu użytkownika

Klucz prywatny zostanie zapisany pod nazwą własną zdefiniowaną w pierwszym polu formularza, w formie pliku z rozszerzeniem **.key**. Na przykład, jeśli nazwa certyfikatu to „moj_certyfikat”, plik zostanie zapisany jako *moj_certyfikat.key*.

Bezpieczne przechowywanie klucza prywatnego

Jest niezwykle istotne, aby plik z kluczem prywatnym zapisać w bezpiecznym folderze na urządzeniu. Zaleca się:

- Przeniesienie pliku z domyślnej lokalizacji pobierania do dedykowanego, bezpiecznego folderu
- Zabezpieczenie folderu hasłem lub szyfrowaniem
- Utworzenie kopii zapasowej w innej bezpiecznej lokalizacji
- Usunięcie pliku z domyślnego folderu pobierania, jeśli został tam zapisany

Wydanie certyfikatu KSeF w MCU

Krok drugi - Przesłanie wniosku

Drugim krokiem w procesie składania wniosku o certyfikat jest ekran zatytułowany „Przesłanie wniosku”. W tym miejscu użytkownik musi określić dwa kluczowe parametry przyszłego certyfikatu.

Pole [1] Przeznaczenie certyfikatu

W tej sekcji użytkownik wybiera jedną z dwóch dostępnych opcji, które definiują sposób wykorzystania certyfikatu:

- **Podpis linku do weryfikacji wystawcy** - opcja ta odpowiada certyfikatowi typu 2 (offline), który będzie wykorzystywany do oznaczania faktur wystawianych w trybach szczególnych
- **Uwierzytelnienie w systemie KSeF** - opcja ta odpowiada certyfikatowi typu 1, który służy do logowania się do systemu KSeF

Wybór przeznaczenia jest **nieodwracalny** - po wydaniu certyfikatu nie można zmienić jego typu. W razie potrzeby korzystania z obu funkcjonalności należy wnioskować o dwa odrębne certyfikaty.

2 z 2

Przesłanie wniosku
Wnioskuj o certyfikat

✓

Wygenerowano klucz prywatny

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

Przeznaczenie certyfikatu * 1

☒ Podpis linku do weryfikacji wystawcy

☐ Uwierzytelnienie w systemie KSeF

Certyfikat ważny od *

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

20.09.2025

📅

2

Wyślij wniosek o wydanie certyfikatu

3

Pamiętaj, że należy zachować plik z kluczem prywatnym w bezpiecznym folderze. Dodatkowo można usunąć go z miejsca, gdzie został zapisany domyślnie przez system, i przenieść do lokalizacji znanej wyłącznie użytkownikowi, zapewniającej maksymalną ochronę.

Wydanie certyfikatu KSeF w MCU

Określanie daty ważności i wysyłka wniosku

Pole [2] Certyfikat ważny od

System automatycznie ustawi w tym polu **aktualną datę** jako datę początku ważności certyfikatu. Od tej daty certyfikat będzie ważny przez okres **dokładnie 2 lat**.

Użytkownik ma możliwość zmiany daty początku ważności certyfikatu na datę przyszłą. Może to być przydatne, gdy:

- Planujemy wymianę certyfikatu z wyprzedzeniem
- Chcemy, aby nowy certyfikat stał się aktywny dopiero po wygaśnięciu obecnego
- Synchronizujemy okresy ważności kilku certyfikatów

Przycisk [3] Wyślij wniosek

Po uzupełnieniu wszystkich wymaganych pól i sprawdzeniu poprawności wprowadzonych danych, należy użyć przycisku **[3] Wyślij wniosek o wydanie certyfikatu**.

Kliknięcie tego przycisku **uruchamia proces wydawania certyfikatu KSeF**. Od tego momentu system rozpoczyna:

1. Weryfikację poprawności danych
2. Sprawdzenie limitów certyfikatów
3. Generowanie certyfikatu
4. Podpisanie certyfikatu przez CA KSeF

Po wystaniu wniosku nie ma możliwości cofnięcia tej operacji ani modyfikacji parametrów certyfikatu.

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

20.09.2025



2

Wyślij wniosek o wydanie certyfikatu

3

Ważna uwaga: Przy zmianie daty początku ważności należy pamiętać o obowiązujących limitach w zakresie posiadanych certyfikatów. System weryfikuje, czy użytkownik nie przekroczy maksymalnej liczby aktywnych certyfikatów w danym okresie.

Wydanie certyfikatu KSeF w MCU

Po uruchomieniu procesu wydawania certyfikatu KSeF system rozpoczyna szereg operacji kryptograficznych i weryfikacyjnych. **Proces ten może potrwać kilka minut**, w zależności od obciążenia systemu oraz liczby jednocześnie przetwarzanych wniosków.

Monitorowanie postępu

Podczas oczekiwania na zakończenie procesu użytkownik widzi ekran z informacją o trwającym przetwarzaniu. System nie wymaga żadnych dodatkowych działań ze strony użytkownika - wystarczy poczekać na zakończenie operacji.

Nie należy zamykać okna przeglądarki ani opuszczać strony podczas przetwarzania wniosku, ponieważ może to przerwać proces wydawania certyfikatu.

Funkcja odświeżania

System udostępnia przycisk „**Odśwież**”, który służy do ponownego załadowania aktualnie otwartej strony i aktualizacji jej zawartości. Użycie tego przycisku pozwala sprawdzić, czy certyfikat KSeF został już wydany i jest gotowy do pobrania.

Przycisk ten można używać wielokrotnie, szczególnie jeśli proces trwa dłużej niż przewidywane kilka minut.



Wydanie certyfikatu KSeF w MCU

Pomyślne zakończenie procesu

Po poprawnym wydaniu certyfikatu przez system KSeF, użytkownik zobaczy ekran z informacją o **pomyślnym zakończeniu procesu**. To potwierdzenie oznacza, że certyfikat został wygenerowany, podpisany przez CA KSeF i jest gotowy do użycia.

Dostępne opcje

Z poziomu tego ekranu podsumowującego użytkownik ma do wyboru dwie możliwości:

Opcja [1] Pobierz certyfikatTen przycisk umożliwia natychmiastowe pobranie i zapisanie wydanego certyfikatu na dysku lokalnym urządzenia. Certyfikat zostanie zapisany pod nazwą własną zdefiniowaną w pierwszym kroku formularza, w formie pliku w formacie PEM z rozszerzeniem **.crt**. Przykładowo, jeśli nazwa certyfikatu to „moj_certyfikat”, plik zostanie zapisany jako *moj_certyfikat.crt*.

Opcja [2] Przejdź do listy certyfikatówTen przycisk kieruje użytkownika do pełnej listy wszystkich certyfikatów powiązanych z jego kontem. Lista certyfikatów umożliwia zarządzanie wszystkimi posiadanymi certyfikatami, ich przeglądanie, pobieranie oraz unieważnianie.

Wnioskuj 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.

1

Pobierz certyfikat

2

Przejdź do listy certyfikatów

📄 **Zalecenie:** Nawet jeśli użytkownik pobierze certyfikat bezpośrednio z tego ekranu, zawsze może pobrać go ponownie później z listy certyfikatów. Certyfikat (klucz publiczny) jest przechowywany w systemie przez cały okres jego ważności.

Wydanie certyfikatu KSeF w MCU

Obsługa błędów podczas wydawania certyfikatu

W rzadkich przypadkach może wystąpić sytuacja, w której proces wydawania certyfikatu nie zakończy się pomyślnie. System KSeF jest tak zaprojektowany, aby w przypadku wykrycia jakiegokolwiek problemu wyświetlić użytkownikowi odpowiedni komunikat.

Komunikat o błędzie

Jeśli wystąpi problem z wydaniem certyfikatu, system wyświetli **komunikat błędu z jasną informacją**, że certyfikat KSeF nie został wydany. Komunikat ten może zawierać również dodatkowe szczegóły techniczne, które mogą być przydatne dla administratora systemu.

Procedura postępowania

W przypadku wystąpienia błędu należy postępować według następujących kroków:

1. **Ponowne złożenie wniosku** - pierwszą czynnością powinno być ponowne przejście przez cały proces składania wniosku o wydanie certyfikatu KSeF od początku
2. **Weryfikacja danych** - należy upewnić się, że wszystkie pola zostały wypełnione prawidłowo i zgodnie z wymaganiami
3. **Sprawdzenie limitów** - warto zweryfikować, czy nie został przekroczony limit posiadanych certyfikatów

Kontakt z administratorem

W razie **powtórznego wystąpienia błędu** pomimo prawidłowego wypełnienia wszystkich pól, należy skontaktować się z administratorem systemu KSeF. W tym celu można wykorzystać opcję „Skontaktuj się z nami” umieszczoną w stopce aplikacji MCU. Formularz kontaktowy pozwala opisać problem i otrzymać pomoc techniczną.

Wnioskuj o certyfikat



[← Powrót](#)

Certyfikat nie został wygenerowany.

Spróbuj ponownie lub skontaktuj się z administratorem.

Przeglądanie certyfikatów w MCU

Lista certyfikatów - centralne miejsce zarządzania

Wszystkie informacje o wydanych certyfikatach są zebrane w jednym, centralnym miejscu zwanym **Listą certyfikatów**. Jest to kluczowe narzędzie do zarządzania certyfikatami KSeF, które umożliwia przeglądanie, pobieranie oraz unieważnianie certyfikatów.

Dostęp do listy certyfikatów

Lista certyfikatów wyświetla się jako podzakładka pozycji „Certyfikaty” w menu głównym aplikacji MCU. Po wybraniu tej opcji system prezentuje tabelę zawierającą wszystkie certyfikaty powiązane z identyfikatorem podatkowym zalogowanego użytkownika.

Należy pamiętać, że system uwzględnia **powiązanie identyfikatorów NIP i PESEL** - oznacza to, że na liście pojawią się certyfikaty wydane zarówno na NIP, jak i na powiązany PESEL tej samej osoby.

Struktura tabeli

Tabela z danymi certyfikatów jest przejrzystie zorganizowana i przedstawia wszystkie kluczowe informacje potrzebne do identyfikacji i zarządzania certyfikatami. Każdy wiersz tabeli reprezentuje jeden certyfikat, a kolumny zawierają różne atrybuty tego certyfikatu.

Szczegółowy opis poszczególnych kolumn tabeli zostanie przedstawiony na kolejnych stronach dokumentu, aby zapewnić pełne zrozumienie wszystkich dostępnych informacji.

Listy certyfikatów

Wniosek o certyfikat

Filtrowanie

	1	2	3	4	5	6	7	8	9
	Numer seryjny certyfikatu	Nazwa własna	Przeznaczenie	Identyfikator podmiotu, dla którego wystawiono certyfikat	Nazwa właściciela certyfikatu	Status	Ważny od	Ważny do	Data ostatniego użycia
☐	0199058253829053	Certyfikat_testowy	Podpis linku	NIP: 3333333333	KSeF QA Tester	Aktywny	21.09.2025	21.09.2027	---
☐	014C5FFD6545F85B	Certyfikat_testowy_2	Podpis linku	NIP: 3333333333	KSeF QA Tester	Aktywny	22.09.2025	22.09.2027	---

Pobierz certyfikat

Unieważnij

10 wierszy na stronę

<

1

>

Opis pozycji tabeli zawartych w Liście certyfikatów

Podstawowe informacje identyfikacyjne

1 Numer seryjny certyfikatu

To **unikalny identyfikator** przypisany do każdego certyfikatu przez CA KSeF (Centrum Certyfikacji Krajowego Systemu e-Faktur). Numer ten jest wyrażony w formacie heksadecymalnym i jest niepowtarzalny w całym systemie.

Przykład: 0144f3ae7f078ed8

Numer seryjny służy do jednoznacznej identyfikacji certyfikatu w komunikacji z administratorem systemu oraz w logach systemowych.

2 Nazwa własna

Nazwa własna certyfikatu została przypisana przez użytkownika w trakcie składania wniosku o wydanie certyfikatu KSeF. Jest to nazwa, którą użytkownik sam zdefiniował dla łatwiejszej identyfikacji certyfikatu.

Przykład: BTLA_certyfikat, Certyfikat_Firmy_2025, Cert-Offline-01

Ta nazwa jest używana również przy zapisywaniu plików certyfikatu na dysku lokalnym.

3 Przeznaczenie

Pole to określa **typ i przeznaczenie certyfikatu**. Wyświetlana jest jedna z dwóch możliwych wartości:

- **Podpis linku do weryfikacji wystawcy** - certyfikat typu 2 (offline) do oznaczania faktur w trybach szczególnych
- **Uwierzytelnienie w systemie KSeF** - certyfikat typu 1 do logowania się do systemu

4 Identyfikator podmiotu

To identyfikator (NIP lub PESEL), na który został wydany certyfikat KSeF. Certyfikat jest zawsze wydawany na identyfikator znajdujący się w środku uwierzytelnienia, którym użytkownik posłużył się do zalogowania przed złożeniem wniosku.

Ważna informacja: Identyfikatory NIP i PESEL są w systemie powiązane, co pozwala na ich zamienne użycie. W tabeli zostaną wyświetlone certyfikaty wydane na oba powiązane identyfikatory.

Opis pozycji tabeli zawartych w Liście certyfikatów

Informacje o właścicielu i statusie



[5] Nazwa właściciela certyfikatu

W tym polu wyświetlane jest pełne **imię i nazwisko właściciela certyfikatu** w przypadku osoby fizycznej lub **nazwa firmy** (nazwa podmiotu gospodarczego) w przypadku certyfikatu wydanego na podmiot inny niż osoba fizyczna.

Dane te są pobierane automatycznie z systemu na podstawie identyfikatora podatkowego i muszą być zgodne z danymi zgłoszonymi do urzędu skarbowego.



[6] Status certyfikatu

Status określa **aktualny stan certyfikatu** i jego możliwości użytkowe. System rozróżnia cztery możliwe statusy:

- Aktywny** - certyfikat jest w pełni ważny i można z jego użyciem dokonać uwierzytelnienia oraz wystawiać faktury w trybach szczególnych
- Zablokowany** - certyfikat jest w trakcie procesu unieważnienia i nie można go używać do żadnych operacji
- Unieważniony** - certyfikat został definitywnie unieważniony i nie można go już używać
- Wygasty** - dla certyfikatu minęła data końca ważności i nie można go już wykorzystać



[7] Ważny od

To **data początku okresu ważności certyfikatu**. Od tej daty użytkownik może rozpocząć używanie certyfikatu do uwierzytelnienia w systemie lub do oznaczania faktur w trybach szczególnych.

Data ta jest określona z dokładnością do dnia i została ustalona podczas składania wniosku o wydanie certyfikatu (albo wskazana przez użytkownika, albo automatycznie ustawiona przez system jako data wydania certyfikatu).

Lista certyfikatów									
Wniosek o certyfikat									
Filtrowanie									
	1	2	3	4	5	6	7	8	9
	Numer seryjny certyfikatu	Nazwa własna	Przeznaczenie	Identyfikator podmiotu, dla którego wystawiono certyfikat	Nazwa właściciela certyfikatu	Status	Ważny od	Ważny do	Data ostatniego użycia
☐	0199058253B29053	Certyfikat_testowy	Podpis linku	NIP: 3333333333	KSeF QA Tester	Aktywny	21.09.2025	21.09.2027	...

Opis pozycji tabeli zawartych w Liście certyfikatów

Okresy ważności i mechanizmy filtrowania

[8] Ważny do

Pole to pokazuje **datę końca ważności certyfikatu**, do której użytkownik może go wykorzystywać. Ważność certyfikatu KSeF określona jest z bardzo dużą dokładnością - nie tylko do dnia, ale także do godziny, minuty i sekundy.

Certyfikat może być ważny **maksymalnie przez okres 2 lat** od daty początku ważności. Po upływie tego okresu certyfikat automatycznie przechodzi w status „Wygasty” i nie może być już używany.

Ważne: Po przekroczeniu daty ważności certyfikat staje się bezużyteczny i konieczne jest złożenie wniosku o nowy certyfikat, jeśli użytkownik nadal chce korzystać z tej funkcjonalności.

[9] Data ostatniego użycia

To pole informuje o **dacie ostatniego wykorzystania certyfikatu** do uwierzytelnienia w systemie KSeF. Data ta jest automatycznie aktualizowana przez system za każdym razem, gdy certyfikat zostanie użyty do zalogowania.

Informacja ta może być pomocna przy:

- Identyfikowaniu certyfikatów, które nie są już używane
- Monitorowaniu aktywności certyfikatu
- Wykrywaniu potencjalnego nieautoryzowanego użycia

Funkcja filtrowania wyników

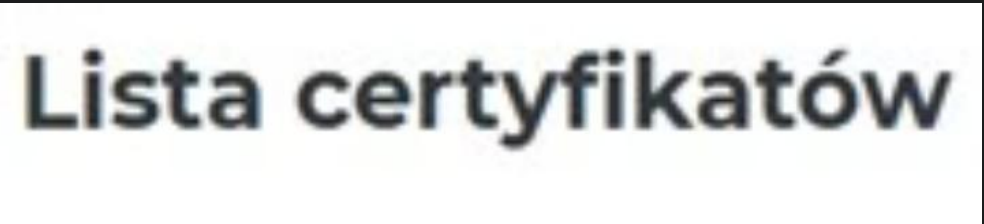
W przypadku gdy użytkownik posiada większą liczbę certyfikatów, aplikacja oferuje zaawansowaną możliwość **filtrowania wyników**. Aby zawęzić wyświetlane wyniki wyszukiwania, należy wprowadzić wybrane wartości w polach objętych filtrowaniem (takie jak status, przeznaczenie czy zakres dat).

W celu wyświetlenia zawężonych wyników należy kliknąć przycisk „Pokaż wyniki”. Jeśli chcemy usunąć wprowadzone filtry i powrócić do pełnej listy, należy kliknąć przycisk „Wyczyść” lub „Wyczyść wszystko”.

Opis pozycji tabeli zawartych w Liście certyfikatów

Wnioskowanie o nowy certyfikat z poziomu listy

Z poziomu strony **Lista certyfikatów** użytkownik ma również możliwość bezpośredniego przejścia do procesu składania wniosku o nowy certyfikat KSeF. Jest to wygodna funkcja, która pozwala na szybkie złożenie wniosku bez konieczności nawigowania przez menu główne aplikacji.



Możliwość wnioskowania o certyfikat jest dostępna wyłącznie wtedy, gdy **nie został wyczerpany żaden z limitów** jego wydawania określonych dla danego typu użytkownika. System automatycznie weryfikuje dostępne limity i aktywuje lub dezaktywuje odpowiedni przycisk.



Procedura wnioskowania

W celu przejścia do formularza składania wniosku o wydanie certyfikatu KSeF należy wybrać przycisk „Wnioskuj o certyfikat” umieszczony w prawym górnym rogu ekranu z listą certyfikatów. Po kliknięciu tego przycisku system przekieruje użytkownika do pierwszego kroku procesu generowania certyfikatu, który został szczegółowo opisany we wcześniejszych sekcjach tego dokumentu.

Filtrowanie

	Numer seryjny certyfikatu	Nazwa własna	Przeznaczenie	Identyfikator podmiotu, dla którego wystawiono certyfikat	Nazwa właściciela certyfikatu	Status	Ważny od	Ważny do	Data ostatniego użycia
☐	0199058253829053	Certyfikat_testowy	Podpis linku	NIP: 3333333333	KSeF QA Tester	Aktywny	21.09.2025	21.09.2027	---

Opis pozycji tabeli zawartych w Liście certyfikatów

Pobieranie certyfikatu z listy

Plik z certyfikatem można pobrać nie tylko bezpośrednio po zakończeniu procesu wydawania certyfikatu, jak to zostało opisane we wcześniejszych sekcjach. System umożliwia **pobranie certyfikatu w dowolnej chwili** z poziomu Listy certyfikatów, co jest szczególnie przydatne w następujących sytuacjach:

- Gdy użytkownik nie pobrał certyfikatu od razu po jego wydaniu
- Gdy plik certyfikatu został przypadkowo usunięty z dysku
- Gdy certyfikat ma być wykorzystany na innym urządzeniu
- Gdy potrzebna jest dodatkowa kopia zapasowa certyfikatu

Ważne ograniczenie

Z poziomu Listy certyfikatów można pobrać **wyłącznie certyfikaty KSeF w statusie „Aktywny”**. Status ten oznacza, że certyfikat został poprawnie wydany i jest w pełni ważny, gotowy do użycia.

Certyfikaty w innych statusach (Zablokowany, Unieważniony, Wygasły) nie są dostępne do pobrania, ponieważ nie mogą być już wykorzystywane w systemie.

Opis pozycji tabeli zawartych w Liście certyfikatów

Procedura pobierania certyfikatu - krok pierwszy

Proces pobierania certyfikatu z Listy certyfikatów składa się z kilku prostych kroków. Pierwszym z nich jest **zaznaczenie certyfikatu**, który użytkownik chce pobrać.

Krok [1] - Zaznaczenie certyfikatu

Aby pobrać wydany certyfikat, należy najpierw zaznaczyć go na liście certyfikatów. W tym celu należy **oznaczyć checkbox** (pole wyboru) znajdujący się w pierwszej kolumnie tabeli, w wierszu odpowiadającym wybranemu certyfikatowi.

System umożliwia **pobieranie od 1 do maksymalnie 10 certyfikatów w jednej operacji**. Oznacza to, że użytkownik może zaznaczyć kilka certyfikatów jednocześnie, a system pobierze je wszystkie jako paczkę w formacie archiwum ZIP.

Praca z wieloma certyfikatami

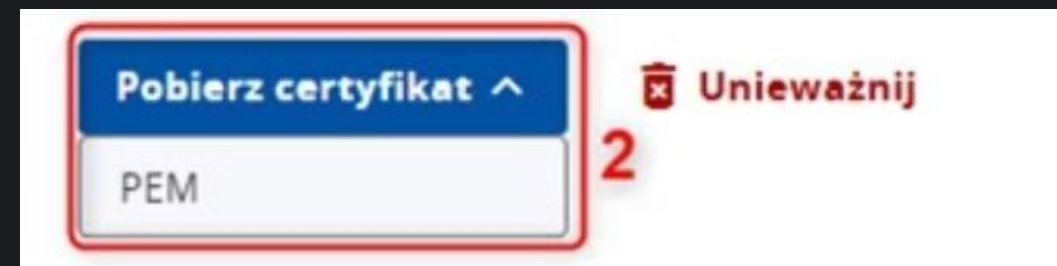
W przypadku gdy użytkownik posiada większą liczbę certyfikatów i chce pobrać więcej niż 10 certyfikatów, zaleca się wykorzystanie funkcji filtrowania dostępnej w aplikacji.

Dzięki filtrowaniu można ograniczyć listę wyświetlanych certyfikatów wyłącznie do tych, które mają zostać pobrane. Na przykład można ustawić filtr według:

- Przeznaczenia certyfikatu (uwierzytelnienie lub offline)
- Zakresu dat ważności
- Nazwy własnej certyfikatu

▼ Filtrowanie

	Numer seryjny certyfikatu	Nazwa własna	Przeznaczenie	Identyfikator podmiotu, dla którego wystawiono certyfikat	Nazwa właściciela certyfikatu	Status	
1	☒	019905B253B29053	Certyfikat_testowy	Podpis linku	NIP: 3333333333	KSeF QA Tester	Aktywny
	☐	015AAA5C18BED4CE	Certyfikat_testowy_1	Uwierzytelnienie	NIP: 3333333333	KSeF QA Tester	Aktywny



Opis pozycji tabeli zawartych w Liście certyfikatów

Procedura pobierania certyfikatu - wybór formatu

Po zaznaczeniu przynajmniej jednego certyfikatu na liście, przycisk **[2] Pobierz certyfikat** stanie się aktywny i możliwy do kliknięcia. Wcześniej przycisk ten jest nieaktywny (wyszarzony), co zapobiega przypadkowemu kliknięciu bez wybrania certyfikatu.

Wybór formatu PEM

Aby pobrać zaznaczony certyfikat lub certyfikaty, należy rozwinąć przycisk **[2] Pobierz certyfikat** i wybrać format PEM. Jest to standardowy format certyfikatów cyfrowych, który jest zgodny z wymaganiami systemu KSeF oraz większości aplikacji wykorzystujących certyfikaty.

Format PEM (Privacy Enhanced Mail) to tekstowy format kodowania dla certyfikatów, który wykorzystuje kodowanie Base64. Certyfikaty w tym formacie są łatwo przenośne między różnymi systemami i aplikacjami.

Co się dzieje po wyborze formatu?

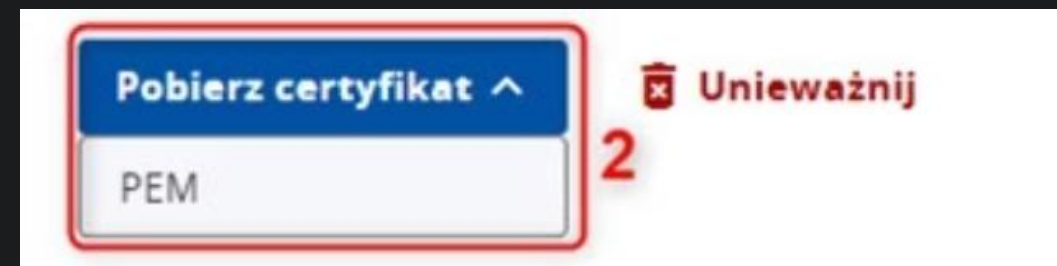
Po wybraniu formatu PEM system automatycznie inicjuje proces pobierania certyfikatu. W zależności od ustawień przeglądarki internetowej użytkownika:

- Plik może zostać automatycznie zapisany w domyślnym folderze pobierania
- Może pojawić się okno dialogowe z prośbą o wskazanie lokalizacji zapisu
- Plik może pojawić się na pasku pobierania w dolnej części przeglądarki

Zaleca się natychmiastowe przeniesienie pobranego certyfikatu do bezpiecznej lokalizacji i usunięcie go z folderu domyślnego pobierania, jeśli taki został użyty przez przeglądarkę.

Filtrowanie

	Numer seryjny certyfikatu	Nazwa własna	Przeznaczenie	Identyfikator podmiotu, dla którego wystawiono certyfikat	Nazwa właściciela certyfikatu	Status	
1	☒	019905B253B29053	Certyfikat_testowy	Podpis linku	NIP: 3333333333	KSeF QA Tester	Aktywny
	☐	015AAA5C18BED4CE	Certyfikat_testowy_1	Uwierzytelnienie	NIP: 3333333333	KSeF QA Tester	Aktywny



Opis pozycji tabeli zawartych w Liście certyfikatów

Konwencje nazewnictwa plików certyfikatów

Pojedynczy certyfikat

System automatycznie pobierze certyfikat na urządzenie użytkownika zgodnie z ustalonymi zasadami nazewnictwa. **Certyfikat jest zapisywany pod nazwą własną certyfikatu**, która została zdefiniowana przez użytkownika w trakcie składania wniosku o wydanie certyfikatu.

Certyfikaty KSeF są pobierane w formacie PEM z rozszerzeniem pliku **.crt** (certificate). Przykładowo, jeśli nazwa własna certyfikatu to „moj_certyfikat”, plik zostanie zapisany jako:

✔ Pobrano certyfikat Certyfikat_testowy.crt w formacie PEM.

Ta konwencja nazewnictwa zapewnia, że użytkownik może łatwo zidentyfikować pobrany certyfikat na podstawie nadanej mu wcześniej nazwy.

Wiele certyfikatów jednocześnie

Jeżeli użytkownik zaznaczy i pobierze **kilka certyfikatów jednocześnie**, system zastosuje inną strategię zapisywania plików. Zamiast osobnych plików dla każdego certyfikatu, system zapisze wszystkie certyfikaty w formie **archiwum ZIP**.

Paczka certyfikatów jest zapisywana pod automatycznie wygenerowaną nazwą zawierającą aktualną datę:

✔ Pobrano paczkę Certyfikaty_KSeF_20250921.zip zaznaczonych certyfikatów w formacie PEM.

Gdzie data jest zapisana w formacie RRRRMMDD (rok-miesiąc-dzień), na przykład: Certyfikaty_KSeF_20251115.zip

Po rozpakowaniu archiwum ZIP użytkownik znajdzie wewnątrz poszczególne pliki certyfikatów, każdy zapisany pod swoją nazwą własną z rozszerzeniem .crt.

Opis pozycji tabeli zawartych w Liście certyfikatów

Pobrać można jedynie certyfikat z kluczem publicznym

Jest to **absolutnie fundamentalna informacja**, którą każdy użytkownik musi zrozumieć i zapamiętać. System KSeF przechowuje i umożliwia pobieranie wyłącznie certyfikatu zawierającego klucz publiczny. **Klucz prywatny nigdy nie jest przesyłany do systemu KSeF** i pozostaje wyłącznie na urządzeniu użytkownika, na którym został pierwotnie wygenerowany.

Co to oznacza w praktyce?

Jeśli w jakikolwiek sposób dostęp do klucza prywatnego zostanie utracony - na przykład przez przypadkowe usunięcie pliku, utratę urządzenia, awarię dysku twardego lub zapomnienie hasła zabezpieczającego klucz - ponowne pobranie istniejącego certyfikatu z systemu KSeF **nie przywróci zdolności do uwierzytelniania czy autoryzowania faktur**.

Pobrany certyfikat będzie zawierał wyłącznie klucz publiczny, który sam w sobie nie pozwala na wykonywanie operacji wymagających posiadania pary kluczy (publicznego i prywatnego).

Konsekwencje utraty klucza prywatnego

Klucz prywatny konieczny do uwierzytelnienia w systemie oraz do oznaczania faktur w trybach szczególnych posiada **wyłącznie użytkownik**. System KSeF nigdy nie ma dostępu do tego klucza i z tego powodu nie może go odzyskać ani udostępnić ponownie. W przypadku utraty klucza prywatnego jedynym rozwiązaniem jest:

1. Unieważnienie starego certyfikatu (jeśli to możliwe)
2. Złożenie wniosku o wydanie nowego certyfikatu
3. Wygenerowanie nowej pary kluczy

Dlatego tak istotne jest bezpieczne przechowywanie klucza prywatnego oraz hasła do niego. Zaleca się tworzenie kopii zapasowych klucza prywatnego w bezpiecznych lokalizacjach (np. na zewnętrznym dysku twardym przechowywanym w sejfie lub w zaszyfrowanej chmurze).

Opis pozycji tabeli zawartych w Liście certyfikatów

Unieważnianie certyfikatu - podstawowe informacje

Z poziomu Listy certyfikatów dostępna jest również funkcja **unieważniania certyfikatu**. Unieważnienie certyfikatu to nieodwracalna operacja, która skutecznie uniemożliwia dalsze wykorzystywanie certyfikatu w systemie KSeF.

Zasady unieważniania

Certyfikat KSeF można unieważnić **wyłącznie pojedynczo** - system nie umożliwia jednoczesnego unieważnienia kilku certyfikatów w jednej operacji. Jest to celowe zabezpieczenie mające zapobiec przypadkowemu unieważnieniu wielu certyfikatów naraz.

Użytkownik może unieważniać **tylko certyfikaty własne**, czyli takie, które zostały wydane na jego identyfikator podatkowy. Nie ma możliwości unieważnienia certyfikatu należącego do innej osoby lub podmiotu.

Wymagania uwierzytelnienia

Aby unieważnić certyfikat zawierający dany identyfikator (NIP lub PESEL), **należy uwierzytelnić się środkiem uwierzytelnienia zawierającym ten sam identyfikator**. Na przykład:

- Jeśli certyfikat został wydany na NIP firmy, należy zalogować się przy użyciu pieczęci kwalifikowanej tej firmy
- Jeśli certyfikat został wydany na PESEL osoby fizycznej, należy zalogować się profilem zaufanym lub podpisem kwalifikowanym tej osoby

Powiązanie NIP-PESEL

Proces unieważniania certyfikatu KSeF uwzględnia powiązanie NIP-PESEL, pozwalające na zamienne użycie identyfikatorów podatkowych NIP i PESEL identyfikujących tę samą osobę. W praktyce oznacza to, że:

- Można uwierzytelnić się z użyciem numeru PESEL i unieważnić certyfikaty KSeF wydane na powiązany NIP
- Można uwierzytelnić się z użyciem NIP i unieważnić certyfikaty KSeF wydane na powiązany PESEL

Opis pozycji tabeli zawartych w Liście certyfikatów

Procedura unieważniania certyfikatu - krok pierwszy

Aby **unieważnić wydany certyfikat**, należy najpierw dokonać jego wyboru na liście certyfikatów. Proces ten jest analogiczny do procesu pobierania certyfikatu, ale z kluczową różnicą - można wybrać tylko jeden certyfikat naraz.

Krok [1] - Zaznaczenie certyfikatu

Należy zaznaczyć certyfikat przeznaczony do unieważnienia na liście certyfikatów, **oznaczając checkbox w tabeli** (pole wyboru znajdujące się w pierwszej kolumnie). System umożliwia zaznaczenie wyłącznie jednego certyfikatu - jeśli użytkownik zaznaczy więcej niż jeden, przycisk „Unieważnij” pozostanie nieaktywny.

W jednej operacji można unieważnić **tylko jeden certyfikat**. Jest to świadome ograniczenie mające na celu ochronę przed przypadkowym unieważnieniem większej liczby certyfikatów.

Krok [2] - Aktywacja przycisku

Po wyborze dokładnie jednego certyfikatu przycisk **[2] Unieważnij** stanie się aktywny i będzie możliwy do kliknięcia. Wcześniej przycisk ten jest nieaktywny (wyszarzony), co zapobiega przypadkowemu uruchomieniu procesu unieważniania.

Przed kliknięciem przycisku warto jeszcze raz upewnić się, że zaznaczony został właściwy certyfikat - operacja unieważnienia jest nieodwracalna.

▼ Filtrowanie

	Numer seryjny certyfikatu	Nazwa własna	Przeznaczenie	Identyfikator podmiotu, dla którego wystawiono certyfikat	Nazwa właściciela certyfikatu	Status	
1	☒	019905B253B29053	Certyfikat_testowy	Podpis linku	NIP: 3333333333	KSeF QA Tester	Aktywny
	☐	015AAA5C188ED4CE	Certyfikat_testowy_1	Uwierzytelnienie	NIP: 3333333333	KSeF QA Tester	Aktywny



Opis pozycji tabeli zawartych w Liście certyfikatów

Wybór powodu unieważnienia certyfikatu

Po wybraniu przycisku **[2] Unieważnij** system wyświetli okno dialogowe z polem **[3] Powód unieważnienia**. Jest to rozwijalna lista wyboru, z której należy wybrać jeden z dostępnych powodów unieważnienia certyfikatu.

Lista dostępnych powodów

System oferuje trzy kategorie powodów unieważnienia, które obejmują najczęstsze scenariusze:

1. Certyfikat został zastąpiony nowym

Ten powód należy wybrać, gdy certyfikat nie będzie już wykorzystywany, ponieważ został zastąpiony nowym certyfikatem. Najczęściej dotyczy to sytuacji, gdy użytkownik wygenerował nowy certyfikat z przesuniętym okresem ważności lub z innymi parametrami, a stary certyfikat nie jest już potrzebny.

Przykład: Przedsiębiorca wygenerował nowy certyfikat z datą ważności przesuniętą o rok do przodu i chce unieważnić stary certyfikat, aby zachować porządek w liście certyfikatów.

Unieważnić wybrany certyfikat?



Operacji nie będzie już można cofnąć

Powód unieważnienia * **3**

Wybierz



Pole wymagane

2. Bezpieczeństwo klucza prywatnego zostało naruszone

To najpoważniejszy powód unieważnienia. Należy go wybrać, gdy właściciel **utracił kontrolę nad kluczem prywatnym** do certyfikatu lub doszło do ujawnienia klucza prywatnego osobom trzecim.

Przykłady: kradzież urządzenia z kluczem prywatnym, przypadkowe przestanie klucza prywatnego niezabezpieczoną pocztą email, podejrzenie włamania do systemu, w którym przechowywany jest klucz, ujawnienie hasła zabezpieczającego klucz.

3. Powód unieważnienia nie jest określony

Ten ogólny powód należy wybrać, gdy decyzja o unieważnieniu certyfikatu **nie wynika bezpośrednio** z zastąpienia certyfikatu nowym ani z kompromitacji bezpieczeństwa klucza prywatnego.

Przykłady: zmiana struktury organizacyjnej firmy, zaprzestanie korzystania z określonej funkcjonalności KSeF, reorganizacja systemu zarządzania certyfikatami, inne przyczyny administracyjne.

Opis pozycji tabeli zawartych w Liście certyfikatów

Finalizacja procesu unieważniania

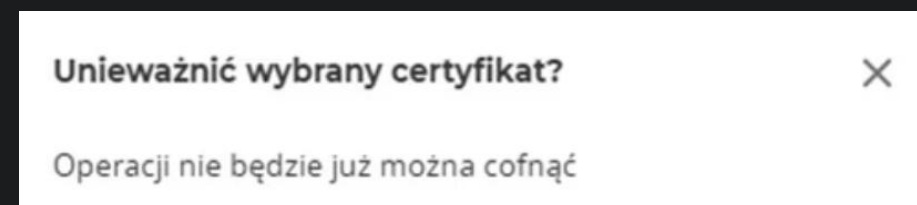
Możliwość anulowania

Po wyborze powodu unieważnienia z listy, użytkownik ma jeszcze **ostatnią szansę na rezygnację** z unieważnienia certyfikatu. W tym celu należy użyć przycisku **[5] Anuluj**.

Kliknięcie przycisku „Anuluj” spowoduje:

- Zamknięcie okna dialogowego
- Powrót do Listy certyfikatów
- Certyfikat pozostanie ważny i aktywny
- Żadne zmiany nie zostaną wprowadzone

Jest to ostatnia chwila na zmianę decyzji przed nieodwracalnym unieważnieniem certyfikatu.



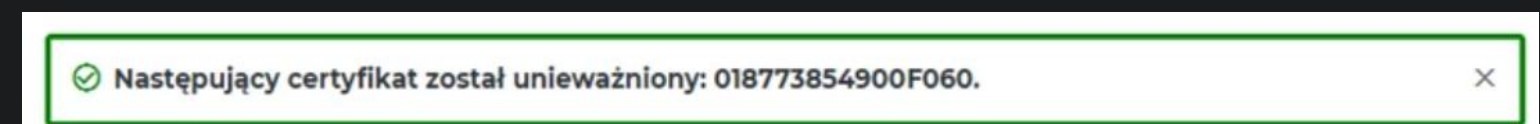
Potwierdzenie unieważnienia

Aby **definitywnie potwierdzić unieważnienie certyfikatu**, należy użyć przycisku **[4] Unieważnij certyfikat**. Po kliknięciu tego przycisku:

- System rozpocznie proces unieważniania certyfikatu
- Operacja ta jest **całkowicie nieodwracalna**
- Certyfikat nie będzie mógł być ponownie aktywowany
- Będzie konieczne wygenerowanie nowego certyfikatu, jeśli funkcjonalność będzie potrzebna w przyszłości

Potwierdzenie operacji

Po pomyślnym zakończeniu procesu unieważniania certyfikatu, system wyświetli komunikat potwierdzający wykonanie operacji. Status certyfikatu na Liście certyfikatów zmieni się natychmiast lub po krótkim czasie przetwarzania.



Opis pozycji tabeli zawartych w Liście certyfikatów

Statusy certyfikatu po unieważnieniu

Po zleceniu unieważnienia certyfikatu, jego status na Liście certyfikatów może przyjąć jedną z dwóch wartości, w zależności od szybkości przetwarzania operacji przez system KSeF.

Status „Unieważniony”

Certyfikat może pojawić się na liście **od razu w statusie „Unieważniony”**. Oznacza to, że proces unieważniania certyfikatu został zakończony natychmiast i certyfikat jest już całkowicie nieaktywny. Jest to najczęstsza sytuacja, gdy system przetwarza żądanie bardzo szybko.

Certyfikat w tym statusie:

- Nie może być używany do żadnych operacji w systemie KSeF
- Nie może być ponownie aktywowany
- Nadal jest widoczny na liście certyfikatów dla celów historycznych i audytowych

Status „Zablokowany”

W niektórych przypadkach certyfikat może pojawić się w statusie „Zablokowany”. Oznacza to, że **proces unieważniania certyfikatu został uruchomiony, ale jeszcze jest w trakcie realizacji**. System przetwarza żądanie i za chwilę zmieni status na „Unieważniony”.

Certyfikat w tym statusie:

- Jest traktowany jak unieważniony - nie można go używać
- Za moment automatycznie zmieni status na „Unieważniony”
- Nie wymaga żadnych dodatkowych działań ze strony użytkownika

Kluczowa zasada bezpieczeństwa

Certyfikatów KSeF w statusach „Unieważniony” i „Zablokowany” absolutnie nie można używać do jakichkolwiek operacji w systemie KSeF. Próba użycia takiego certyfikatu zakończy się błędem lub zostanie odrzucona przez system.

Certyfikatu w statusie „Unieważniony” lub „Zablokowany” nie wolno pod żadnym pozorem użyć do oznaczania faktur w trybach szczególnych, ponieważ faktura oznaczona przy użyciu nieważnego certyfikatu **nie spełnia wymogów ustawowych** i może być uznana za nieprawidłowo wystawioną przez organy skarbowe.

Opis rodzajów podmiotu

Klasyfikacja podmiotów w systemie KSeF

System KSeF rozróżnia różne rodzaje podmiotów, które mogą składać wnioski o certyfikaty i korzystać z systemu. Każdy rodzaj podmiotu ma swoje specyficzne cechy i wymagania. Poniżej przedstawiono szczegółowy opis poszczególnych kategorii.

1	2	3
Podmiot niebędący osobą fizyczną Do tej kategorii zaliczają się osoby prawne, organizacje oraz inne podmioty niebędące osobą fizyczną. Obejmuje to szerokie spektrum jednostek organizacyjnych działających w obrocie gospodarczym. Przykłady podmiotów w tej kategorii: • Spółki z ograniczoną odpowiedzialnością (sp. z o.o.) • Spółki akcyjne (S.A.) • Spółki komandytowe i komandytowo-akcyjne • Fundacje i stowarzyszenia • Instytucje publiczne • Jednostki samorządu terytorialnego Podmioty te uwierzytelniają się w systemie przy użyciu kwalifikowanej pieczęci elektronicznej, która jest odpowiednikiem podpisu elektronicznego dla jednostek organizacyjnych.	Organ egzekucyjny Ta kategoria jest zaznaczana w przypadku, gdy organizacja wnioskująca pełni również rolę organu egzekucyjnego. Jest to szczególna funkcja związana z wykonywaniem określonych uprawnień władczych. W takim przypadku oprócz zaznaczenia pola „organ egzekucyjny” należy również zaznaczyć pole „podmiot niebędący osobą fizyczną”, ponieważ organ egzekucyjny zawsze jest jednostką organizacyjną, a nie osobą fizyczną. Przykłady organów egzekucyjnych: • Komornik sądowy • Urząd skarbowy (w kontekście egzekucji należności) • Zakład Ubezpieczeń Społecznych (przy egzekucji składek)	Osoba fizyczna To pole zaznacza się w specyficznych przypadkach związanych ze zgłaszaniem danych unikalnych powiązanych z certyfikatem kwalifikowanego podpisu elektronicznego podatnika będącego osobą fizyczną. Dotyczy to sytuacji, gdy certyfikat kwalifikowanego podpisu nie zawiera numeru identyfikacji podatkowej (NIP) ani numeru PESEL podatnika będącego osobą fizyczną. W takim przypadku wykorzystywane są dane wyznaczone z tego certyfikatu po użyciu funkcji skrótu kryptograficznego opartej na algorytmie SHA-256. Ten mechanizm, znany jako „<i>odcisk palca podpisu kwalifikowanego</i>”, pozwala na jednoznaczną identyfikację użytkownika bez konieczności posiadania w certyfikacie bezpośrednio numeru NIP czy PESEL.

Rodzaje identyfikatora osoby wskazanej do pracy w KSeF

Identyfikatory podatkowe

System KSeF umożliwia różne sposoby identyfikacji osób upoważnionych do pracy w systemie. Wybór odpowiedniego identyfikatora zależy od sytuacji konkretnego użytkownika oraz posiadanych przez niego dokumentów tożsamości.

Identyfikator NIP

NIP (Numer Identyfikacji Podatkowej) to podstawowy identyfikator dla osób prowadzących działalność gospodarczą oraz dla podmiotów prawnych. Przy wyborze tego identyfikatora należy podać:

- **Numer NIP** wskazanej osoby
- **Imię i nazwisko** wskazanej osoby
- **Adres e-mail** (pole obowiązkowe) - na ten adres zostanie przesłana informacja systemowa o zrealizowaniu formularza ZAW-FA, zarówno przy nadawaniu, jak i odbieraniu uprawnień
- **Numer telefonu kontaktowego** (pole dobrowolne) - dla celów komunikacyjnych

NIP jest wymagany dla wszystkich przedsiębiorców prowadzących działalność gospodarczą, niezależnie od jej formy prawnej.

Identyfikator PESEL

PESEL to uniwersalny numer identyfikacyjny osoby fizycznej w Polsce. Przy wyborze tego identyfikatora należy podać:

- **Numer PESEL** wskazanej osoby
- **Imię i nazwisko** wskazanej osoby
- **Adres e-mail** (pole obowiązkowe) - na ten adres zostanie przesłana informacja systemowa o zrealizowaniu formularza ZAW-FA, zarówno przy nadawaniu, jak i odbieraniu uprawnień
- **Numer telefonu kontaktowego** (pole dobrowolne)

PESEL może być używany przez osoby fizyczne, które nie prowadzą działalności gospodarczej lub w przypadkach, gdy powiązanie NIP-PESEL jest wykorzystywane do zarządzania uprawnieniami.

Rodzaje identyfikatora osoby wskazanej do pracy w KSeF

Brak identyfikatora - rejestracja nierezydentów

System KSeF przewiduje również możliwość rejestracji osób, które **nie posiadają polskiego identyfikatora podatkowego**. Ta opcja jest przeznaczona przede wszystkim dla nierezydentów, którzy nie mają przypisanego numeru NIP ani PESEL, ale muszą korzystać z polskiego systemu elektronicznych faktur.

Kiedy stosować?

Opcję „Brak identyfikatora” należy **zaznaczyć/wypełnić w przypadku nierezydenta**, który nie posiada identyfikatora podatkowego w Polsce. Dotyczy to na przykład:

- Przedsiębiorców zagranicznych prowadzących działalność w Polsce
- Pracowników zagranicznych firm delegowanych do pracy w Polsce
- Innych osób zobowiązanych do wystawiania faktur w polskim systemie KSeF, które nie posiadają polskiego NIP ani PESEL

Wymagane dane podstawowe

W przypadku wyboru opcji „Brak identyfikatora” system wymaga podania szerszego zestawu danych identyfikacyjnych, który zastępuje standardowy identyfikator podatkowy:

- **Imię i nazwisko** wskazanej osoby (pełne dane zgodne z dokumentem tożsamości)
- **Data urodzenia** w formacie DD-MM-RRRR
- **Adres e-mail** (pole obowiązkowe)
- **Numer telefonu kontaktowego** (pole dobrowolne)

01

Rodzaj dokumentu potwierdzającego tożsamość

Należy wybrać z listy rozwijanej typ dokumentu, na podstawie którego następuje identyfikacja osoby. Dostępne opcje to zazwyczaj: paszport, dowód osobisty (dla obywateli UE), karta pobytu, lub inny dokument tożsamości uznawany na terytorium Polski.

02

Numer i seria dokumentu potwierdzającego tożsamość

Należy wpisać **pełny numer oraz serię dokumentu** (jeśli dokument posiada serię). Dane te muszą być dokładnie zgodne z informacjami zawartymi w oryginalnym dokumencie tożsamości.

03

Kraj wydania dokumentu potwierdzającego tożsamość

Należy wskazać państwo, które wydało dokument tożsamości. Informacja ta jest kluczowa dla weryfikacji autentyczności dokumentu oraz dla celów międzynarodowej wymiany informacji podatkowych.

❏ **Obowiązek podania adresu e-mail:** Niezależnie od wybranego rodzaju identyfikatora, system **zawsze wymaga podania adresu e-mail**. Na wskazany adres zostanie przesłana informacja systemowa o zrealizowaniu formularza ZAW-FA - zarówno przy nadawaniu uprawnień, jak i przy ich odbieraniu. Adres e-mail jest kluczowym kanałem komunikacji między systemem KSeF a użytkownikiem.