

Moduł Certyfikatów i Uprawnień KSeF

Kompleksowy przewodnik po logowaniu, nadawaniu uprawnień i zarządzaniu dostępem do systemu KSeF 2.0



Jak uzyskać dostęp do MCU?

Moduł Certyfikatów i Uprawnień KSeF jest dostępny pod dwoma adresami internetowymi, co zapewnia elastyczność w dostępie do systemu. Główny adres to **https://mcu.mf.gov.pl/web/login**, natomiast alternatywnie można skorzystać z adresu **https://ksef.mf.gov.pl/web/**.

Oba adresy prowadzą do tego samego systemu, więc przedsiębiorca może wybrać ten, który jest dla niego wygodniejszy lub łatwiejszy do zapamiętania. Warto zapisać wybrany adres w zakładkach przeglądarki, aby mieć szybki dostęp do modułu MCU w każdej chwili.

System jest dostępny przez całą dobę, siedem dni w tygodniu, co pozwala na zarządzanie uprawnieniami i certyfikatami w dogodnym dla użytkownika czasie. Przed pierwszym logowaniem warto upewnić się, że posiadamy odpowiednie środki uwierzytelnienia, takie jak Profil Zaufany lub certyfikat kwalifikowany.

Ekran startowy MCU

Pierwsze kroki w systemie

Po wejściu na stronę MCU użytkownik zostaje powitany ekranem startowym, który stanowi bramę do całego systemu. Ten ekran jest zaprojektowany w sposób intuicyjny i przejrzysty, aby ułatwić rozpoczęcie pracy z modułem.

Ekran startowy pełni kluczową funkcję - pozwala na rozpoczęcie procesu uwierzytelnienia w aplikacji. To właśnie tutaj użytkownik podejmuje decyzję o metodzie, którą chce się zalogować do systemu.

Proces uwierzytelnienia rozpoczyna się od wyboru odpowiedniej metody autoryzacji, która najlepiej odpowiada potrzebom i możliwościom użytkownika. System oferuje kilka opcji, aby zapewnić maksymalną dostępność dla wszystkich przedsiębiorców.

Dostępne metody

- Profil Zaufany - bezpłatne rozwiązanie dla każdego
- Certyfikat kwalifikowany z NIP lub PESEL
- Certyfikat kwalifikowany bez NIP i PESEL



Metody uwierzytelnienia w MCU

Profil Zaufany

Bezpłatne rozwiązanie dostępne dla każdego przedsiębiorcy. Umożliwia logowanie za pomocą Podpisu Zaufanego, który jest wydawany przez zaufane instytucje publiczne. To najprostsza i najczęściej wybierana metoda autoryzacji.

Certyfikat kwalifikowany

Rozwiązanie płatne, przeznaczone dla posiadaczy certyfikatów kwalifikowanych lub pieczęci kwalifikowanej. Zapewnia najwyższy poziom bezpieczeństwa i jest szczególnie polecane dla firm prowadzących intensywną działalność w systemie e-faktur.

Odcisk palca certyfikatu

Specjalne rozwiązanie pomocne w sytuacji, gdy posiadany certyfikat kwalifikowany nie zawiera identyfikatora NIP ani PESEL. Użycie tego certyfikatu wymaga uprzedniego nadania uprawnień na tzw. odcisk palca certyfikatu.

Rozpoczęcie procesu logowania

Proces logowania do MCU składa się z kilku prostych, ale ważnych kroków. Każdy z nich został zaprojektowany tak, aby zapewnić maksymalne bezpieczeństwo przy jednoczesnym zachowaniu wygody użytkowania.

01

Wprowadzenie kontekstu logowania

Użytkownik wybiera rodzaj identyfikatora: NIP firmy, identyfikator wewnętrzny lub VAT-UE. To kluczowy krok, który określa, w jakim kontekście będziemy pracować w systemie.

02

Wypełnienie formularza

Pole formularza dynamicznie dostosowuje się do wybranego w pierwszym kroku rodzaju identyfikatora, co ułatwia wprowadzenie prawidłowych danych.

03

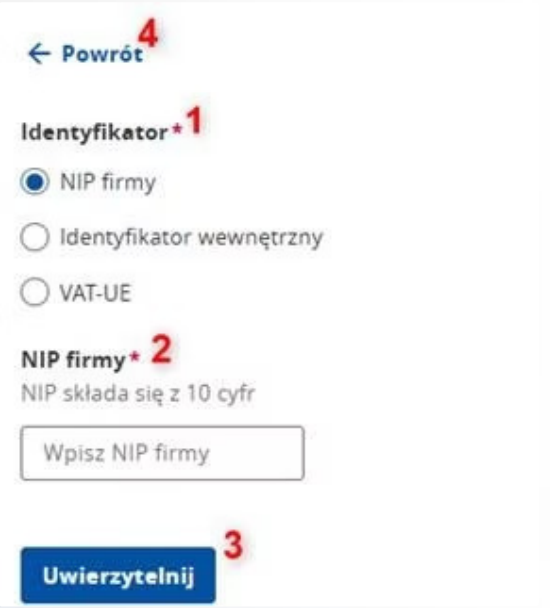
Uwierzytelnienie

Po wpisaniu numeru identyfikatora wybieramy przycisk "Uwierzytelnij", który przenosi nas do kolejnego etapu procesu logowania.

04

Możliwość powrotu

W każdym momencie możemy wrócić do poprzedniego ekranu, wybierając przycisk "Powrót", co pozwala na korektę wprowadzonych danych.



Profil zaufany i mObywatel

Profil Zaufany to narzędzie identyfikacyjne stworzone przez administrację publiczną, które pozwala potwierdzić tożsamość obywatela w usługach państwowych bez konieczności osobistej wizyty w urzędzie. Działa jak „cyfrowy dowód" – umożliwia podpisywanie wniosków, logowanie do systemów publicznych i potwierdzanie działań wymagających uwierzytelnienia. Opiera się na bezpiecznym mechanizmie powiązania użytkownika z jego danymi, a każda operacja jest rejestrowana i chroniona.

Aplikacja mObywatel pełni natomiast funkcję cyfrowego portfela dokumentów i narzędzia do obsługi usług administracji z poziomu telefonu. Umożliwia korzystanie z dokumentów elektronicznych, odbieranie urzędowych powiadomień, zarządzanie dostępami oraz wykonywanie czynności wymagających potwierdzenia tożsamości. System integruje dane z wielu rejestrów publicznych, co pozwala użytkownikowi na szybkie potwierdzanie uprawnień, pobieranie zaświadczeń czy autoryzację dostępu w usługach cyfrowych.

W praktyce Profil Zaufany oraz mObywatel tworzą wspólny ekosystem identyfikacji elektronicznej, który ma zapewnić jednolite, bezpieczne i zgodne z przepisami potwierdzanie tożsamości w kontaktach z administracją, w tym w systemach takich jak KSeF.

Autoryzacja certyfikatem - krok pierwszy

Proces autoryzacji za pomocą certyfikatu kwalifikowanego rozpoczyna się od kluczowego pytania o zawartość certyfikatu. System musi wiedzieć, czy certyfikat, którego zamierzamy użyć, zawiera identyfikator NIP lub PESEL.

Na ekranie pojawia się pytanie z dwoma opcjami do wyboru. Pierwsza opcja dotyczy certyfikatów zawierających identyfikator NIP lub PESEL, druga - certyfikatów, które takich identyfikatorów nie posiadają. Wybór odpowiedniej opcji jest kluczowy dla dalszego przebiegu procesu autoryzacji.

Po dokonaniu wyboru użytkownik może przejść do następnego ekranu, klikając przycisk umożliwiający kontynuację. W każdej chwili istnieje również możliwość powrotu do poprzedniego ekranu za pomocą dedykowanego przycisku "Powrót".





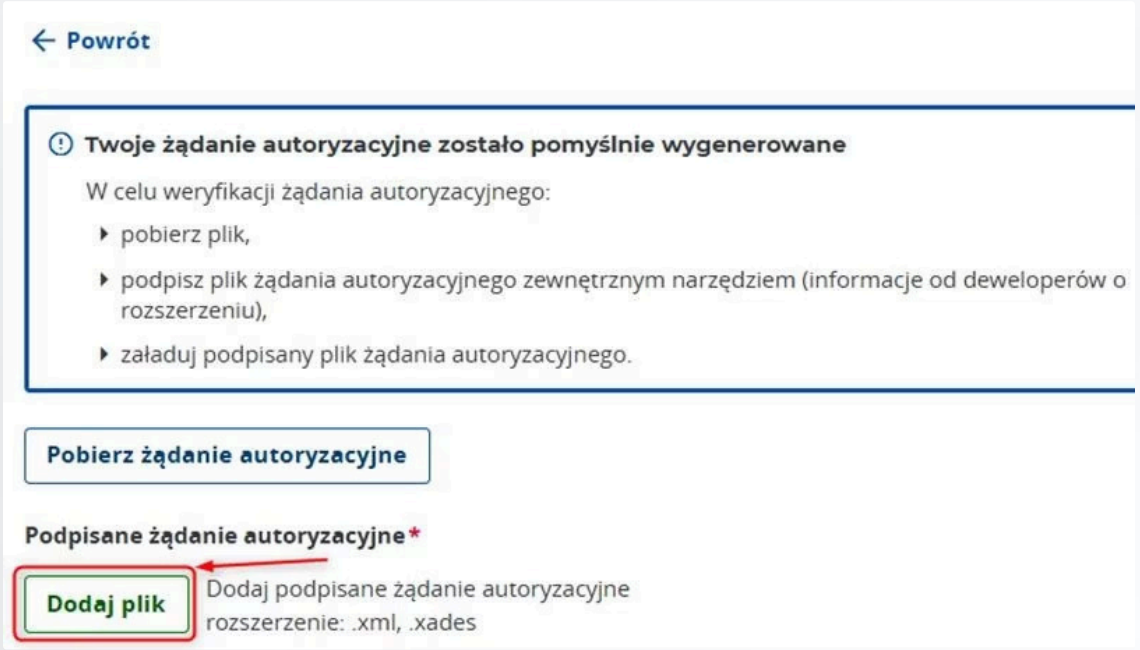
Pobieranie żądania autoryzacyjnego

Po określeniu typu certyfikatu system przechodzi do kluczowego etapu - generowania i pobierania żądania autoryzacyjnego. Ten etap jest niezbędny do bezpiecznego potwierdzenia tożsamości użytkownika.

Na ekranie pojawia się przycisk "Pobierz żądanie autoryzacyjne". Po jego kliknięciu system rozpoczyna proces generowania specjalnego pliku, który należy zapisać na dysku komputera. Ten plik jest unikalny dla każdej sesji logowania i zawiera zaszyfrowane dane niezbędne do autoryzacji.

Pobrany plik należy następnie podpisać za pomocą posiadanego certyfikatu kwalifikowanego lub pieczęci kwalifikowanej. Proces podpisywania odbywa się lokalnie na komputerze użytkownika, przy użyciu oprogramowania obsługującego certyfikaty kwalifikowane.

W każdej chwili można wrócić do poprzedniego ekranu, klikając przycisk "Powrót", jeśli zajdzie potrzeba zmiany wcześniej wprowadzonych informacji.

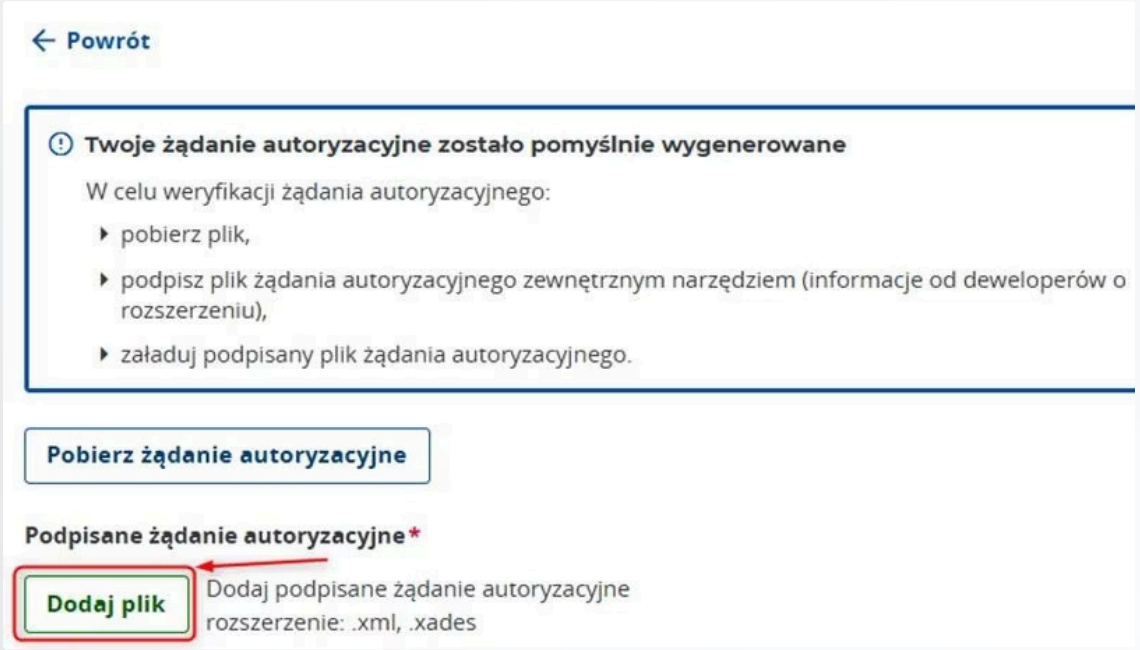


Potwierdzenie pobrania żądania

Po pomyślnym wygenerowaniu i pobraniu żądania autoryzacyjnego system wyświetla komunikat potwierdzający, że operacja zakończyła się sukcesem. Ten ekran informuje użytkownika, że plik został prawidłowo utworzony i zapisany na dysku komputera.

Teraz użytkownik powinien odszukać pobrany plik na swoim komputerze i podpisać go za pomocą certyfikatu kwalifikowanego. Proces podpisywania wymaga użycia specjalistycznego oprogramowania do obsługi certyfikatów, które powinno być zainstalowane na komputerze użytkownika.

Po podpisaniu pliku należy wrócić do aplikacji MCU i przejść do kolejnego kroku, który polega na przesłaniu podpisanego dokumentu z powrotem do systemu. Cały proces jest zabezpieczony wielopoziomowym szyfrowaniem, co gwarantuje najwyższy poziom bezpieczeństwa.



Przesyłanie podpisanego pliku

Po podpisaniu żądania autoryzacyjnego na swoim komputerze, użytkownik musi przesłać podpisany plik z powrotem do systemu MCU. Ten krok jest kluczowy dla zakończenia procesu autoryzacji.

Na ekranie pojawia się przycisk "Dodaj plik", który po kliknięciu otwiera standardowe okno wyboru plików w systemie operacyjnym. Użytkownik powinien odszukać na dysku podpisany wcześniej plik i go wybrać.

Bardzo ważne jest, aby załączany dokument miał odpowiednie rozszerzenie - system akceptuje wyłącznie pliki z rozszerzeniem .xml lub .xades. Są to standardowe formaty dla dokumentów podpisanych elektronicznie, które zapewniają integralność i autentyczność przesyłanych danych.

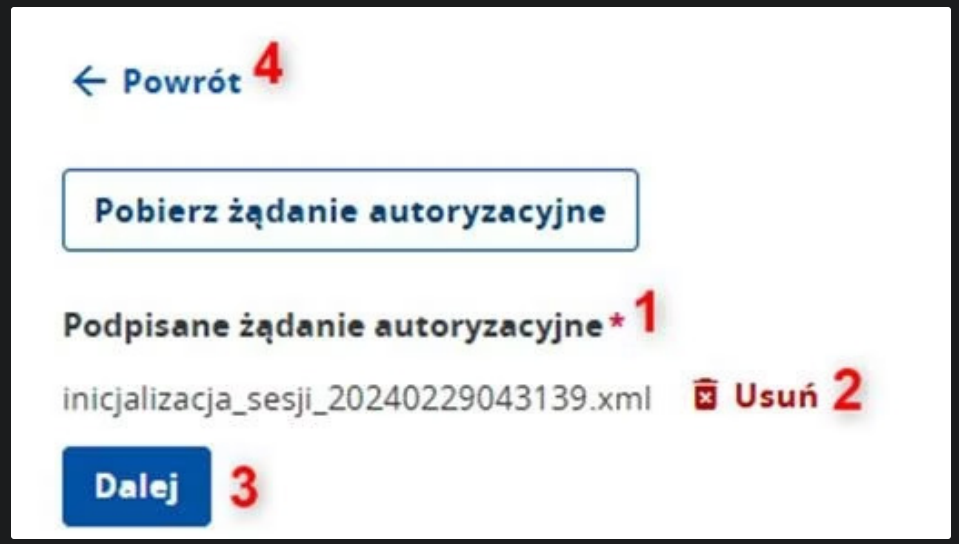
Jeśli plik ma niewłaściwe rozszerzenie lub został nieprawidłowo podpisany, system wyświetli odpowiedni komunikat błędu i poprosi o ponowne wykonanie operacji.

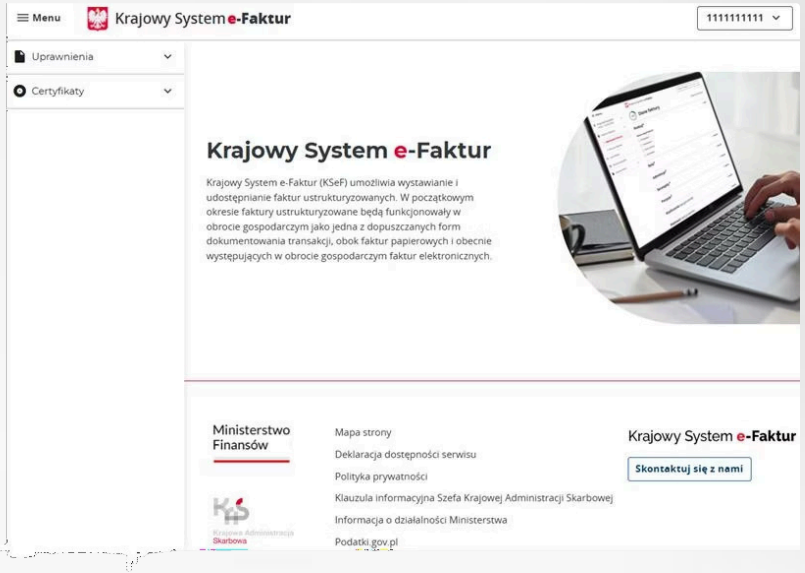
Weryfikacja załączonego pliku

Po poprawnym dodaniu podpisanego pliku żądania autoryzacyjnego system wyświetla ekran potwierdzający, na którym widoczny jest nazwa załączonego dokumentu. To pozwala użytkownikowi upewnić się, że przesłał właściwy plik.

W przypadku gdy użytkownik zauważy, że załączył niewłaściwy plik, system oferuje możliwość jego usunięcia. Wystarczy kliknąć przycisk "Usuń" znajdujący się obok nazwy pliku, a następnie dodać poprawny dokument. Ta funkcjonalność zapobiega błędom i pozwala na szybką korektę.

Aby sfinalizować proces uwierzytelnienia, należy kliknąć przycisk "Dalej". System wtedy przystąpi do weryfikacji podpisanego dokumentu, sprawdzając jego autentyczność i integralność. Jeśli w dowolnym momencie użytkownik zdecyduje się przerwać proces, może kliknąć przycisk "Powrót", który przeniesie go do poprzedniego ekranu.





Pomyślne zakończenie autoryzacji

Gdy proces autoryzacji zakończy się sukcesem, system automatycznie przekierowuje użytkownika na stronę główną MCU. To oznacza, że wszystkie kroki weryfikacji zostały pomyślnie zakończone i użytkownik uzyskał pełny dostęp do funkcjonalności modułu.

Strona główna MCU prezentuje wszystkie dostępne opcje i funkcje, do których użytkownik ma uprawnienia w ramach wybranego kontekstu logowania. Stąd można przejść do zarządzania uprawnieniami, składania wniosków o certyfikaty lub przeglądania już nadanych uprawnień.

System zapamiętuje sesję użytkownika, dzięki czemu nie ma potrzeby ponownego logowania przy każdej operacji. Sesja pozostaje aktywna przez określony czas, po którym - ze względów bezpieczeństwa - następuje automatyczne wylogowanie.

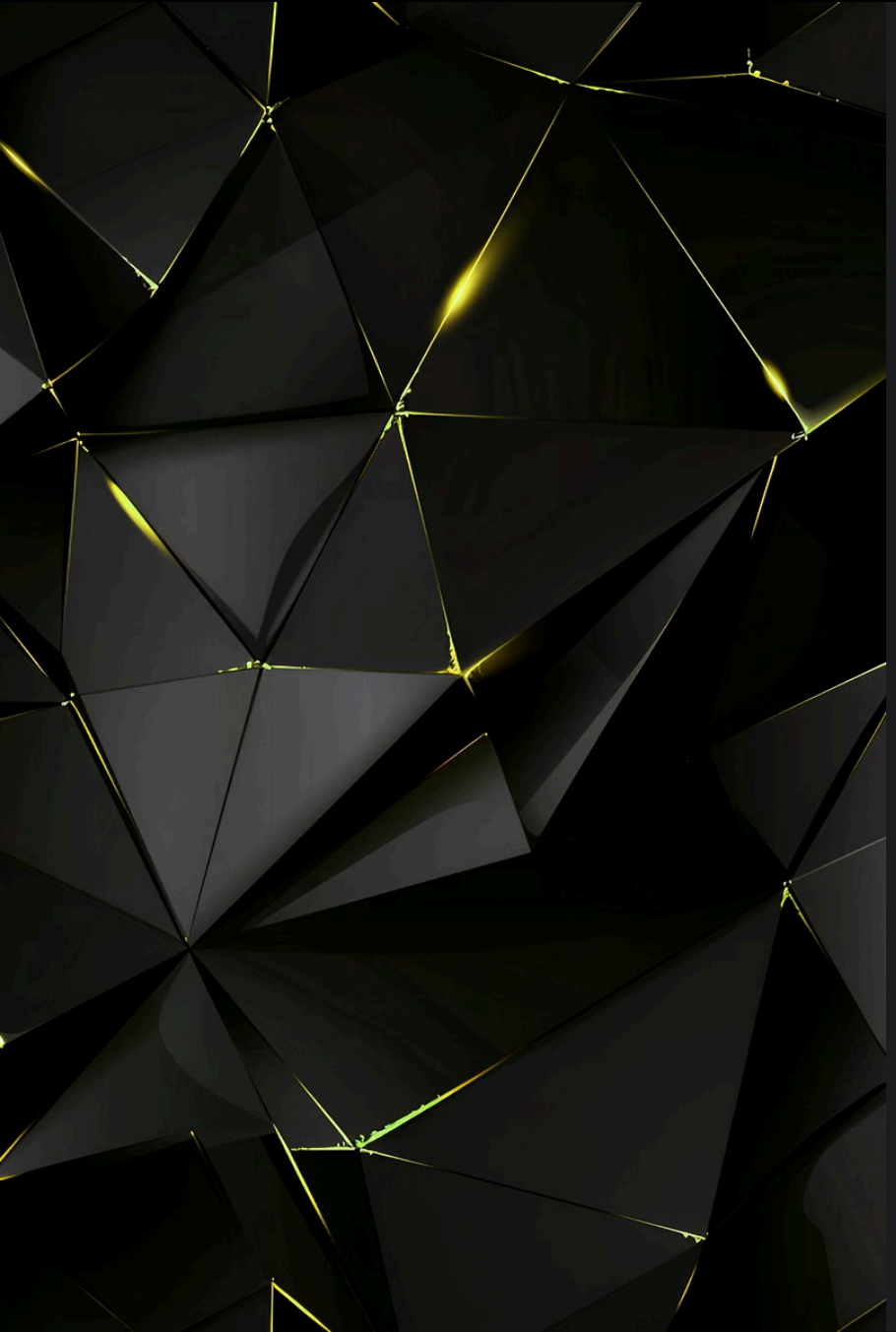
Obsługa błędów autoryzacji

W przypadku gdy proces autoryzacji nie przebiegnie pomyślnie, system wyświetla szczegółowe powiadomienie o błędzie. Komunikaty błędów są zaprojektowane tak, aby jasno wskazywać przyczynę problemu i sugerować sposób jego rozwiązania.

Najczęstsze przyczyny błędów to: nieprawidłowo podpisany plik, użycie niewłaściwego certyfikatu, błędne dane identyfikacyjne lub problemy techniczne z połączeniem. Każdy z tych przypadków jest obsługiwany przez dedykowany komunikat.

Gdy pojawi się komunikat o błędzie, zalecamy uważne przeczytanie jego treści i postępowanie zgodnie z instrukcjami. Często wystarczy powtórzyć proces od początku, upewniając się, że wszystkie kroki są wykonane prawidłowo. W przypadku uporczywych problemów warto skontaktować się z pomocą techniczną.





btla

Autoryzacja przez odcisk palca certyfikatu

Trzecia i ostatnia dostępna ścieżka autoryzacji w MCU to metoda wykorzystująca tzw. odcisk palca certyfikatu kwalifikowanego. Jest to specjalne rozwiązanie przeznaczone dla szczególnych przypadków.

Z tego rozwiązania należy skorzystać w sytuacji, gdy użytkownik posiada certyfikat kwalifikowany, który nie zawiera identyfikatora NIP ani PESEL. W takim przypadku niemożliwe jest bezpośrednie użycie certyfikatu do autoryzacji - najpierw trzeba wygenerować jego unikalny identyfikator, czyli właśnie "odcisk palca".

Odcisk palca certyfikatu to unikalna sekwencja znaków, która jednoznacznie identyfikuje dany certyfikat. Po jego wygenerowaniu można go użyć do nadania uprawnień, a następnie do logowania się w systemie. Proces ten wymaga kilku dodatkowych kroków, ale zapewnia możliwość korzystania z systemu nawet w przypadku certyfikatów bez standardowych identyfikatorów.



Generowanie odcisku palca - proces

Aby uzyskać odcisk palca certyfikatu kwalifikowanego, należy najpierw pobrać specjalny plik do podpisu. Proces ten jest podobny do standardowej autoryzacji certyfikatem, ale służy innemu celowi - wygenerowaniu unikalnego identyfikatora certyfikatu.

Po pobraniu pliku należy go odszukać na dysku komputera i podpisać za pomocą certyfikatu kwalifikowanego, dla którego chcemy wygenerować odcisk palca. Podpisywanie odbywa się przy użyciu standardowego oprogramowania do obsługi certyfikatów.

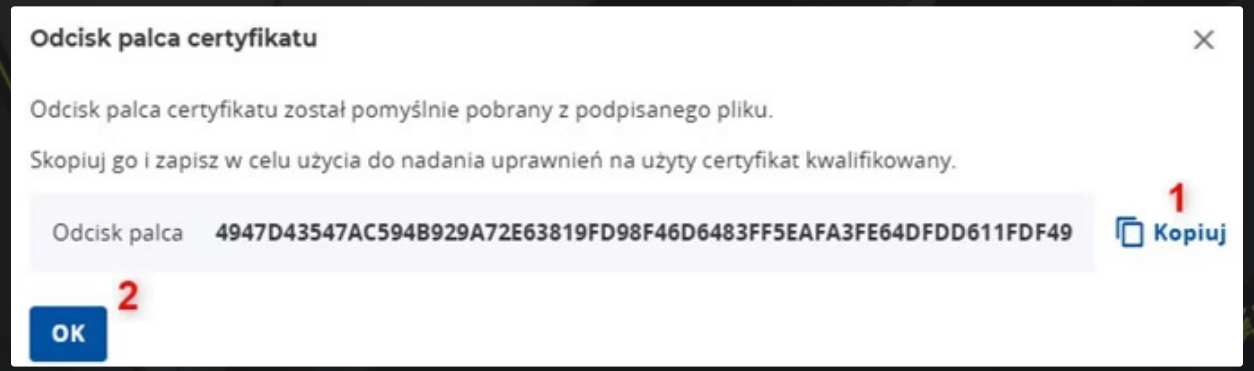
Następnie podpisany plik należy przekazać z powrotem do aplikacji, używając przycisku "Przekaż plik". System przeanalizuje podpisany dokument i na jego podstawie wygeneruje unikalny odcisk palca certyfikatu, który będzie można następnie wykorzystać do nadawania uprawnień.

Pobieranie odcisku palca certyfikatu

Po poprawnym załączeniu podpisanego pliku system aktywuje przycisk "Pobierz odcisk palca". To sygnał, że wszystkie niezbędne dane zostały przetworzone i system jest gotowy do wygenerowania unikalnego identyfikatora certyfikatu.

Po kliknięciu przycisku "Pobierz odcisk palca" na ekranie pojawia się okno modalne zawierające wygenerowany odcisk palca. Jest to długi ciąg znaków składający się z 64 znaków z przedziału od 0 do 9 oraz od A do F. Ten ciąg jest unikalnym identyfikatorem certyfikatu.

Bardzo ważne jest, aby skopiować ten odcisk palca i bezpiecznie go zapisać. Można to zrobić za pomocą przycisku "Kopiuj", który automatycznie kopiuje cały ciąg do schowka systemowego. Odcisk palca będzie potrzebny przy nadawaniu uprawnień na ten certyfikat. Po skopiowaniu i zapisaniu odcisku palca należy kliknąć przycisk "OK", aby zakończyć proces.





btla

Wylogowanie z MCU - opcje

System MCU oferuje dwa sposoby zakończenia pracy i wylogowania się z aplikacji. Każdy z nich został zaprojektowany z myślą o bezpieczeństwie danych użytkownika oraz wygodzie korzystania z systemu.

Samodzielne wylogowanie

Użytkownik może w każdej chwili samodzielnie zakończyć sesję, klikając odpowiedni przycisk w interfejsie. Ta opcja daje pełną kontrolę nad momentem zakończenia pracy w systemie i jest zalecana po zakończeniu wszystkich operacji.

Automatyczne wylogowanie

System automatycznie wylogowuje użytkownika po określonym czasie bezczynności. To zabezpieczenie chroni przed nieautoryzowanym dostępem w sytuacji, gdy użytkownik zapomni się wylogować lub odejdzie od komputera.

Proces samodzielnego wylogowania

Aby samodzielnie wylogować się z aplikacji MCU, należy kliknąć przycisk z identyfikatorem kontekstu użytkownika, który znajduje się w prawym górnym rogu ekranu. Po kliknięciu rozwija się menu z różnymi opcjami, w tym opcją "Wyloguj".

Po wybraniu opcji "Wyloguj" system wyświetla okno modalne z prośbą o potwierdzenie zamiaru wylogowania. To dodatkowe zabezpieczenie zapobiega przypadkowemu wylogowaniu się z systemu. W oknie modalnym dostępne są dwie opcje.

Kliknięcie przycisku "Wyloguj" potwierdza zamiar zakończenia sesji i powoduje natychmiastowe wylogowanie użytkownika z systemu. Wszystkie niezapisane zmiany mogą zostać utracone, dlatego przed wylogowaniem warto upewnić się, że wszystkie operacje zostały zakończone.

Jeśli użytkownik zmieni zdanie, może kliknąć przycisk "Pozostań" lub ikonę "X" w prawym górnym rogu okna modalnego. To przerywa proces wylogowania i pozwala na kontynuowanie pracy w aplikacji.



Automatyczne wylogowanie - ostrzeżenie

Gdy użytkownik przez określony systemowo czas nie wykonuje żadnych działań w aplikacji, system wyświetla komunikat ostrzegawczy informujący o zbliżającym się wygaśnięciu sesji. To zabezpieczenie ma na celu ochronę danych w przypadku, gdy użytkownik odszedł od komputera.

Komunikat zawiera informację o czasie pozostałym do automatycznego wylogowania. Użytkownik ma możliwość przedłużenia sesji i kontynuowania pracy w aplikacji, klikając przycisk "Przedłuż sesję" lub ikonę "X" w oknie komunikatu.

Jeśli użytkownik nie zareaguje na komunikat w określonym czasie, nastąpi automatyczne wylogowanie z aplikacji. System wyświetli wtedy kolejny komunikat informujący o zakończeniu sesji. Wszystkie niezapisane dane mogą zostać utracone, dlatego ważne jest regularne zapisywanie postępów pracy.

Po automatycznym wylogowaniu, aby ponownie uzyskać dostęp do systemu, należy przejść przez cały proces logowania od początku, wybierając odpowiednią metodę uwierzytelnienia.



Potwierdzenie automatycznego wylogowania

Po upływie czasu określonego w komunikacie ostrzegawczym, jeśli użytkownik nie przedłużył sesji, następuje automatyczne wylogowanie z aplikacji. System wyświetla wtedy końcowy komunikat informujący o tym fakcie.

Komunikat o wylogowaniu potwierdza, że sesja została zakończona ze względów bezpieczeństwa. To standardowa procedura w systemach obsługujących wrażliwe dane, która chroni przed nieautoryzowanym dostępem.

Po wyświetleniu tego komunikatu użytkownik zostaje przekierowany do ekranu logowania. Aby ponownie rozpocząć pracę w systemie MCU, należy przejść przez cały proces uwierzytelnienia, wybierając jedną z dostępnych metod autoryzacji: Profil Zaufany, certyfikat kwalifikowany z NIP/PESEL lub certyfikat bez tych identyfikatorów.



Kiedy konieczne jest nadanie uprawnień

Konieczność ponownego nadania uprawnień w module MCU wystąpi w dwóch konkretnych sytuacjach, które są ściśle związane z przejściem na nowy system KSeF 2.0. Zrozumienie tych przypadków jest kluczowe dla prawidłowego przygotowania się do pracy w nowym systemie.

Pierwsza sytuacja dotyczy osób fizycznych, które nie zostały uprawnione na podstawie formularza ZAW-FA w systemie KSeF 1.0 do 31 października 2025 roku. Jeśli ktoś nie zdążył uzyskać uprawnień w starym systemie przed tą datą, będzie musiał przejść przez proces nadawania uprawnień w module MCU.

Druga sytuacja odnosi się do podmiotów, które otrzymały uprawnienia do KSeF do 31 października 2025 roku, ale muszą je odnowić lub zaktualizować w nowym systemie. Po ponownym nadaniu uprawnień w module MCU, zarówno osoby fizyczne jak i podmioty będą mogły wystąpić o certyfikat KSeF i w pełni korzystać z systemu elektronicznych faktur.

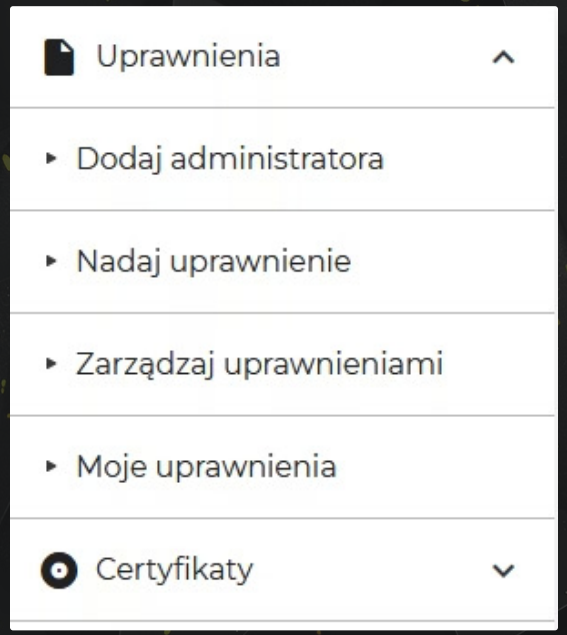
Dodatkowo, nadawanie uprawnień w MCU będzie konieczne dla wszystkich nowych użytkowników, którzy będą chcieli rozpocząć pracę w KSeF od 1 lutego 2026 roku i wcześniej nie posiadali nadanych uprawnień w systemie.

Rozpoczęcie nadawania uprawnień

Aby rozpocząć proces nadawania uprawnień w module MCU, należy z menu głównego aplikacji wybrać pozycję "Uprawnienia". Po jej wybraniu rozwija się lista podzakładek, z których każda odpowiada za inną funkcjonalność związaną z zarządzaniem uprawnieniami.

Menu zawiera kilka opcji, w tym "Dodaj administratora", która zostanie szczegółowo omówiona w module poświęconym jednostkom samorządu terytorialnego (JST). W niniejszym przewodniku skupimy się na trzech głównych funkcjach, które są najczęściej wykorzystywane przez przedsiębiorców.

Te trzy kluczowe funkcje to: "Nadaj uprawnienia" - służąca do przyznawania nowych uprawnień użytkownikom, "Zarządzaj uprawnieniami" - umożliwiająca przeglądanie i odbieranie już nadanych uprawnień, oraz "Moje uprawnienia" - pozwalająca na sprawdzenie uprawnień przypisanych do aktualnie zalogowanego użytkownika.



Opis podzakładek uprawnień

Nadaj uprawnienie

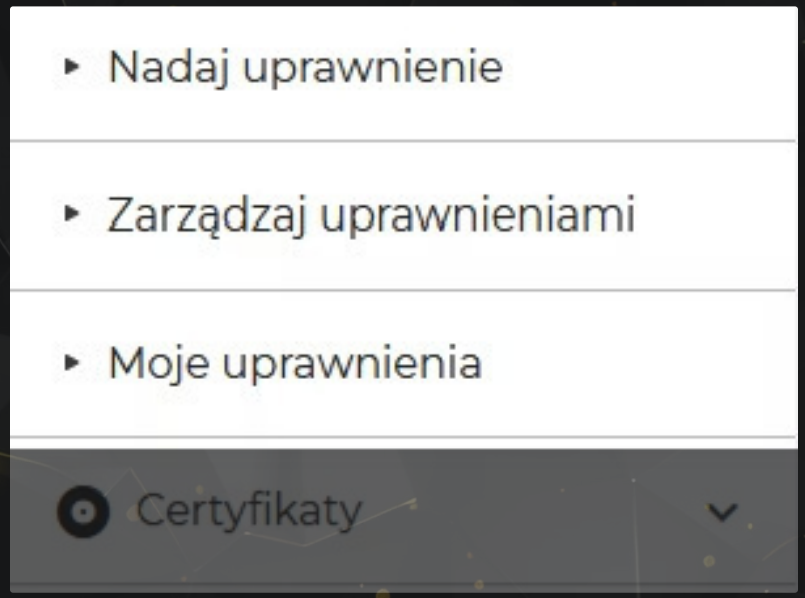
Ta podzakładka prowadzi do ekranu, na którym użytkownik ma możliwość nadawania uprawnień przyszłym użytkownikom aplikacji. To tutaj rozpoczyna się proces przyznawania dostępu do systemu KSeF dla pracowników, współpracowników lub innych osób, które będą działać w imieniu firmy.

Zarządzaj uprawnieniami

Podzakładka prowadzi do ekranu, na którym użytkownik może przeglądać wszystkie nadane uprawnienia oraz je odbierać w razie potrzeby. To narzędzie kontroli i zarządzania dostępem do systemu, które pozwala na bieżąco monitorować, kto ma dostęp do jakich funkcji.

Moje uprawnienia

Ta opcja prowadzi do ekranu prezentującego uprawnienia otrzymane przez aktualnie zalogowanego użytkownika w kontekście logowania. Pozwala to na szybkie sprawdzenie, do jakich funkcji system daje dostęp i w jakim zakresie można działać.



Ekran nadawania uprawnień

Po wybraniu podzakładki "Nadawanie uprawnień" system uruchamia dedykowany ekran z formularzem. Ekran ten został zaprojektowany w sposób intuicyjny, aby maksymalnie ułatwić proces nadawania uprawnień różnym użytkownikom.

Na ekranie znajdują się dwa kluczowe elementy. Pierwszy z nich to pole "Uprawniający", które zostało automatycznie wypełnione danymi użytymi do zalogowania w MCU. Oznacza to, że system wie, kto nadaje uprawnienia i w jakim kontekście to robi. Te dane nie wymagają edycji i służą jedynie informacyjnie.

Drugi element to pole "Rodzaj uprawnień", które użytkownik musi wypełnić samodzielnie, wybierając odpowiednią opcję z rozwijanej listy. Podanie rodzaju uprawnienia jest obowiązkowe - bez tego nie można przejść dalej w procesie. Lista zawiera wszystkie dostępne typy uprawnień, które można nadać w systemie KSeF.



Rodzaje uprawnień w MCU

System MCU oferuje szeroki wachlarz rodzajów uprawnień, które można nadawać różnym użytkownikom. Każdy rodzaj uprawnienia odpowiada konkretnym potrzebom biznesowym i określa zakres działań, które uprawniona osoba lub podmiot będzie mogła wykonywać w systemie.

Osobie fizycznej do pracy w KSeF

Podstawowe uprawnienie dla pracowników firmy, którzy będą bezpośrednio pracować w systemie KSeF w ramach danego podmiotu.

Osobie fizycznej do pracy dla klienta

Uprawnienie pośrednie selektywne, pozwalające pracować w imieniu konkretnego klienta wskazanego przez NIP.

Osobie fizycznej do pracy dla wszystkich klientów

Uprawnienie pośrednie generalne, dające możliwość pracy w imieniu wszystkich klientów danego podmiotu.

Podmiotowi do wystawiania faktur w trybie samofakturowania

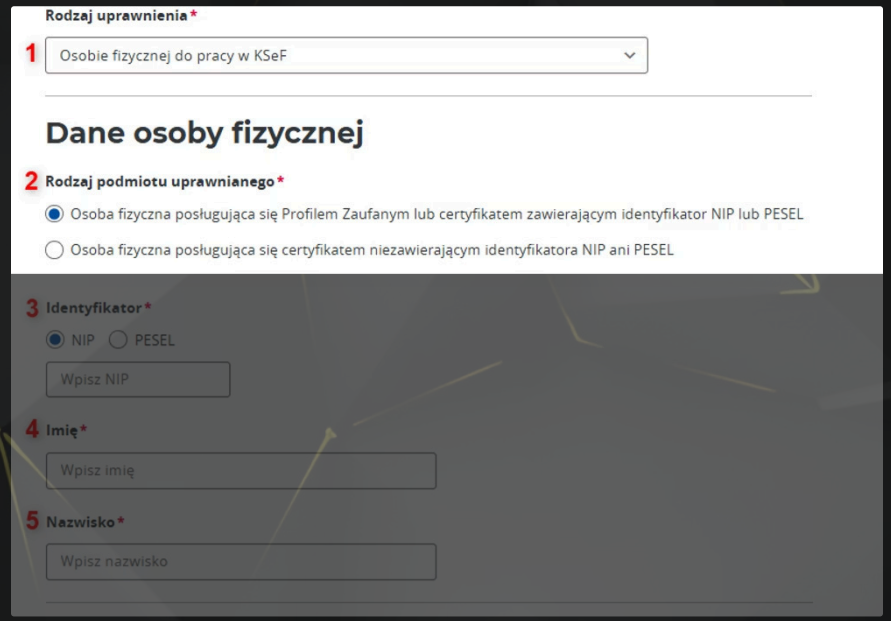
Specjalne uprawnienie dla podmiotów, które będą wystawiać faktury w imieniu sprzedawcy.

Nadawanie uprawnień osobie fizycznej - profil zaufany

Pierwsza ścieżka nadawania uprawnień dotyczy osoby fizycznej do pracy w KSeF, która będzie posługiwać się Profilem Zaufanym lub certyfikatem zawierającym identyfikator NIP lub PESEL. To najczęściej wybierana opcja przez przedsiębiorców.

Po wybraniu rodzaju uprawnienia "Osobie fizycznej do pracy w KSeF" pojawia się dodatkowe pole umożliwiające określenie rodzaju podmiotu uprawnionego. System oferuje dwie opcje do wyboru: osobę fizyczną posługującą się Profilem Zaufanym lub certyfikatem zawierającym identyfikator NIP lub PESEL, oraz osobę fizyczną posługującą się certyfikatem niezawierającym identyfikatora NIP ani PESEL.

Wybór pierwszej opcji prowadzi do formularza, w którym należy podać podstawowe dane osoby, której nadajemy uprawnienia. System wymaga wskazania rodzaju identyfikatora (NIP lub PESEL), a następnie wprowadzenia imienia i nazwiska osoby uprawnionej. Te dane są kluczowe dla prawidłowej identyfikacji użytkownika w systemie.



Zakres uprawnień dla osoby fizycznej

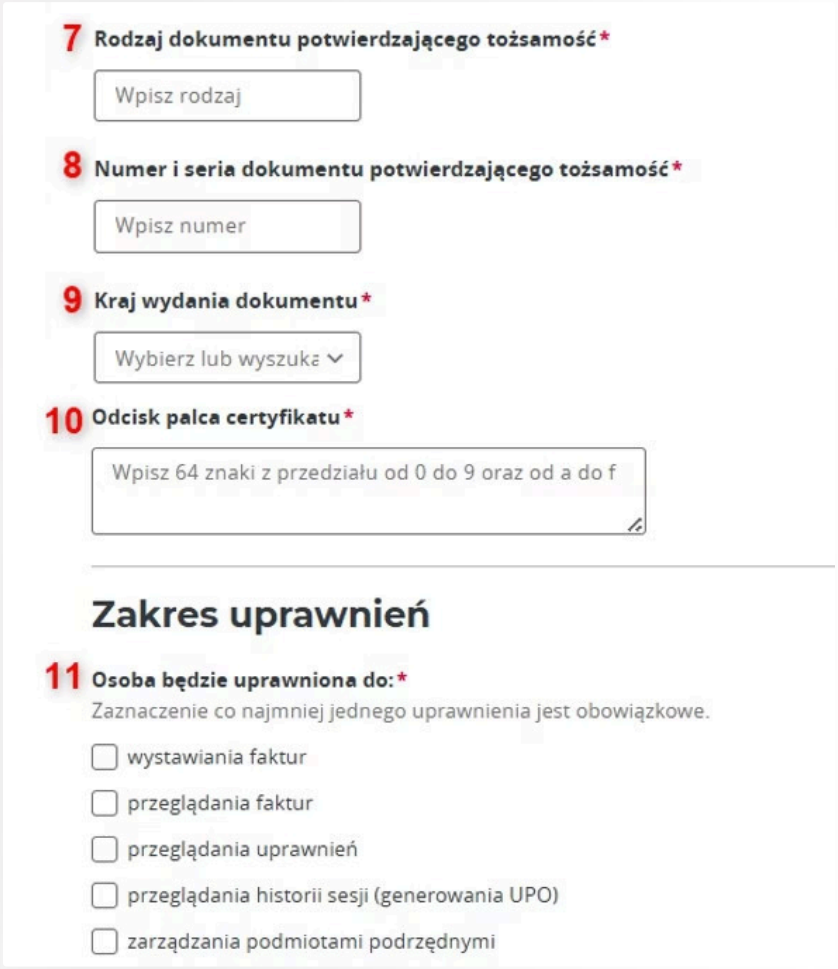
Po wprowadzeniu danych identyfikacyjnych osoby uprawnionej, system wymaga określenia zakresu uprawnień, które mają zostać nadane. To kluczowy moment, w którym decydujemy, do jakich funkcji system KSeF będzie miała dostęp dana osoba.

System oferuje szeroki wybór uprawnień, które można nadać osobie fizycznej. Lista obejmuje: zarządzanie uprawnieniami, przeglądanie uprawnień, wystawianie faktur, przeglądanie faktur, przeglądanie historii sesji (generowania UPO), zarządzanie jednostkami podrzędnymi oraz wykonywanie operacji egzekucyjnych.

Użytkownik może wybrać jedno lub więcej uprawnień z listy, zaznaczając odpowiednie pola wyboru. Każde uprawnienie daje dostęp do konkretnych funkcjonalności systemu. Na przykład, uprawnienie do wystawiania faktur pozwala na tworzenie i wysyłanie faktur elektronicznych, podczas gdy uprawnienie do przeglądania faktur umożliwia jedynie ich odczyt bez możliwości edycji.

Warto zauważyć, że w przypadku komornika sądowego i organu egzekucyjnego zakres uprawnień zawiera dodatkową pozycję: wykonywanie operacji egzekucyjnych. Ta opcja jest dostępna wyłącznie dla tych specyficznych ról i nie pojawia się dla standardowych użytkowników.





Nadawanie uprawnień - certyfikat bez NIP/PESEL

Druga ścieżka nadawania uprawnień osobie fizycznej do pracy w KSeF dotyczy sytuacji, gdy osoba będzie posługiwać się certyfikatem niezawierającym identyfikatora NIP ani PESEL. Ta opcja jest mniej popularna, ale niezbędna w niektórych specyficznych przypadkach.

Po wyborze tej opcji formularz rozszerza się o dodatkowe pola wymagane do pełnej identyfikacji osoby. System wymaga podania rodzaju identyfikatora (NIP, PESEL lub Brak), imienia i nazwiska osoby fizycznej oraz daty urodzenia osoby, której są nadawane uprawnienia.

Dodatkowo, formularz zawiera pola dotyczące dokumentu tożsamości: nazwę rodzaju dokumentu potwierdzającego tożsamość, numer i serię dokumentu oraz pole zawierające słownik z nazwami krajów. Te informacje są niezbędne do jednoznacznej identyfikacji osoby w systemie.

Kluczowym elementem tego formularza jest pole umożliwiające wprowadzenie odcisku palca certyfikatu. Odcisk palca składa się z 64 znaków z przedziału od 0 do 9 oraz od A do F. To unikalny identyfikator certyfikatu, który został wygenerowany wcześniej w procesie opisanym w poprzednich sekcjach tego przewodnika.

Uprawnienia pośrednie selektywne

Uprawnienia pośrednie selektywne to specjalny rodzaj uprawnień, który pozwala osobie fizycznej pracować w systemie KSeF dla konkretnego klienta. Ta opcja jest szczególnie przydatna dla biur rachunkowych i firm świadczących usługi księgowe dla wielu klientów.

Proces nadawania tego typu uprawnień rozpoczyna się od wyboru rodzaju uprawnienia "Osobie fizycznej do pracy dla klienta". Następnie, podobnie jak w poprzednich przypadkach, należy określić, czy osoba będzie posługiwać się Profilem Zaufanym lub certyfikatem zawierającym NIP lub PESEL, czy też certyfikatem bez tych identyfikatorów.

Po wprowadzeniu danych osobowych uprawnianej osoby (rodzaj identyfikatora, imię, nazwisko), system wymaga podania identyfikatora podatkowego NIP klienta lub identyfikatora wewnętrznego (IDWew), który nadał uprawnienia podmiotowi. To kluczowa różnica w porównaniu do uprawnień bezpośrednich - tutaj precyzyjnie określamy, dla którego klienta osoba będzie mogła pracować.

Zakres uprawnień w tym przypadku jest ograniczony do dwóch opcji: wystawianie faktur oraz przeglądanie faktur. Użytkownik może wybrać jedną lub obie opcje, w zależności od potrzeb. To uprawnienie nie daje dostępu do zarządzania uprawnieniami czy innych zaawansowanych funkcji - koncentruje się wyłącznie na operacjach związanych z fakturami dla wskazanego klienta.



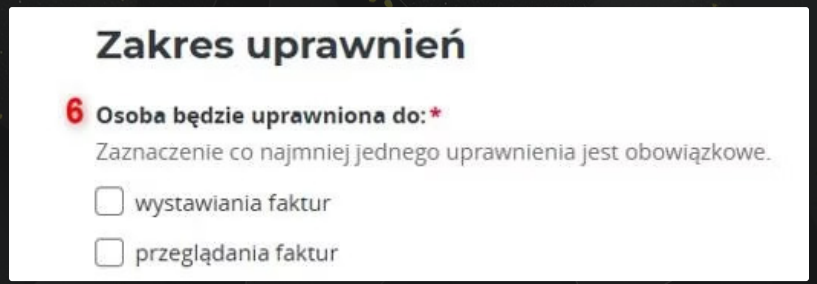
Uprawnienia pośrednie generalne

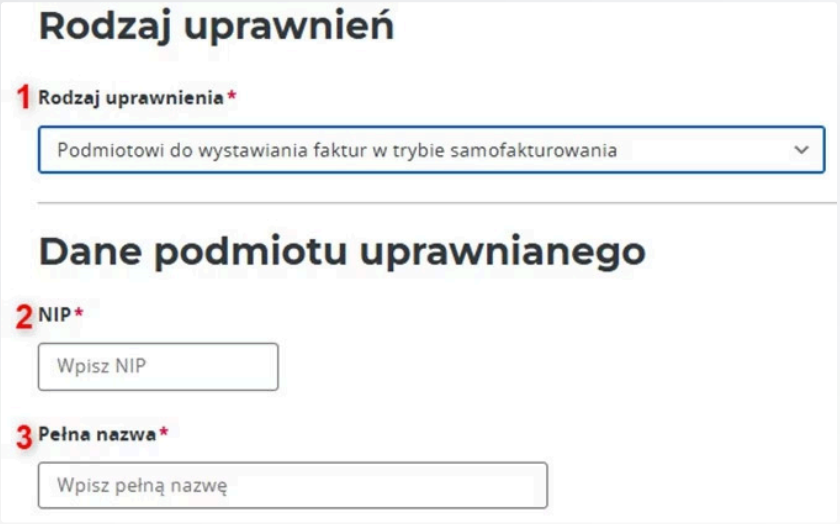
Uprawnienia pośrednie generalne stanowią najbardziej rozbudowaną formę delegowania uprawnień w systemie MCU. W przeciwieństwie do uprawnień selektywnych, które dotyczą konkretnego klienta, uprawnienia generalne pozwalają osobie fizycznej pracować w imieniu wszystkich klientów danego podmiotu.

Proces nadawania tego typu uprawnień rozpoczyna się od wyboru rodzaju uprawnienia "Osobie fizycznej do pracy dla wszystkich klientów". Ta opcja jest szczególnie przydatna dla większych biur rachunkowych, które obsługują wielu klientów i potrzebują elastycznego systemu zarządzania dostępem.

Formularz nadawania uprawnień pośrednich generalnych jest podobny do formularza dla uprawnień selektywnych, z jedną kluczową różnicą - nie wymaga podawania konkretnego NIP klienta. Zamiast tego, po wprowadzeniu danych osobowych uprawnianej osoby (rodzaj identyfikatora, imię, nazwisko), użytkownik przechodzi bezpośrednio do wyboru zakresu uprawnień.

Zakres uprawnień również jest ograniczony do dwóch opcji: wystawianie faktur oraz przeglądanie faktur. Jednak w tym przypadku wybrane uprawnienia będą obowiązywać dla wszystkich klientów podmiotu, co znacznie zwiększa elastyczność i zakres działania uprawnionej osoby. To rozwiązanie wymaga szczególnej ostrożności przy nadawaniu, ponieważ daje bardzo szerokie możliwości działania w systemie.





Uprawnienia podmiotowe - samofakturowanie

Uprawnienia podmiotowe stanowią odrębną kategorię uprawnień w systemie MCU, która dotyczy relacji między podmiotami gospodarczymi, a nie między podmiotem a osobą fizyczną. Pierwszym rodzajem uprawnień podmiotowych jest uprawnienie do wystawiania faktur w trybie samofakturowania.

Samofakturowanie to specjalny tryb, w którym nabywca wystawia fakturę w imieniu sprzedawcy. Jest to rozwiązanie stosowane w określonych sytuacjach biznesowych, które wymaga uprzedniego uzyskania zgody i nadania odpowiednich uprawnień przez sprzedawcę.

Proces nadawania tego uprawnienia jest stosunkowo prosty. Po wyborze rodzaju uprawnienia "Podmiotowi do wystawiania faktur w trybie samofakturowania" z listy, system wymaga podania dwóch podstawowych informacji: numeru identyfikacji podatkowej (NIP) podmiotu, któremu nadajemy uprawnienie, oraz pełnej nazwy tego podmiotu.

Po wprowadzeniu tych danych i zatwierdzeniu formularza, wskazany podmiot otrzyma możliwość wystawiania faktur w trybie samofakturowania w imieniu podmiotu nadającego uprawnienie. To uprawnienie jest szczególnie istotne w relacjach B2B, gdzie taki tryb współpracy został uzgodniony między stronami.

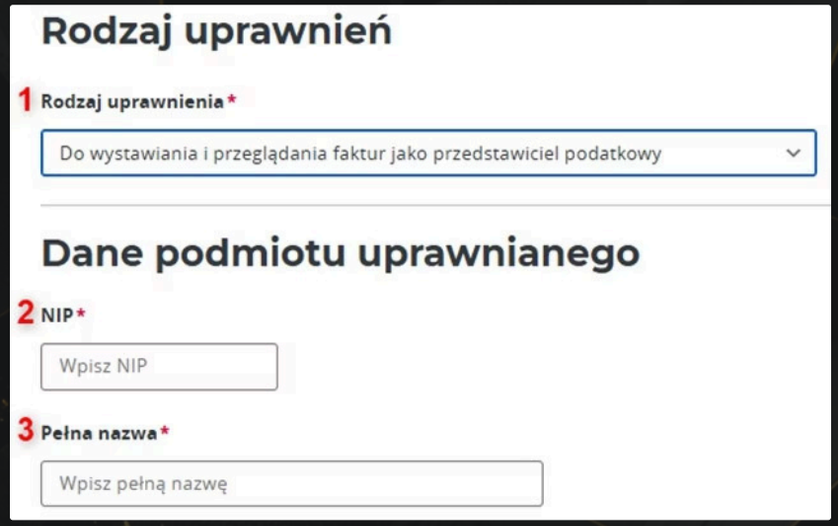
Uprawnienia przedstawiciela podatkowego

Kolejnym rodzajem uprawnień podmiotowych jest uprawnienie do wystawiania i przeglądania faktur jako przedstawiciel podatkowy. Ta funkcja jest szczególnie istotna w kontekście transakcji międzynarodowych i specyficznych sytuacji podatkowych.

Przedstawiciel podatkowy to podmiot, który działa w imieniu podatnika w określonych sytuacjach przewidzianych przepisami prawa podatkowego. Może to dotyć na przykład podmiotów zagranicznych prowadzących działalność w Polsce, które muszą wyznaczyć przedstawiciela podatkowego.

Proces nadawania tego uprawnienia jest analogiczny do procesu dla samofakturowania. Po wyborze rodzaju uprawnienia "Do wystawiania i przeglądania faktur jako przedstawiciel podatkowy" z listy rozwijanej, system wymaga podania numeru identyfikacji podatkowej (NIP) podmiotu oraz jego pełnej nazwy.

Po nadaniu tego uprawnienia wskazany podmiot będzie mógł wystawiać i przeglądać faktury w imieniu podmiotu, który go upoważnił. To uprawnienie jest szersze niż w przypadku samofakturowania, ponieważ obejmuje również możliwość przeglądania faktur, co jest istotne dla pełnienia funkcji przedstawiciela podatkowego.



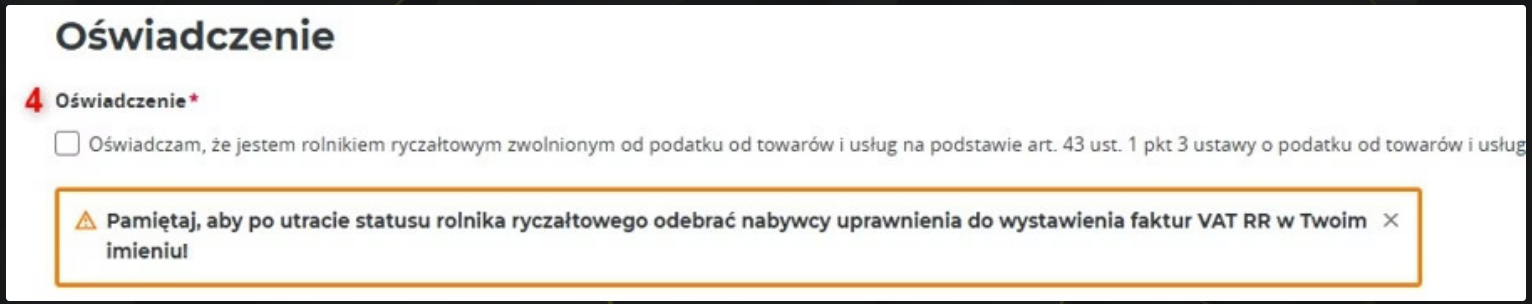
Uprawnienia dla faktur VAT RR

Faktury VAT RR to specjalny rodzaj faktur stosowanych w obrocie z rolnikami ryczałtowymi. System MCU przewiduje dedykowany rodzaj uprawnień dla podmiotów, które będą wystawiać i przeglądać tego typu faktury.

Po wyborze rodzaju uprawnienia "Podmiotowi do wystawiania i przeglądania faktur VAT RR" z listy, system wymaga standardowych informacji: numeru identyfikacji podatkowej (NIP) podmiotu oraz jego pełnej nazwy. Te dane są niezbędne do jednoznacznej identyfikacji podmiotu w systemie.

Istotną cechą tego rodzaju uprawnień jest dodatkowe pole wyboru, które pojawia się w przypadku nadawania uprawnień przez rolnika ryczałtowego. Jeśli podmiot nadający uprawnienia sam jest rolnikiem ryczałtowym, musi zaznaczyć odpowiednie oświadczenie potwierdzające ten fakt. To zabezpieczenie zapewnia, że uprawnienia są nadawane zgodnie z przepisami dotyczącymi obrotu rolniczego.

Po nadaniu tego uprawnienia wskazany podmiot będzie mógł wystawiać i przeglądać faktury VAT RR w systemie KSeF, co jest szczególnie istotne dla podmiotów zajmujących się skupem produktów rolnych lub świadczących usługi dla rolników ryczałtowych.



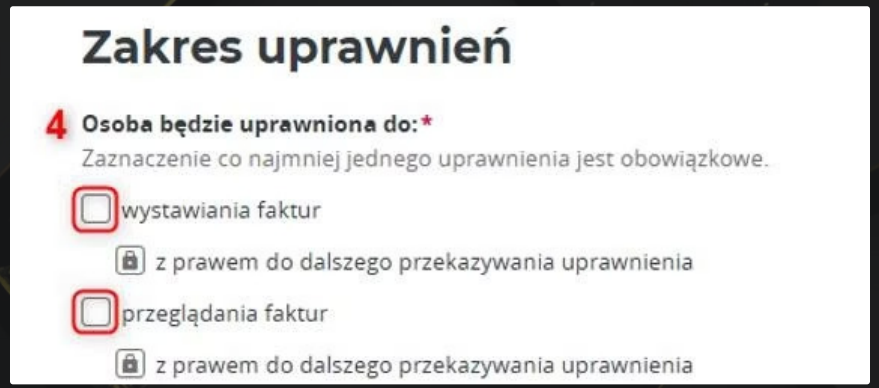
Ogólne uprawnienia podmiotowe

Najbardziej uniwersalnym rodzajem uprawnień podmiotowych jest uprawnienie do wystawiania i przeglądania faktur. To podstawowe uprawnienie, które może być nadawane w różnych konfiguracjach i z różnym zakresem możliwości dalszego przekazywania.

Po wyborze rodzaju uprawnienia "Podmiotowi do wystawiania i przeglądania faktur" z listy, system wymaga podania standardowych danych: numeru identyfikacji podatkowej (NIP) podmiotu oraz jego pełnej nazwy. Te informacje są podstawą dla utworzenia uprawnienia w systemie.

Kluczowym elementem tego formularza jest pole umożliwiające wybór konkretnych uprawnień, które mają zostać nadane. System oferuje dwie opcje: wystawianie faktur oraz przeglądanie faktur. Użytkownik może wybrać jedną lub obie opcje, w zależności od potrzeb i charakteru współpracy z danym podmiotem.

Bardzo ważną funkcjonalnością jest możliwość oznaczenia, czy nadawane uprawnienie może być przekazywane dalej. Po wyborze uprawnienia pojawia się pole "z prawem do dalszego przekazywania uprawnienia". Zaznaczenie tego pola umożliwi podmiotowi otrzymującemu uprawnienia zastosowanie uprawnień pośrednich selektywnych lub generalnych, czyli dalsze delegowanie dostępu do systemu. Warto zauważyć, że opcja dalszego przekazywania uprawnień nie jest dostępna dla wszystkich ról i kontekstów - system automatycznie kontroluje, kto może korzystać z tej funkcjonalności.



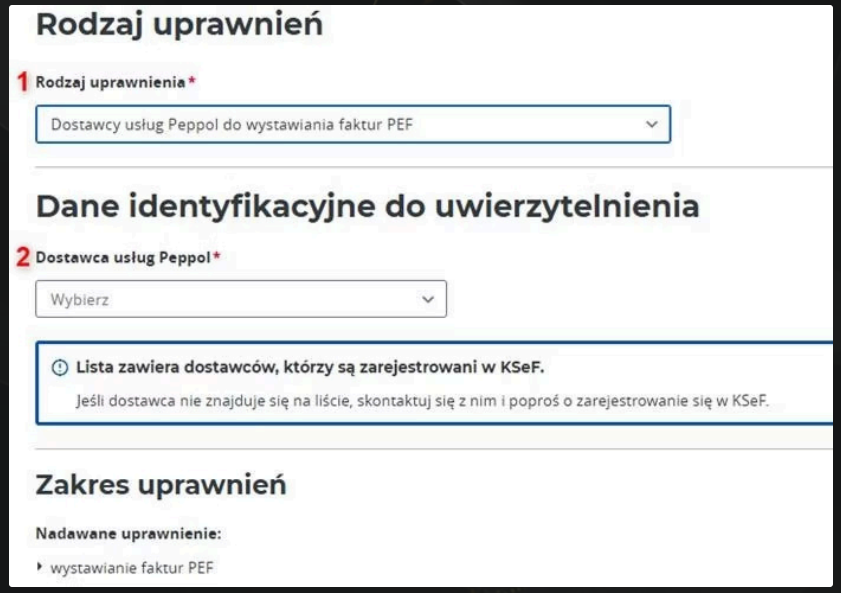
Uprawnienia dla dostawców usług PEPPOL

PEPPOL to międzynarodowa sieć wymiany dokumentów elektronicznych, która umożliwia bezpieczną i standaryzowaną wymianę faktur elektronicznych między podmiotami w różnych krajach. System MCU przewiduje specjalny rodzaj uprawnień dla dostawców usług PEPPOL.

Po wyborze rodzaju uprawnienia "Dostawca usług PEPPOL do wystawiania faktur PEF" z listy rozwijanej, system prezentuje listę zawierającą dostawców usług PEPPOL, którzy są zarejestrowani w systemie KSeF. Użytkownik wybiera z tej listy konkretnego dostawcę, któremu chce nadać uprawnienia.

W przypadku tego rodzaju uprawnień zakres jest ściśle określony i nie wymaga dodatkowego wyboru. System automatycznie nadaje wszystkie niezbędne uprawnienia związane z wystawianiem faktur w formacie PEF (PEPPOL E-Faktura) przez wybranego dostawcę usług.

To uprawnienie jest szczególnie istotne dla przedsiębiorców, którzy prowadzą działalność międzynarodową lub współpracują z kontrahentami zagranicznymi. Korzystanie z usług dostawcy PEPPOL zapewnia zgodność z międzynarodowymi standardami wymiany faktur elektronicznych i ułatwia komunikację biznesową z partnerami z innych krajów.



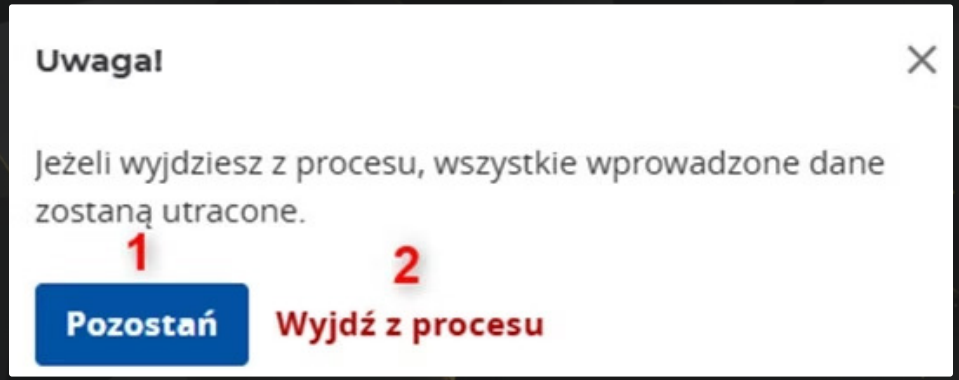
Finalizacja procesu nadawania uprawnień

Wszystkie przedstawione ścieżki nadawania uprawnień kończą się tym samym etapem finalizacji. Po wypełnieniu wszystkich wymaganych pól formularza użytkownik ma do dyspozycji dwa przyciski, które pozwalają na zakończenie lub przerwanie procesu.

Aby sfinalizować proces nadawania uprawnień i faktycznie przyznać wybrane uprawnienia wskazanej osobie lub podmiotowi, należy kliknąć przycisk "Nadaj uprawnienie". System wtedy przetworzy wprowadzone dane, zweryfikuje ich poprawność i utworzy nowe uprawnienie w bazie danych.

Jeśli w trakcie wypełniania formularza użytkownik zmieni zdanie lub zauważy błąd, który wymaga rozpoczęcia procesu od nowa, może kliknąć przycisk "Zrezygnuj". Po kliknięciu tego przycisku system wyświetli okno modalne z prośbą o potwierdzenie zamiaru rezygnacji z nadawania uprawnień.

W oknie modalnym dostępne są dwie opcje. Przycisk "Pozostań" pozwala na kontynuowanie pracy z formularzem - jest to przydatne, gdy użytkownik przypadkowo kliknął "Zrezygnuj". Natomiast przycisk "Wyjdź z procesu" definitywnie przerywa proces nadawania uprawnień i wszystkie wprowadzone dane zostaną utracone. Po wybraniu tej opcji użytkownik zostanie przeniesiony do ekranu głównego uprawnień.



Potwierdzenie nadania uprawnień

Po kliknięciu przycisku "Nadaj uprawnienie" i pomyślnym zakończeniu procesu, system wyświetla komunikat potwierdzający, że uprawnienia zostały prawidłowo nadane. Ten ekran informuje użytkownika o sukcesie operacji i oferuje dwie możliwości dalszego działania.

Z poziomu ekranu potwierdzenia użytkownik może przejść bezpośrednio do listy uprawnień, klikając przycisk "Zarządzaj uprawnieniami". Ta opcja jest przydatna, gdy chcemy od razu sprawdzić, jak nadane uprawnienie wygląda na liście wszystkich uprawnień lub gdy planujemy zarządzać już istniejącymi uprawnieniami.

Druga opcja to przycisk "Dodaj kolejne uprawnienia", który pozwala na natychmiastowe rozpoczęcie procesu nadawania uprawnień kolejnemu podmiotowi lub osobie. System przenosi użytkownika z powrotem do pustego formularza nadawania uprawnień, zachowując kontekst logowania. To rozwiązanie znacznie przyspiesza pracę, gdy musimy nadać uprawnienia wielu użytkownikom jednocześnie.

Komunikat potwierdzający zawiera również szczegółowe informacje o nadanym uprawnieniu, takie jak identyfikator uprawnionej osoby lub podmiotu, rodzaj nadanego uprawnienia oraz zakres uprawnień. Te informacje można zapisać lub wydrukować na potrzeby dokumentacji wewnętrznej firmy.



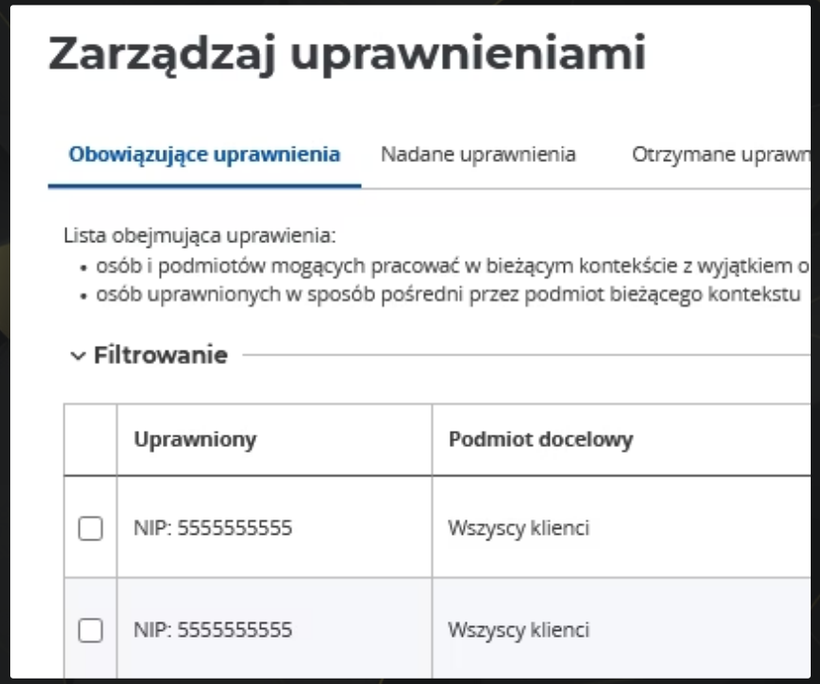
Zarządzaj uprawnieniami - przegląd

Wybór podzakładki "Zarządzaj uprawnieniami" uruchamia rozbudowany ekran z systemem zakładek, który pozwala na kompleksowe zarządzanie wszystkimi aspektami uprawnień w systemie MCU. To centrum kontroli dostępu do systemu KSeF.

Na ekranie widoczne są różne zakładki, z których każda prezentuje inny aspekt uprawnień. Po wyborze danej zakładki uruchamiana jest tabela przedstawiająca zestawienie odpowiednich danych. System prezentuje uprawnienia nadane przez aktualny kontekst zalogowanego użytkownika, uprawnienia przypisane do użytkownika oraz wiele innych kategorii.

Dostępne tabele to: Obowiązujące uprawnienia, Nadane uprawnienia, Otrzymane uprawnienia podmiotowe, Nadane uprawnienia podmiotowe, Uprawnienia w jednostkach podrzędnych, Uprawnienia podmiotów unijnych, Role podmiotu oraz Podmioty podrzędne. Każda z tych zakładek służy innemu celowi i prezentuje dane w sposób dostosowany do specyfiki danego rodzaju uprawnień.

Interfejs został zaprojektowany w sposób intuicyjny, z możliwością filtrowania i sortowania danych według różnych kryteriów. To pozwala na szybkie odnalezienie interesujących nas informacji nawet w przypadku dużej liczby nadanych uprawnień.



Funkcje filtrowania i odbierania uprawnień

Każda tabela w sekcji "Zarządzaj uprawnieniami" posiada zaawansowane możliwości filtrowania danych po określonych parametrach. To niezwykle przydatna funkcja, szczególnie gdy mamy do czynienia z dużą liczbą uprawnień i chcemy szybko znaleźć konkretne informacje.

Użytkownicy posiadający odpowiednie uprawnienia zobaczą pod tabelami przedstawiającymi listę uprawnień dodatkowy przycisk "Odbierz uprawnienia". Ten przycisk służy do odbierania zaznaczonych uprawnień i jest kluczowym narzędziem w zarządzaniu dostępem do systemu.

Przycisk "Odbierz uprawnienia" aktywuje się dopiero w momencie zaznaczenia wybranego uprawnienia za pomocą pola wyboru znajdującego się przy każdym wpisie w tabeli. Można zaznaczyć jedno lub więcej uprawnień jednocześnie, co pozwala na masowe operacje.

Po kliknięciu przycisku "Odbierz uprawnienia" system wyświetla komunikat z prośbą o potwierdzenie wykonywanej czynności. To zabezpieczenie zapobiega przypadkowemu odebraniu uprawnień. W oknie modalnym dostępne są dwa przyciski: jeden zatwierdza odebranie uprawnień, drugi pozwala zrezygnować z procesu i wrócić do tabeli bez wprowadzania zmian.

W przypadku potwierdzenia i poprawnie zakończonego procesu, odebrane uprawnienie znika z listy aktywnych uprawnień i zostaje wyświetlony komunikat sukcesu. System automatycznie aktualizuje widok tabeli, pokazując aktualny stan uprawnień.



Szybki dostęp do funkcji

Na ekranie "Zarządzaj uprawnieniami" dostępne są także przyciski umożliwiające szybki dostęp do najważniejszych funkcji systemu. Te skróty znacznie przyspieszają pracę i eliminują konieczność nawigowania przez menu.

Pierwszy z przycisków to "Nadaj uprawnienia", który prowadzi bezpośrednio do formularza nadawania uprawnień. Dzięki temu, nawet będąc w widoku zarządzania uprawnieniami, możemy szybko przejść do nadawania nowych uprawnień bez konieczności wracania do menu głównego.

Drugi przycisk to "Dodaj administratora", który prowadzi do specjalnego formularza dodawania administratorów. Ta funkcjonalność zostanie szczegółowo omówiona w module poświęconym jednostkom samorządu terytorialnego (JST), ponieważ jest szczególnie istotna w kontekście zarządzania strukturami hierarchicznymi.

Te przyciski są zawsze widoczne na ekranie zarządzania uprawnieniami, niezależnie od tego, którą zakładkę aktualnie przeglądamy. To zapewnia spójność interfejsu i ułatwia nawigację po systemie.

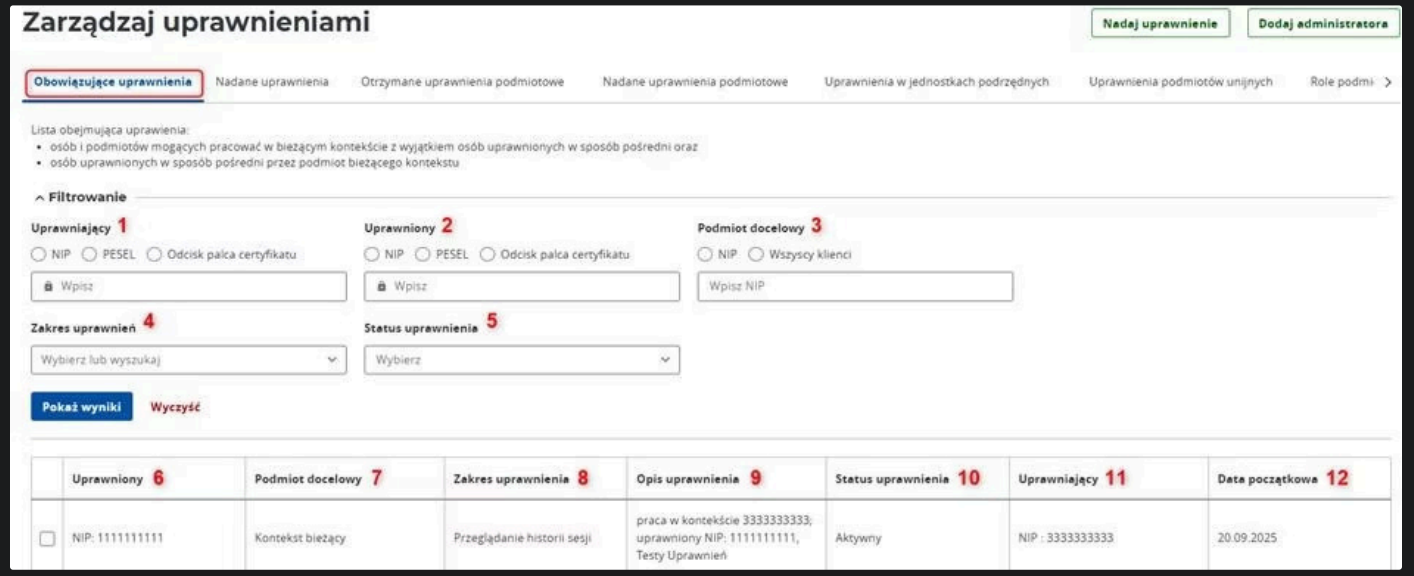


Zakładka Obowiązujące uprawnienia

Tabela "Obowiązujące uprawnienia" prezentuje kompleksową listę wszystkich aktywnych uprawnień w bieżącym kontekście. To jedno z najważniejszych narzędzi do monitorowania, kto ma dostęp do systemu i w jakim zakresie. Lista obejmuje uprawnienia osób i podmiotów mogących pracować w bieżącym kontekście, z wyjątkiem osób uprawnionych w sposób pośredni. Dodatkowo prezentowane są osoby uprawnione w sposób pośredni przez podmiot bieżącego kontekstu. To rozróżnienie jest istotne dla zrozumienia struktury uprawnień w organizacji.

Tabela zawiera szereg kolumn z różnymi informacjami: identyfikator uprawnionego, rodzaj podmiotu docelowego (kontekst bieżący lub klient), nazwę rodzaju nadanego uprawnienia, opis nadanego uprawnienia, status uprawnienia (aktywny lub nieaktywny), identyfikator uprawniającego oraz datę początku obowiązywania uprawnienia.

System oferuje zaawansowane możliwości filtrowania danych. Można filtrować listę po identyfikatorze uprawnionego (NIP, PESEL, odcisk palca certyfikatu), po podmiocie docelowym (NIP lub wszyscy klienci), po zakresie uprawnień (zarządzanie uprawnieniami, przeglądanie uprawnień, wystawianie faktur, przeglądanie faktur, przeglądanie historii sesji, zarządzanie jednostkami podrzędnymi, operacje egzekucyjne) oraz po statusie (aktywny lub nieaktywny).



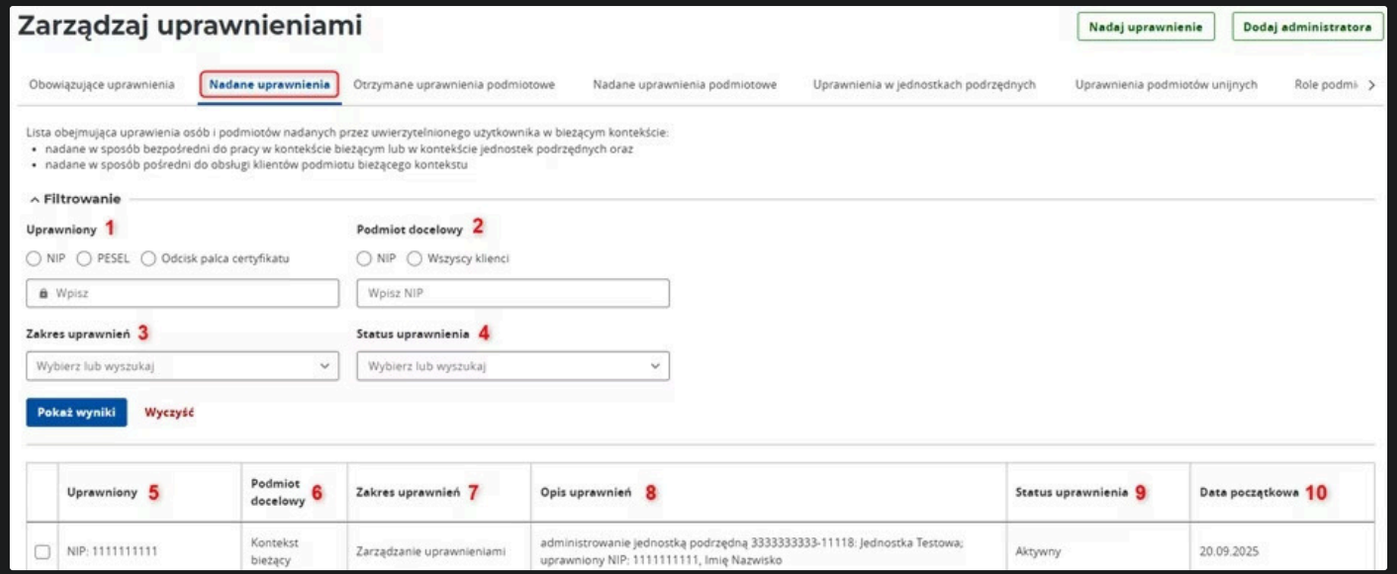
Zakładka Nadane uprawnienia

Tabela "Nadane uprawnienia" prezentuje listę obejmującą uprawnienia osób i podmiotów nadanych przez uwierzytelnionego użytkownika w bieżącym kontekście. To narzędzie pozwala na śledzenie wszystkich uprawnień, które zostały przyznane przez aktualnie zalogowanego użytkownika.

Lista zawiera uprawnienia nadane w sposób bezpośredni do pracy w kontekście bieżącym lub w kontekście jednostek podrzędnych. Dodatkowo prezentowane są uprawnienia nadane w sposób pośredni do obsługi klientów podmiotu bieżącego kontekstu. To rozróżnienie jest kluczowe dla zrozumienia, jakie uprawnienia zostały nadane bezpośrednio, a jakie poprzez mechanizm uprawnień pośrednich.

Tabela oferuje podobne możliwości filtrowania jak zakładka "Obowiązujące uprawnienia". Użytkownik może zawęzić listę do wskazanego identyfikatora (NIP, PESEL, odcisk palca certyfikatu), do wskazanego podmiotu docelowego (NIP lub wszyscy klienci), do wybranego zakresu uprawnień oraz do konkretnego statusu (aktywny lub nieaktywny).

Kolumny tabeli prezentują szczegółowe informacje o każdym nadanym uprawnieniu: identyfikator uprawnionego, rodzaj podmiotu docelowego, nazwę rodzaju nadanego uprawnienia, opis nadanego uprawnienia, status uprawnienia oraz datę początku obowiązywania uprawnienia. Te informacje pozwalają na pełną kontrolę nad nadanymi uprawnieniami i łatwe zarządzanie nimi.



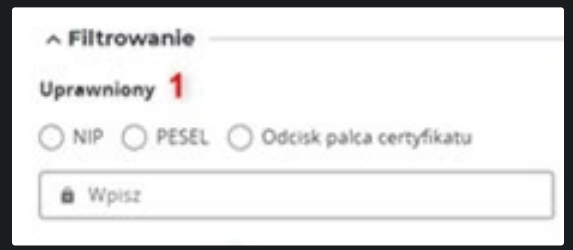
Filtrowanie w zakładce Nadane uprawnienia

Zakładka "Nadane uprawnienia" oferuje rozbudowany system filtrów, który pozwala na precyzyjne wyszukiwanie konkretnych uprawnień w systemie. Każdy filtr został zaprojektowany tak, aby maksymalnie ułatwić odnalezienie potrzebnych informacji.

Pierwszy filtr zawęża listę uprawnień do wskazanego identyfikatora. Użytkownik może wprowadzić jeden z następujących identyfikatorów: NIP, PESEL lub odcisk palca certyfikatu. System automatycznie rozpoznaje typ wprowadzonego identyfikatora i przeprowadza odpowiednie wyszukiwanie.

Drugi filtr pozwala zawęzić listę uprawnień do wskazanego podmiotu docelowego. Użytkownik może wybrać opcję NIP (dla uprawnień pośrednich selektywnych dotyczących konkretnego klienta) lub opcję "Wszyscy klienci" (dla uprawnień pośrednich generalnych). To rozróżnienie jest szczególnie przydatne dla biur rachunkowych obsługujących wielu klientów.

Trzeci filtr zawęża listę uprawnień do wybranego zakresu uprawnień. Użytkownik może zaznaczyć minimum jeden z dostępnych rodzajów uprawnień: zarządzanie uprawnieniami, przeglądanie uprawnień, wystawianie faktur, przeglądanie faktur, przeglądanie historii sesji, zarządzanie jednostkami podrzędnymi oraz operacje egzekucyjne. Możliwość zaznaczenia wielu opcji jednocześnie pozwala na elastyczne wyszukiwanie.



Struktura danych w tabeli Nadane uprawnienia

Tabela "Nadane uprawnienia" prezentuje dane w przejrzystej, uporządkowanej strukturze kolumn. Każda kolumna zawiera specyficzne informacje niezbędne do pełnego zrozumienia charakteru nadanego uprawnienia.

Ostatni dostępny filtr zawęża listę uprawnień do konkretnego statusu. Użytkownik może zaznaczyć jeden z dwóch rodzajów statusów: aktywny lub nieaktywny. Status aktywny oznacza, że uprawnienie jest obecnie obowiązujące i uprawniona osoba lub podmiot może z niego korzystać. Status nieaktywny wskazuje na uprawnienia, które zostały odebrane lub wygasły.

Kolumny tabeli prezentują następujące informacje: identyfikator uprawnionego (NIP, PESEL lub odcisk palca certyfikatu osoby lub podmiotu, któremu nadano uprawnienie), rodzaj podmiotu docelowego (czy uprawnienie dotyczy kontekstu bieżącego czy konkretnego klienta), nazwę rodzaju nadanego uprawnienia (np. "Osobie fizycznej do pracy w KSeF"), opis nadanego uprawnienia (szczegółowy zakres uprawnień), status uprawnienia (aktywny lub nieaktywny) oraz datę początku obowiązywania uprawnienia.

Wszystkie te informacje są prezentowane w sposób czytelny i uporządkowany, co pozwala na szybką ocenę sytuacji i podjęcie odpowiednich decyzji dotyczących zarządzania uprawnieniami. System automatycznie aktualizuje dane w tabeli po każdej zmianie, zapewniając dostęp do najbardziej aktualnych informacji.



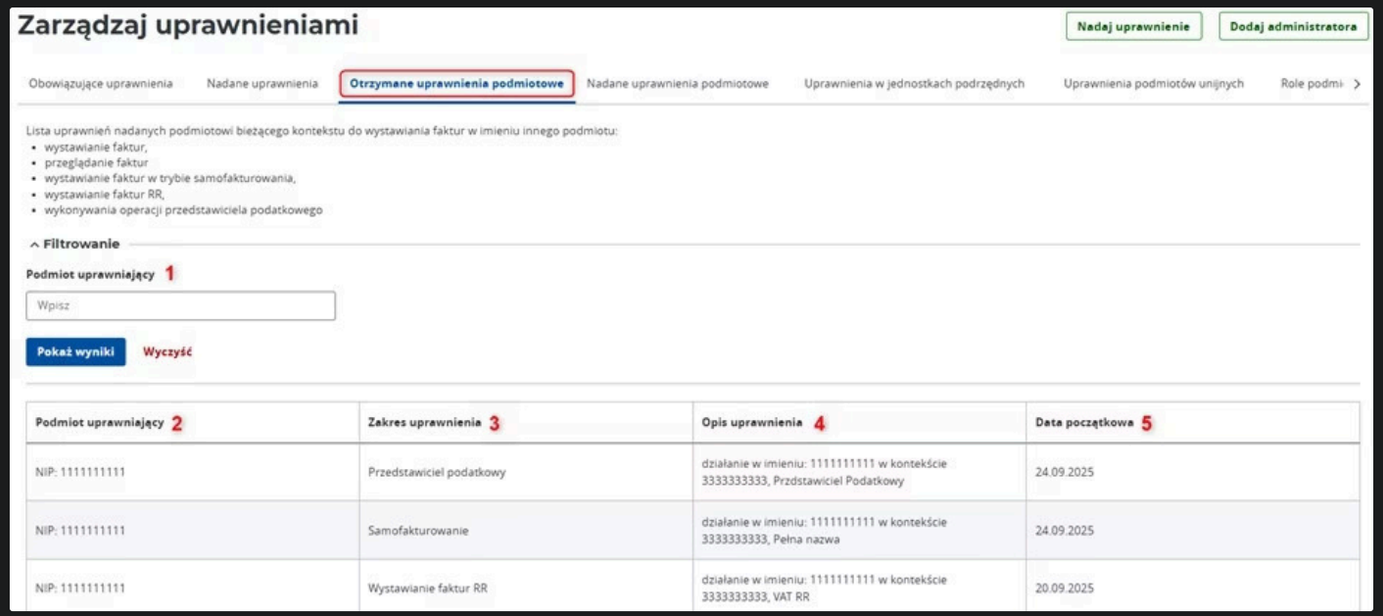
Zakładka Otrzymane uprawnienia podmiotowe

Tabela "Otrzymane uprawnienia podmiotowe" prezentuje listę uprawnień nadanych podmiotowi bieżącego kontekstu do wystawiania faktur w imieniu innego podmiotu. To szczególnie ważna zakładka dla podmiotów, które działają jako pośrednicy lub przedstawiciele innych firm.

Lista obejmuje różne rodzaje uprawnień podmiotowych: wystawianie faktur, przeglądanie faktur, wystawianie faktur w trybie samofakturowania, wystawianie faktur VAT RR oraz wykonywanie operacji przedstawiciela podatkowego. Każdy z tych rodzajów uprawnień daje inne możliwości działania w systemie KSeF.

Tabela zawiera kluczowe informacje o każdym otrzymanym uprawnieniu. Filtr pozwala zawęzić listę uprawnień do wskazanego identyfikatora podmiotu uprawniającego, co jest szczególnie przydatne, gdy podmiot otrzymał uprawnienia od wielu różnych kontrahentów.

Kolumny tabeli prezentują: identyfikator podmiotu uprawniającego (NIP firmy, która nadała uprawnienie), nazwę rodzaju nadanego uprawnienia (np. "Do wystawiania faktur w trybie samofakturowania"), opis nadanego uprawnienia (szczegółowy zakres możliwości) oraz datę początku obowiązywania uprawnienia. Te informacje są kluczowe dla zrozumienia, w czyim imieniu podmiot może działać i w jakim zakresie.



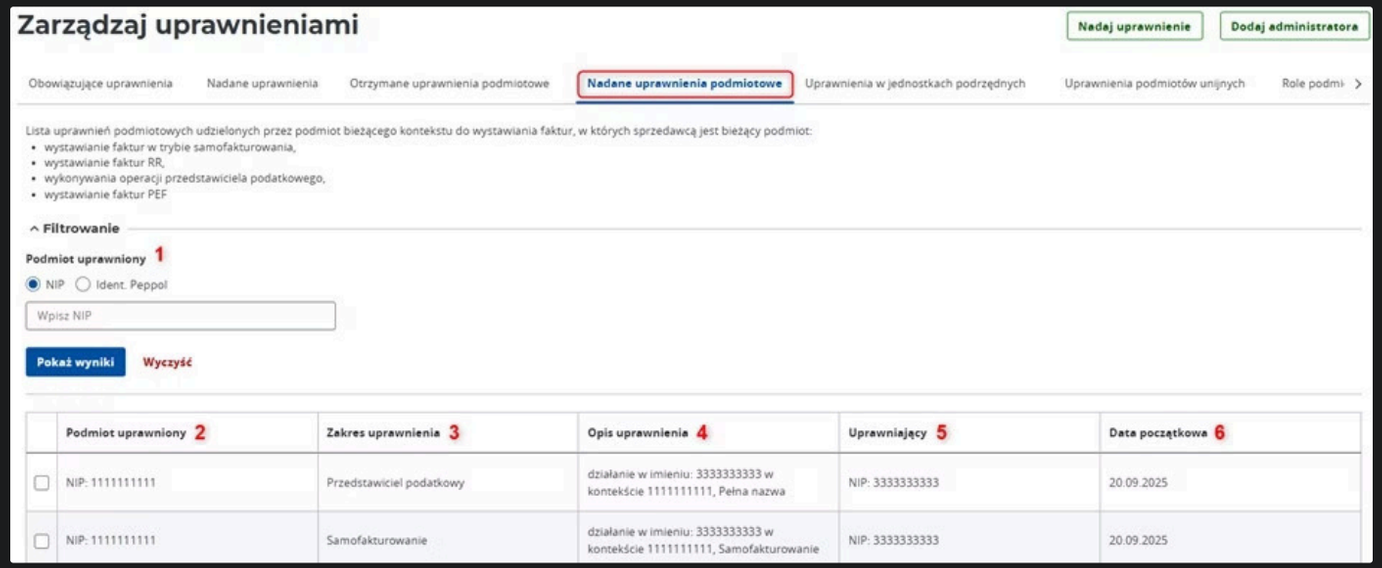
Zakładka Nadane uprawnienia podmiotowe

Tabela "Nadane uprawnienia podmiotowe" prezentuje listę uprawnień podmiotowych udzielonych przez podmiot bieżącego kontekstu do wystawiania faktur, w których sprzedawcą jest bieżący podmiot. To lustrzane odbicie zakładki "Otrzymane uprawnienia podmiotowe" - tutaj widzimy uprawnienia, które my nadaliśmy innym.

Lista obejmuje następujące rodzaje uprawnień: wystawianie faktur w trybie samofakturowania (gdy pozwalamy innemu podmiotowi wystawiać faktury w naszym imieniu), wystawianie faktur VAT RR (dla podmiotów zajmujących się obrotem z rolnikami ryczałtowymi), wykonywanie operacji przedstawiciela podatkowego (dla podmiotów działających jako nasi przedstawiciele podatkowi) oraz wystawianie faktur PEF (dla dostawców usług PEPPOL).

Tabela oferuje filtrowanie po identyfikatorze podmiotu uprawnionego, który może być numerem NIP lub identyfikatorem PEPPOL. To pozwala na szybkie odnalezienie uprawnień nadanych konkretnemu podmiotowi, co jest szczególnie przydatne przy dużej liczbie kontrahentów.

Bardzo ważną funkcjonalnością tej zakładki jest możliwość odbierania nadanych uprawnień. Przy każdym uprawnieniu znajduje się pole wyboru, które po zaznaczeniu aktywuje przycisk "Odbierz uprawnienia". Kolumny tabeli prezentują: nazwę rodzaju nadanego uprawnienia, opis nadanego uprawnienia, identyfikator osoby uprawniającej (kto z naszej firmy nadał to uprawnienie) oraz datę początku obowiązywania uprawnienia.



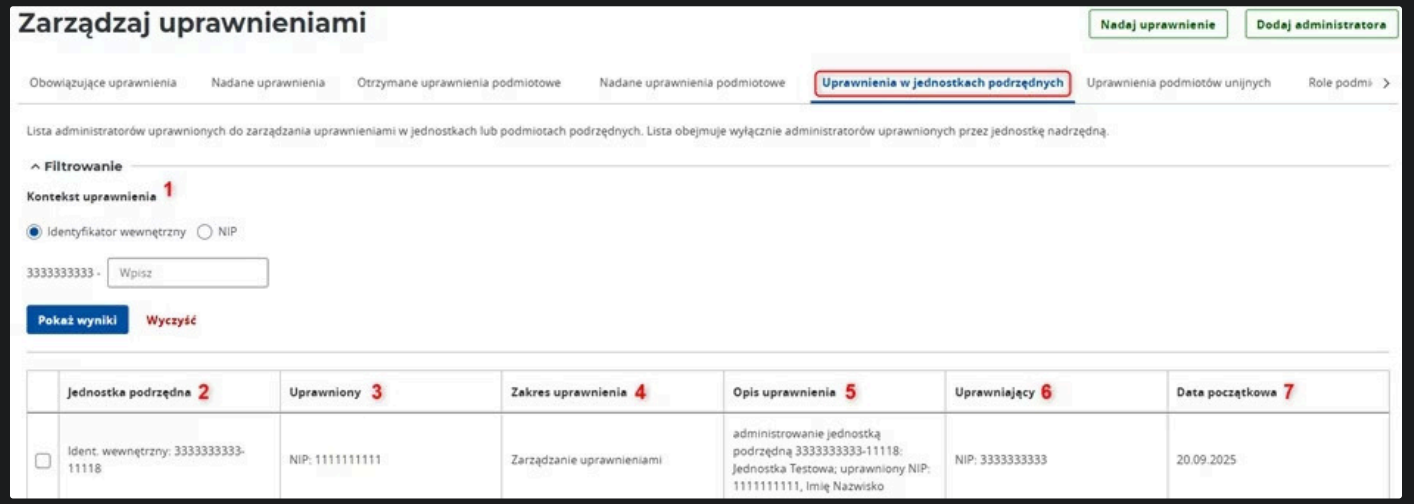
Zakładka Uprawnienia w jednostkach podrzędnych

Tabela "Uprawnienia w jednostkach podrzędnych" prezentuje listę administratorów uprawnionych do zarządzania uprawnieniami w jednostkach lub podmiotach podrzędnych. Ta zakładka jest szczególnie istotna dla organizacji o strukturze hierarchicznej, takich jak jednostki samorządu terytorialnego czy grupy kapitałowe.

Lista obejmuje wyłącznie administratorów uprawnionych przez jednostkę nadrzędną. To oznacza, że widzimy tutaj osoby, którym nadano specjalne uprawnienia do zarządzania uprawnieniami w podległych jednostkach organizacyjnych. To kluczowe narzędzie do zarządzania dostępem w złożonych strukturach organizacyjnych.

System oferuje filtrowanie po identyfikatorze podmiotu uprawnionego, który może być numerem NIP lub identyfikatorem wewnętrznym. To rozróżnienie jest istotne, ponieważ niektóre jednostki podrzędne mogą nie posiadać własnego numeru NIP i są identyfikowane wyłącznie przez identyfikator wewnętrzny nadany przez jednostkę nadrzędną.

Kolumny tabeli prezentują szczegółowe informacje: identyfikator (NIP lub ID wewnętrzny) jednostki podrzędnej, identyfikator osoby uprawnionej (kto został administratorem), nazwę rodzaju nadanego uprawnienia, opis nadanego uprawnienia (zakres możliwości zarządzania), identyfikator osoby uprawniającej (kto nadał to uprawnienie) oraz datę początku obowiązywania uprawnienia. Te dane pozwalają na pełną kontrolę nad strukturą uprawnień w całej organizacji.



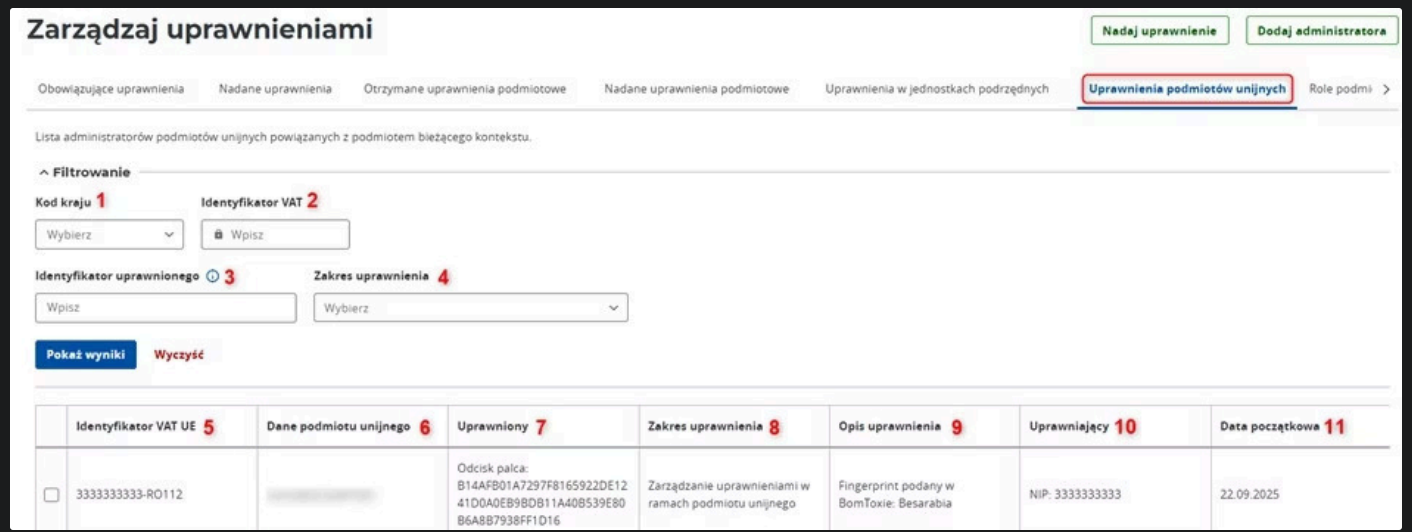
Zakładka Uprawnienia podmiotów unijnych

Tabela "Uprawnienia podmiotów unijnych" prezentuje listę administratorów podmiotów unijnych powiązanych z podmiotem bieżącego kontekstu. Ta zakładka jest szczególnie istotna dla firm prowadzących działalność międzynarodową w ramach Unii Europejskiej.

System oferuje zaawansowane możliwości filtrowania dostosowane do specyfiki podmiotów unijnych. Pierwszy filtr zawiera słownik z nazwami krajów, co pozwala na zawężenie listy do podmiotów z konkretnego kraju członkowskiego UE. To szczególnie przydatne dla firm współpracujących z kontrahentami z wielu różnych krajów.

Drugi filtr zawęża listę uprawnień do wskazanego numeru identyfikacyjnego VAT-UE. Jest to specjalny numer nadawany przedsiębiorcom zarejestrowanym do transakcji wewnątrzwspólnotowych w Unii Europejskiej. Każdy podmiot prowadzący handel wewnątrzunijny posiada taki numer, który jednoznacznie go identyfikuje w systemach podatkowych UE.

Trzeci filtr pozwala zawęzić listę do wpisanego identyfikatora odcisku palca certyfikatu. W tym przypadku należy uzupełnić co najmniej 4 pierwsze znaki odcisku palca, a system automatycznie wyszuka wszystkie pasujące certyfikaty. Dodatkowo dostępny jest filtr zakresu uprawnień, analogiczny do innych zakładek, pozwalający na wybór konkretnych rodzajów uprawnień.



Zakładka "Role podmiotu"

Tabela "Role podmiotu" prezentuje listę ról przypisanych do podmiotu w systemie KSeF. Role określają specyficzny status podmiotu w systemie i wpływają na dostępne funkcjonalności oraz wymagania prawne.

Każdy podmiot w systemie KSeF może mieć przypisaną jedną lub więcej ról, które określają jego status prawny i możliwości działania. Przykładowe role to: podatnik VAT, rolnik ryczałtowy, komornik sądowy, organ egzekucyjny, przedstawiciel podatkowy czy członek grupy VAT. Każda z tych ról niesie ze sobą specyficzne uprawnienia i obowiązki.

Tabela składa się z czterech głównych kolumn. Pierwsza kolumna zawiera opis roli, czyli pełną nazwę i charakterystykę przypisanej roli. Druga kolumna prezentuje identyfikator podmiotu nadrzędnego, jeśli taki istnieje - jest to szczególnie istotne dla członków grup VAT czy jednostek podrzędnych w strukturach hierarchicznych.

Trzecia kolumna zawiera opis powiązania, który wyjaśnia charakter relacji między podmiotem a ewentualnym podmiotem nadrzędnym. Może to być na przykład "członek grupy VAT" lub "jednostka podrzędna JST". Czwarta kolumna prezentuje datę początku obowiązywania uprawnienia, czyli moment, od którego dana rola jest aktywna w systemie. Te informacje są kluczowe dla zrozumienia statusu prawnego podmiotu w systemie KSeF.



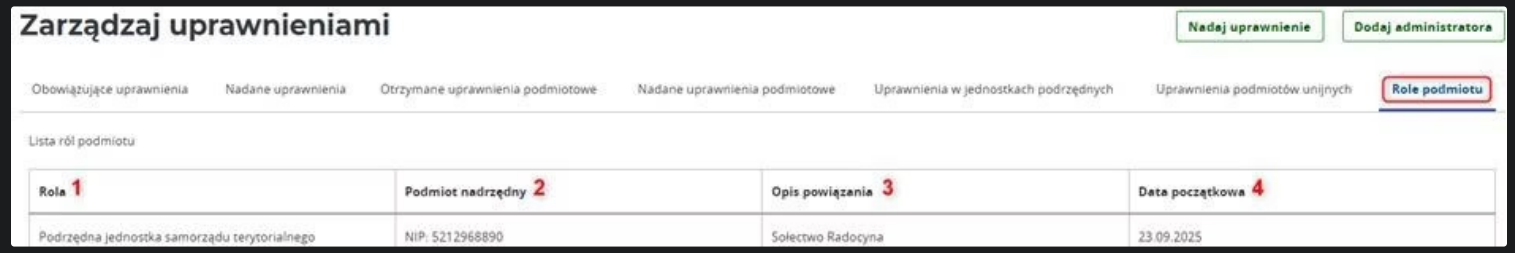
Zakładka "Podmioty podrzędne"

Tabela "Podmioty podrzędne" prezentuje listę podmiotów podrzędnych względem podmiotu bieżącego kontekstu. Ta zakładka jest kluczowa dla organizacji o strukturze hierarchicznej, które zarządzają wieloma jednostkami organizacyjnymi.

Lista obejmuje dwa główne typy podmiotów podrzędnych: podrzędne jednostki samorządu terytorialnego (JST) oraz członków grupy VAT. Jednostki samorządu terytorialnego często mają złożoną strukturę organizacyjną z wieloma jednostkami podległymi, takimi jak szkoły, przedszkola, ośrodki kultury czy zakłady budżetowe. Grupy VAT to z kolei struktury, w których kilka podmiotów jest traktowanych jako jeden podatnik VAT.

System oferuje filtrowanie po numerze NIP podmiotu podrzędnego, co pozwala na szybkie odnalezienie konkretnej jednostki w przypadku dużych organizacji z wieloma podmiotami podrzędnymi. To szczególnie przydatne dla dużych JST czy grup kapitałowych.

Kolumny tabeli prezentują: identyfikator podmiotu podrzędnego (NIP lub identyfikator wewnętrzny), typ powiązania (np. "jednostka podrzędna JST" lub "członek grupy VAT"), opis powiązania (szczegółowe informacje o charakterze relacji) oraz datę początku obowiązywania uprawnienia. Te dane pozwalają na pełne zrozumienie struktury organizacyjnej i zarządzanie dostępem w całej hierarchii podmiotów.



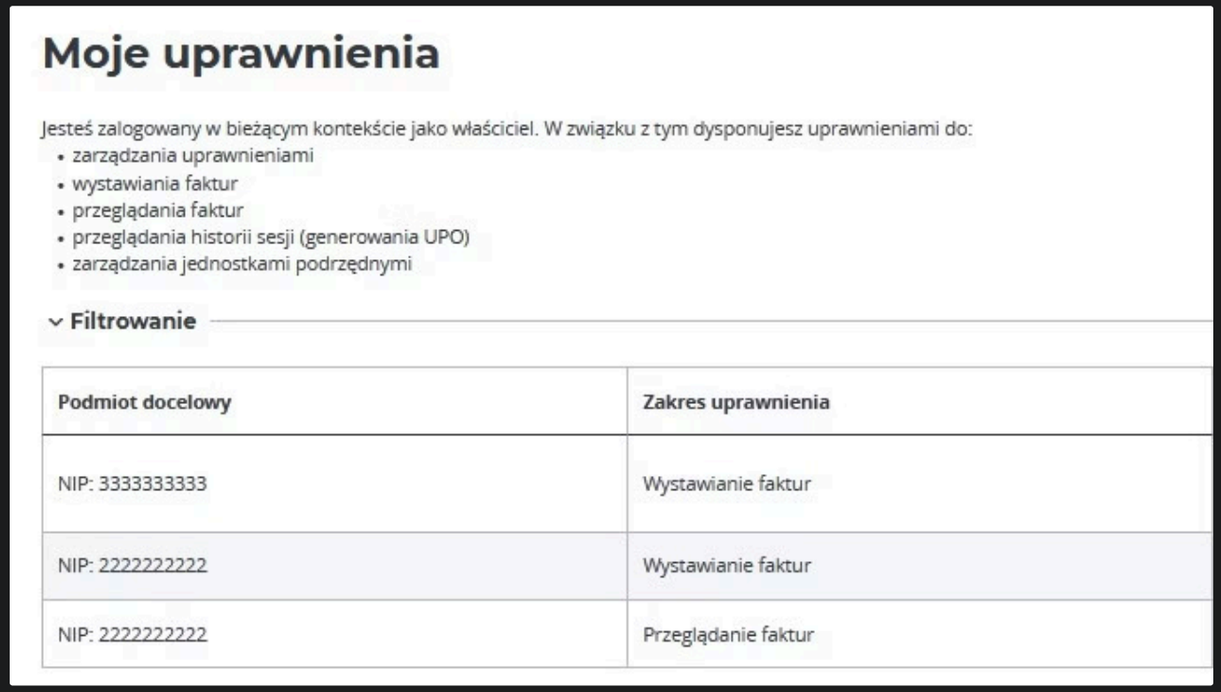
Zakładka Moje uprawnienia - przegląd

Wybór podzakładki "Moje uprawnienia" uruchamia ekran prezentujący listę uprawnień użytkownika w bieżącym kontekście. To osobista przestrzeń każdego użytkownika, gdzie może sprawdzić, do jakich funkcji systemu ma dostęp.

Tabela "Moje uprawnienia" pokazuje wszystkie uprawnienia, które zostały nadane aktualnie zalogowanemu użytkownikowi w ramach bieżącego kontekstu logowania. To niezwykle przydatne narzędzie, które pozwala na szybkie sprawdzenie swoich możliwości w systemie bez konieczności pytania administratora.

W przypadku użytkownika zalogowanego jako właściciel podmiotu, system automatycznie wyświetla pełen zakres uprawnień. Właściciel dysponuje uprawnieniami do: zarządzania uprawnieniami (może nadawać i odbierać uprawnienia innym użytkownikom), wystawiania faktur (może tworzyć i wysyłać faktury elektroniczne), przeglądania faktur (ma dostęp do wszystkich faktur podmiotu), przeglądania historii sesji (może sprawdzać historię generowania UPO) oraz zarządzania jednostkami podrzędnymi (jeśli podmiot ma strukturę hierarchiczną).

Dla użytkowników, którzy nie są właścicielami, tabela pokazuje tylko te uprawnienia, które zostały im faktycznie nadane przez administratora. To pozwala każdemu użytkownikowi na jasne zrozumienie zakresu swoich możliwości w systemie.



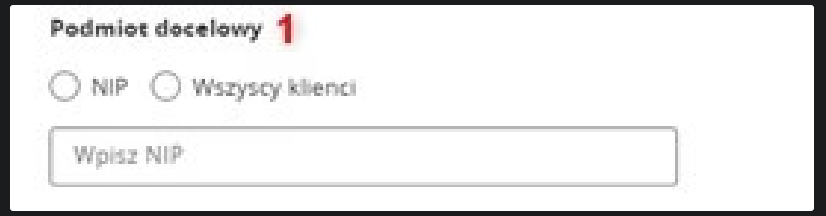
Filtrowanie w zakładce Moje uprawnienia

Zakładka "Moje uprawnienia" oferuje system filtrów, który pozwala na precyzyjne przeglądanie własnych uprawnień. Chociaż lista uprawnień pojedynczego użytkownika jest zazwyczaj krótsza niż w innych zakładkach, filtry są przydatne dla użytkowników z wieloma różnymi uprawnieniami.

Pierwszy filtr zawęża listę uprawnień do wskazanego podmiotu docelowego. Użytkownik może wybrać opcję NIP (dla uprawnień dotyczących konkretnego klienta) lub opcję "Wszyscy klienci" (dla uprawnień generalnych). To rozróżnienie jest szczególnie istotne dla pracowników biur rachunkowych, którzy mogą mieć różne uprawnienia dla różnych klientów.

Drugi filtr zawęża listę uprawnień do wybranego zakresu uprawnień. Użytkownik może zaznaczyć minimum jeden z dostępnych rodzajów uprawnień: zarządzanie uprawnieniami, przeglądanie uprawnień, wystawianie faktur, przeglądanie faktur, przeglądanie historii sesji, zarządzanie jednostkami podrzędnymi oraz operacje egzekucyjne. To pozwala na szybkie sprawdzenie, czy mamy dostęp do konkretnej funkcjonalności.

Trzeci filtr zawęża listę uprawnień do konkretnego statusu - aktywny lub nieaktywny. Choć zazwyczaj w zakładce "Moje uprawnienia" wyświetlane są tylko aktywne uprawnienia, filtr ten może być przydatny do przeglądania historii uprawnień, które zostały odebrane lub wygasły.





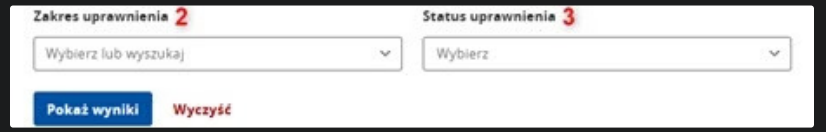
Struktura danych w Moich uprawnieniach

Tabela "Moje uprawnienia" prezentuje dane w przejrzystej strukturze kolumn, która pozwala na szybkie zrozumienie zakresu własnych możliwości w systemie. Każda kolumna zawiera specyficzne informacje o nadanych uprawnieniach.

Pierwsza kolumna prezentuje identyfikator podmiotu podrzędnego, jeśli uprawnienie dotyczy pracy w jednostce podrzędnej. To pole jest wypełnione tylko w przypadku, gdy użytkownik ma uprawnienia do zarządzania lub pracy w ramach jednostek podległych głównemu podmiotowi.

Druga kolumna pokazuje rodzaj podmiotu docelowego, czyli informację, czy uprawnienie dotyczy kontekstu bieżącego (praca bezpośrednio dla podmiotu) czy konkretnego klienta (praca w ramach uprawnień pośrednich). To kluczowe rozróżnienie dla zrozumienia, w czyim imieniu użytkownik może działać.

Trzecia kolumna zawiera nazwę rodzaju nadanego uprawnienia, na przykład "Osobie fizycznej do pracy w KSeF" lub "Osobie fizycznej do pracy dla klienta". Czwarta kolumna prezentuje szczegółowy opis nadanego uprawnienia, który precyzyjnie określa zakres możliwości. Piąta kolumna pokazuje status uprawnienia (aktywny lub nieaktywny), a szósta kolumna zawiera datę początku obowiązywania uprawnienia. Te informacje pozwalają na pełne zrozumienie własnej pozycji w systemie i dostępnych możliwości działania.



Podsumowanie funkcji MCU

Moduł Certyfikatów i Uprawnień (MCU) stanowi kompleksowe narzędzie do zarządzania dostępem do systemu KSeF 2.0. Jego funkcjonalność obejmuje wszystkie aspekty nadawania, przeglądania i odbierania uprawnień, co czyni go niezbędnym elementem pracy z elektronicznymi fakturami.

Elastyczność autoryzacji

System oferuje trzy różne metody uwierzytelnienia, co zapewnia dostępność dla wszystkich typów użytkowników - od osób korzystających z bezpłatnego Profilu Zaufanego po posiadaczy certyfikatów kwalifikowanych.

Kompleksowe zarządzanie

MCU umożliwia zarządzanie uprawnieniami na wielu poziomach - od uprawnień bezpośrednich dla pracowników, przez uprawnienia pośrednie dla biur rachunkowych, po uprawnienia podmiotowe dla różnych form współpracy biznesowej.

Przejrzystość i kontrola

Rozbudowany system zakładek i filtrów pozwala na pełną kontrolę nad nadanymi i otrzymanymi uprawnieniami, zapewniając transparentność zarządzania dostępem do systemu.

Najlepsze praktyki w MCU

Efektywne korzystanie z Modułu Certyfikatów i Uprawnień wymaga przestrzegania kilku kluczowych zasad, które zapewnią bezpieczeństwo danych i sprawne zarządzanie dostępem do systemu KSeF.

Regularne przeglądy uprawnień

Zaleca się systematyczne przeglądanie listy nadanych uprawnień i odbieranie dostępu osobom, które już nie potrzebują pracy w systemie. To podstawowa zasada bezpieczeństwa, która minimalizuje ryzyko nieautoryzowanego dostępu.

Zasada najmniejszych uprawnień

Nadawaj użytkownikom tylko te uprawnienia, które są niezbędne do wykonywania ich obowiązków. Nie przyznawaj automatycznie pełnego zakresu uprawnień - każde uprawnienie powinno być uzasadnione konkretnymi potrzebami biznesowymi.

Dokumentacja uprawnień

Prowadź wewnętrzną dokumentację dotyczącą nadanych uprawnień, szczególnie w przypadku uprawnień pośrednich i podmiotowych. To ułatwi zarządzanie dostępem i będzie pomocne w przypadku audytów.

Bezpieczne przechowywanie certyfikatów

Jeśli korzystasz z certyfikatów kwalifikowanych, zadbaj o ich bezpieczne przechowywanie.

Rozwiązywanie typowych problemów

W trakcie pracy z MCU użytkownicy mogą napotkać różne sytuacje wymagające interwencji. Poniżej przedstawiamy najczęstsze problemy i sposoby ich rozwiązania.

1

Problem z logowaniem

Jeśli nie możesz się zalogować, sprawdź poprawność wprowadzonego identyfikatora (NIP, PESEL, VAT-UE). Upewnij się, że wybrałeś właściwy kontekst logowania i metodę autoryzacji odpowiadającą posiadanym środkom uwierzytelnienia.

2

Błąd przy podpisywaniu

Jeśli system nie akceptuje podpisanego pliku, sprawdź czy plik ma właściwe rozszerzenie (.xml lub .xades) i czy został podpisany właściwie.

3

Brak uprawnień

Jeśli nie widzisz oczekiwanych funkcji w systemie, sprawdź zakładkę "Moje uprawnienia". Jeśli brakuje Ci niezbędnych uprawnień, skontaktuj się z administratorem podmiotu, który może je nadać.

4

Automatyczne wylogowanie

Jeśli system często Cię wylogowuje, pamiętaj o regularnym przedłużaniu sesji poprzez kliknięcie przycisku w komunikacie ostrzegawczym. Zapisuj swoją pracę na bieżąco, aby uniknąć utraty danych.

Bezpieczeństwo w MCU

Bezpieczeństwo danych i dostępu do systemu jest najwyższym priorytetem w MCU. System został zaprojektowany z wykorzystaniem najnowszych standardów bezpieczeństwa, ale jego skuteczność zależy również od odpowiednich praktyk użytkowników.

Zabezpieczenia systemowe

MCU wykorzystuje wielopoziomowe szyfrowanie danych, bezpieczne protokoły komunikacji oraz zaawansowane mechanizmy uwierzytelnienia. Wszystkie operacje są logowane, co pozwala na śledzenie historii zmian i wykrywanie potencjalnych zagrożeń.

System automatycznie wylogowuje użytkowników po okresie bezczynności, co chroni przed nieautoryzowanym dostępem w przypadku pozostawienia komputera bez nadzoru. Dodatkowo, każda krytyczna operacja wymaga potwierdzenia, co zapobiega przypadkowym zmianom.

Odpowiedzialność użytkownika

Użytkownicy są odpowiedzialni za bezpieczne przechowywanie swoich środków uwierzytelnienia - haseł do Profilu Zaufanego, certyfikatów kwalifikowanych czy odcisków palca certyfikatów. Nigdy nie udostępniaj tych danych innym osobom.

Regularnie zmieniaj hasła i sprawdzaj listę nadanych uprawnień. Jeśli zauważysz podejrzaną aktywność lub nieautoryzowane uprawnienia, natychmiast skontaktuj się z administratorem i zmień środki uwierzytelnienia.

Przygotowanie do KSeF 2.0

Moduł Certyfikatów i Uprawnień jest kluczowym elementem przygotowania organizacji do pracy w systemie KSeF 2.0. Odpowiednie zaplanowanie i wdrożenie struktury uprawnień zapewni płynne przejście na nowy system.

Inwentaryzacja potrzeb

Rozpocznij od dokładnej analizy, kto w organizacji będzie potrzebował dostępu do systemu KSeF i w jakim zakresie. Przygotuj listę wszystkich osób i podmiotów, którym trzeba będzie nadać uprawnienia.

Nadanie uprawnień

Systematycznie nadawaj uprawnienia zgodnie z przygotowaną listą. Rozpocznij od kluczowych osób, które będą odpowiedzialne za zarządzanie uprawnieniami, a następnie przejdź do pozostałych użytkowników.

Przygotowanie środków uwierzytelnienia

Upewnij się, że wszyscy przyszli użytkownicy posiadają odpowiednie środki uwierzytelnienia - Profil Zaufany lub certyfikat kwalifikowany. W razie potrzeby pomóż im w uzyskaniu tych narzędzi.

Szkolenie użytkowników

Przeprowadź szkolenia dla wszystkich użytkowników, pokazując im jak logować się do systemu, jak sprawdzać swoje uprawnienia i jak korzystać z podstawowych funkcji MCU.

Kontakt i wsparcie

W przypadku pytań lub problemów z Modułem Certyfikatów i Uprawnień dostępne są różne formy wsparcia. System został zaprojektowany jako intuicyjny, ale w razie potrzeby można skorzystać z pomocy.



Pomoc techniczna

W przypadku problemów technicznych z logowaniem, certyfikatami lub innymi aspektami działania systemu, skontaktuj się z pomocą techniczną Ministerstwa Finansów. Dane kontaktowe są dostępne na stronie głównej MCU.



Dokumentacja

Na stronie systemu KSeF dostępna jest szczegółowa dokumentacja techniczna, instrukcje oraz odpowiedzi na najczęściej zadawane pytania. Warto zapoznać się z tymi materiałami przed rozpoczęciem pracy.



Szkolenia

Ministerstwo Finansów organizuje regularne szkolenia z obsługi systemu KSeF, w tym modułu MCU. Informacje o terminach i zapisach są publikowane na oficjalnej stronie internetowej.

Pamiętaj, że Moduł Certyfikatów i Uprawnień to fundament bezpiecznej pracy w systemie KSeF 2.0. Poświęć czas na dokładne zrozumienie jego funkcjonalności i wdrożenie odpowiednich procedur w swojej organizacji. Prawidłowe zarządzanie uprawnieniami od samego początku zaoszczędzi wiele problemów w przyszłości i zapewni bezpieczną, efektywną pracę z elektronicznymi fakturami.