

Uwierzytelnianie wieloskładnikowe MFA

1 Zarządzanie uwierzytelnianiem wieloskładnikowym

W celu lepszego zabezpieczenia procesu logowania, Portal SZOI, SNRL oraz eWUŚ umożliwia uwierzytelnianie wieloskładnikowe MFA. Dzięki temu każda autoryzacja wymaga podwójnej weryfikacji tożsamości. Rozwiązanie to znacząco ogranicza nieautoryzowany dostęp do systemu przez osoby nieuprawnione.

Jak działa uwierzytelnianie wieloskładnikowe w NFZ?

Podczas standardowego logowania operatora do systemu musi on podać tylko login oraz hasło. Jeżeli osoba nieuprawniona zdobędzie te informacje w sposób nieuprawniony (np. poprzez tak zwany phishing), może bez problemu zalogować się na jego konto.

Uwierzytelnianie dwuskładnikowe wymaga od użytkownika podania dwóch elementów uwierzytelniających takich jak:

- przydzielony login oraz hasło do systemu
- kod hasła jednorazowego generowany w aplikacji zewnętrznej

Wykorzystując dwuetapowe uwierzytelnianie wieloskładnikowe, użytkownik logując się do powyższych systemów będzie musiał podać dotychczas wykorzystywane hasło oraz jednorazowy kod TOTP generowany w aplikacji zewnętrznej np. na telefonie lub tablecie.

Kod TOTP (Time-based One-Time Password) jest jednorazowym kodem generowanym w aplikacji, który jest dostępny dla użytkownika przez określony czas. W przypadku logowania do Portalu SZOI operator ma 30 sekund na jego uzupełnienie. Po jego wygaśnięciu aplikacja generuje automatycznie nowy kod, który będzie obowiązywał przez kolejne 30 sekund.

Aby móc skorzystać z powyższego mechanizmu konieczne jest posiadanie aplikacji, która obsługuje otwarty standard TOTP. Liczba aplikacji generujących tokeny TOTP jest bardzo duża i są to zarówno produkty darmowe jak i komercyjne. Poniżej kilka przykładów:

- Google Authenticator – Google LLC
- Microsoft Authenticator - Microsoft Corporation
- Aegis Authenticator - Beem Development
- FreeOTP Authenticator – Red Hat
- Wizyta Lekarska – Kamssoft S.A.
- LastPass Authenticator - LastPass
- Sophos Authenticator - Sophos GmbH
- Twilio Authy - Authy

Oprócz aplikacji generujących kody MFA na urządzenia mobilne dostępny jest cały szereg rozwiązań alternatywnych.

Natomiast w przeciwieństwie do aplikacji na telefony komórkowe / tablety są one powiązane z danym kontem użytkownika na danym komputerze.

Są to przykładowo dodatki do przeglądarek internetowych. Do wielu przeglądarek dostępny jest cały szereg rozwiązań tego typu. Poniżej kilka przykładów:

- **Authenticator** - dodatek do przeglądarki Chrome <https://chromewebstore.google.com/detail/authenticator/bhghoaapcdpbohphigoooaddinpkbai?pli=1>
- **Authenticator: 2FA Client** - dodatek do przeglądarki Microsoft Edge <https://microsoftedge.microsoft.com/addons/detail/authenticator-2fa-client/ocglkepbibnalbgmbachknglpdipeoio>
- **Authenticator by MindStorm** - dodatek do przeglądarki Firefox <https://addons.mozilla.org/en-US/firefox/addon/auth-helper/>

Inną alternatywą są aplikacje dla systemów operacyjnych desktopowych, np. dla systemu Windows, które dostępne są w Windows Store:

- **OTPKEY Authenticator** <https://apps.microsoft.com/detail/xp9mcl9t4jfz0b?hl=en-us&gl=US>
- **Oracle Mobile Authenticator** - <https://apps.microsoft.com/detail/9nblggh4nsh8?hl=en-us&gl=US>

- **Authme - Two factor (2FA) authenticator** <https://apps.microsoft.com/detail/xp9m33rjsvd6jr?hl=pl-pl&gl=PL>

Aplikacje o tych samych funkcjach występują również w środowiskach Linuxowych czy też dla platformy IOS.

Należy mieć świadomość, że wyżej wymienione rozwiązania to tylko jedne z wielu dostępnych możliwości.

2 Rejestracja aplikacji

Od 11 czerwca 2024 dla wszystkich operatorów logujących się do Portalu SZOI/SNRL wymagane jest wykorzystywanie mechanizmu wieloskładnikowej autoryzacji (MFA). Konta bez włączonego MFA nie mogą pracować w portalu.

Jeżeli konto nie ma skonfigurowanego MFA po zalogowaniu się operatora do systemu pojawi się poniższy komunikat:

UWAGA

W CELU DALSZEJ PRACY Z SYSTEMEM WYMAGANE JEST WŁĄCZENIE UWIERZYTELNIANIA WIELOSKŁADNIKOWEGO (MFA).

Aby włączyć funkcjonalność skorzystaj z przycisku poniżej ("Uwierzytelnianie wieloskładnikowe") lub wyloguj się z systemu. Szczegółowy opis mechanizmu MFA został opisany w instrukcji w rozdziale *Zarządzanie uwierzytelnianiem wieloskładnikowym*, dostępnej na głównej stronie logowania lub pod poniższym linkiem.

Musisz pamiętać, że dodana aplikacja (urządzenie) będzie wykorzystywana w przyszłości przy każdym logowaniu się operatora do systemu.

Instrukcja obsługi Systemu Zarządzania Obiegiem Informacji: [więcej](#)

Rys. 1 Informacja na temat konieczności konfiguracji uwierzytelnienia wieloskładnikowego

WAŻNE!

Aby operator mógł skonfigurować uwierzytelnianie wieloskładnikowe w SZOI/SNRL musi mieć nadane uprawnienie *Praca z modułem użytkownika SZOI / Praca z modułem użytkownika SNRL*. Jeżeli nie będzie posiadał tego uprawnienia nie będzie się mógł zalogować do systemu

W celu skonfigurowania uwierzytelniania MFA, należy wybrać opcję .

Rozpoczęcie korzystania z mechanizmu MFA wymaga jednorazowego wykonania czynności powiązania konta w portalu z aplikacją do uwierzytelniania.

Pierwszym krokiem włączenia logowania MFA jest rejestracja aplikacji, która będzie wykorzystywana do uwierzytelniania wieloskładnikowego na dostępnym urządzeniu. **Należy pamiętać, że aplikacja (urządzenie) będzie wykorzystywane w przyszłości przy każdym logowaniu się operatora do systemu.**

Uwierzytelnienie wieloskładnikowe

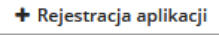
Zarejestrowane aplikacje Kody zapasowe

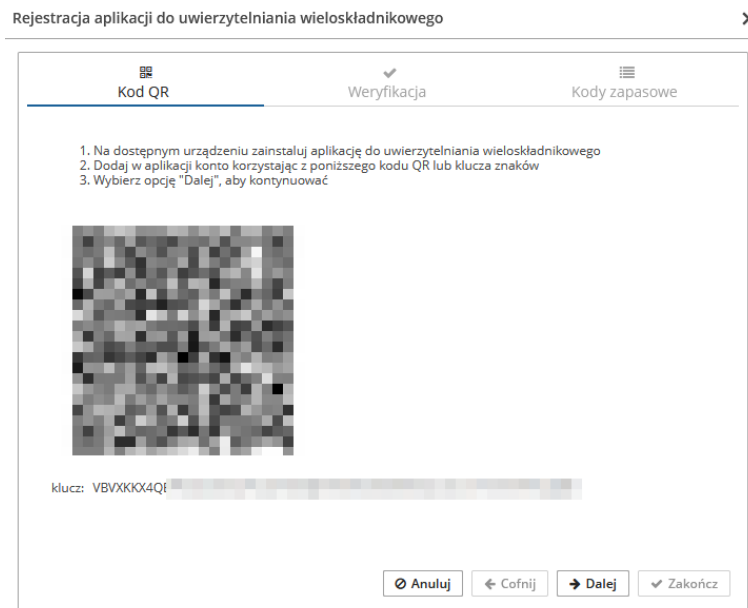
Aktywność
 Data rejestracji

0 pozycji



Lp.	Data rejestracji/usunięcia	Aktywność	Obsługa
Brak danych			

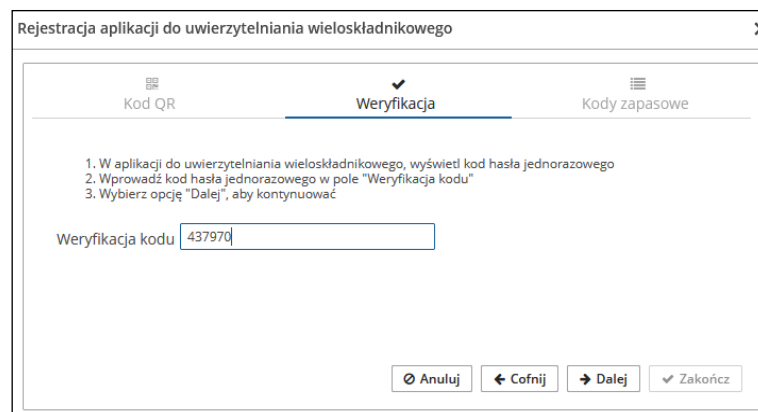
Rys. 2 Uwierzytelnienie wieloskładnikowe

Aby powiązać aplikację z kontem dostępowym, należy z głównego menu SZOI/SNRL wybrać *System* -> *Uwierzytelnianie wieloskładnikowe*, a następnie opcję . Wykorzystując wyświetlony na ekranie kod QR lub klucz znaków należy dodać nowe konto w aplikacji.




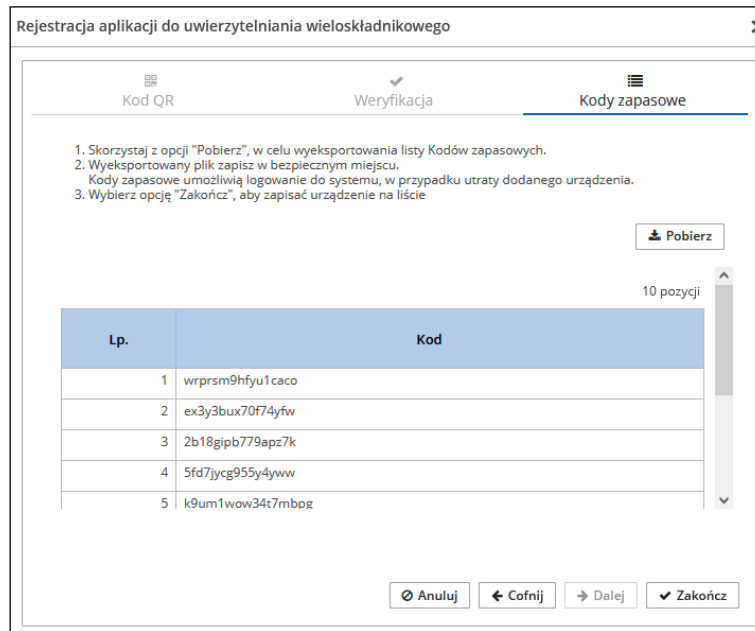
Rys. 3 Rejestracja aplikacji do uwierzytelnienia wieloskładnikowego

Po zarejestrowaniu należy wybrać opcję , a w kolejnym oknie uzupełnić kod hasła jednorazowego (jego ważność to 30 sekund), który jest generowany w aplikacji do uwierzytelniania wieloskładnikowego. Po uzupełnieniu kodu należy wybrać opcję , aby kontynuować.



Rys. 4 Rejestracja aplikacji do uwierzytelnienia wieloskładnikowego - weryfikacja

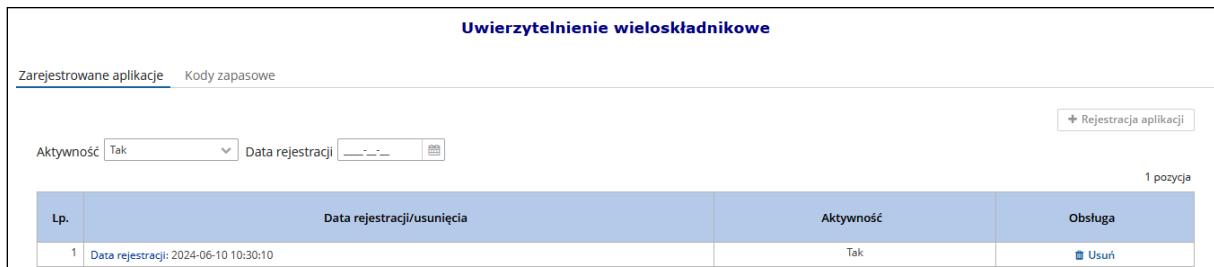
W ostatnim kroku korzystając z opcji , należy pobrać listę kodów zapasowych, które w przyszłości będą wykorzystywane do logowania do systemu w przypadku utraty urządzenia wykorzystywanego do logowania MFA. Pobrany plik TXT, należy zapisać w bezpiecznym miejscu.



Rys. 5 Rejestracja aplikacji do uwierzytelnienia wielokładnikowego – kody zapasowe

Po wybraniu opcji [Zakończ](#) urządzenie zostanie dodane do listy. Od tego momentu podczas logowania się operatora oprócz loginu oraz hasła konieczne będzie podanie kodu weryfikacyjnego wygenerowanego w zarejestrowanej aplikacji. **Jednocześnie konto może mieć zarejestrowaną tylko jedną aktywną aplikację.**

Jeżeli zaistnieje konieczność zmiany formy logowania MFA (np. instalacja aplikacji na innym urządzeniu, zmiana aplikacji z telefonu na wtyczkę do przeglądarki), należy przejść do okna *Uwierzytelnianie wielokładnikowe*, za pomocą opcji **Usuń** dostępnej w kolumnie *Obsługa* wyrejestrować aplikację uwierzytelniającą i zarejestrować nową.



Rys. 6 Uwierzytelnienie wielokładnikowe

3 Kody zapasowe

Kody zapasowe służą do awaryjnego logowania w przypadku braku możliwości skorzystania z aplikacji do uwierzytelniania (zgubienie lub uszkodzenie telefonu, przywrócenie urządzenia do stanu fabrycznego). Są to kody jednorazowego użytku, które zaleca się wydrukować i schować w bezpiecznym miejscu.

Aby zapoznać się z kodami zapasowymi, należy z głównego menu wybrać *System -> Uwierzytelnianie wieloskładnikowe -> Kody zapasowe*. Na liście zawarte będą aktualnie obowiązujące kody odzyskiwania. Pozycje, które zostały już wykorzystane będą oznaczone jako zamglone.

Opcja umożliwia wygenerowanie nowej listy kodów zapasowych. Po ich uzyskaniu należy je ponownie pobrać, wydrukować i schować w bezpiecznym miejscu.



The screenshot shows a web interface titled "Uwierzytelnianie wieloskładnikowe". At the top, there are tabs for "Zarejestrowane aplikacje" and "Kody zapasowe". On the right side, there are two buttons: "+ Nowe kody" and "Pobierz". Below the buttons, there is a pagination indicator: "Bieżący zakres pozycji: 1-10 z [1] [2] [3]". The main content is a table with two columns: "Lp." and "Kod".

Lp.	Kod
1	4woFbdxakmaq2ip
2	q5f8w6kkzu6c553y
3	[blurred]
4	u87v5kenfg57hs1
5	1266jwm4mtl6jys
6	oa741xxcq6gzcj7
7	[blurred]
8	oi36eflekq3st7zb
9	y9uhc2fflk4ze98s
10	c68tdu6kzhm94cq0

Rys. 7 Kody zapasowe do uwierzytelniania wieloskładnikowego

4 Awaryjne usunięcie konfiguracji MFA dla użytkownika

Jeżeli użytkownik utraci możliwość generacji kodów jednorazowych (brak dostępu do aplikacji) oraz nie posiada kodów zapasowych, musi zgłosić się do administratora świadczeniodawcy (operatora mającego nadane uprawnienie *Administracja kontrahentem*), który usunie urządzenie przeznaczone do generacji kodów MFA powiązane z kontem użytkownika. W takim przypadku przy kolejnym logowaniu użytkownika do systemu konieczne będzie skonfigurowanie nowej aplikacji. Jeżeli powyższa sytuacja wystąpi w przypadku konta administratora, należy skontaktować się z OW NFZ.

Kroki postępowania podczas usuwania aplikacji powiązanej z kontem użytkownika:

1. Administrator kontrahenta (operator mający nadane uprawnienie *Administracja kontrahentem*) musi z głównego menu portalu wybrać *Administrator -> Zarządzanie operatorami*.
2. Na liście operatorów, należy wyszukać użytkownika, dla którego konieczne jest awaryjne usunięcie MFA.
3. Z kolumny *Operacje* wybrać opcję **Usunięcie MFA**.

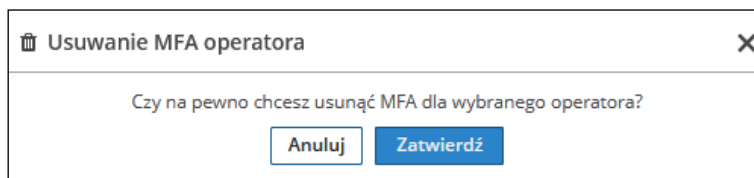


The screenshot shows the 'Operatorzy' management page. At the top right, there are buttons for 'Pobierz raport' and '+ Dodawanie operatora'. Below these are search filters for 'Login' (containing 'Zawiera' and 'TESTHASLA') and a 'Szukaj' button. There are also filters for 'Aktywność' (set to '-- wszystkie --') and 'Aktywność na dzień' (set to '2024-06-10'). A table below shows one operator with the following details:

Lp.	Login	Nazwisko i imię	Aktywność	Obsługa
1.	TESTHASLA	NAZWISKO IMIĘ	Tak	<ul style="list-style-type: none"> Uprawnienia Edytuj Usuń Historia Usunięcie MFA

Rys. 8 Lista operatorów

4. Potwierdzić usunięcie konfiguracji MFA danego operatora



The dialog box is titled 'Usuwanie MFA operatora' and contains the question: 'Czy na pewno chcesz usunąć MFA dla wybranego operatora?'. At the bottom, there are two buttons: 'Anuluj' and 'Zatwierdź'.

5. Konfiguracja uwierzytelnienia użytkownika została usunięta. Podczas kolejnego logowania użytkownika do systemu konieczne będzie ponowne skonfigurowanie MFA.
6. Usunięcie konfiguracji MFA dla podstawowego konta administratora (login konta administratora rozpoczyna się od cyfr np. 150... lub 7000...) wymaga kontaktu z OW NFZ.

5 Najczęściej zadawane pytania

1. Do czego służy weryfikacja wieloetapowa MFA?
 - W celu lepszego zabezpieczenia procesu logowania, Portal SZOI, SNRL oraz eWUŚ umożliwia uwierzytelnianie wieloskładnikowe MFA. Dzięki temu każda autoryzacja wymaga podwójnej weryfikacji tożsamości. Rozwiązanie to znacząco ogranicza nieautoryzowany dostęp do systemu przez osoby nieuprawnione.
2. Do czego służą kody zapasowe?
 - Kody zapasowe umożliwiają awaryjne zalogowanie się operatora do systemu w przypadku braku możliwości skorzystania z aplikacji do uwierzytelniania (zgubienie lub uszkodzenie telefonu, przywrócenie urządzenia do stanu fabrycznego). Kody te nie wpływają na comiesięczną zmianę hasła do systemu i nie należy ich używać w ten sposób.
3. Ile aplikacji przeznaczonych do generacji kodów jednorazowych może być przypisanych do konta użytkownika?
 - Do jednego konta użytkownika można przypisać tylko jedną aplikację do generacji kodów jednorazowych.
4. Co zrobić jeżeli użytkownik utraci dostęp do aplikacji generującej kody jednorazowe, a kody zapasowe nie zostały zapisane i nie można z nich skorzystać?
 - Jeżeli użytkownik utraci możliwość generacji kodów jednorazowych oraz nie posiada kodów zapasowych, musi zgłosić się do administratora świadczeniodawcy (operatora mającego nadane uprawnienie *Administracja kontrahentem*), który usunie urządzenie przeznaczone do generacji kodów MFA powiązane z kontem użytkownika. W takim przypadku przy kolejnym logowaniu użytkownika do systemu konieczne będzie skonfigurowanie nowej aplikacji. Jeżeli powyższa sytuacja wystąpi w przypadku konta administratora, należy skontaktować się z OW NFZ.
5. Gdzie można skonfigurować weryfikację wieloetapową MFA?
 - Weryfikacja wieloetapowa może być skonfigurowana jedynie w Portalu SZOI/SNRL w części *System* -> *Uwierzytelnianie wieloetapowe*.
6. Jakie uprawnienie jest wymagane do konfiguracji uwierzytelniania wieloskładnikowego?
 - Aby operator mógł skonfigurować uwierzytelnianie wieloskładnikowe w SZOI/SNRL musi mieć nadane uprawnienie *Praca z modułem użytkownika SZOI / Praca z modułem użytkownika SNRL*. Jeżeli nie będzie posiadał tego uprawnienia, nie będzie się mógł zalogować do systemu.
7. Co zrobić, aby zmniejszyć ryzyko utraty dostępu do SZOI?
 - Aby zmniejszyć ryzyko związane z utraceniem dostępu do konta, nie należy pracować na koncie administratora (login konta administratora rozpoczyna się od cyfr np. 150... lub 7000...). Do codziennej pracy z systemem należy korzystać z utworzonych kont operatorów z nadanymi tylko niezbędnymi uprawnieniami. Konto administracyjne powinno służyć głównie do nadawania uprawnień innym użytkownikom oraz do awaryjnego usuwania urządzenia MFA.
8. Czy operator może skonfigurować MFA tak, by kody dostępu przychodziły jednocześnie na kilka telefonów, np. lekarza oraz informatyka?
 - Nie. Każda osoba powinna korzystać wyłącznie z własnego konta, a konto może być powiązane tylko z jednym urządzeniem mobilnym. Świadczeniodawca może dodać konta nowych operatorów w SZOI wchodząc w zakładkę *Operatorzy* -> *Dodawanie operatora*.
9. Czy usługi sieciowe wykorzystywane w oprogramowaniu też będą wymagały dodatkowego kodu uwierzytelniającego?
 - Nie. Ani usługa służąca do weryfikacji uprawnień eWUŚ ani usługa dostępowa służąca do wymiany komunikatów XML nie wymaga dodatkowego kodu uwierzytelniającego.

6 Logowanie MFA do Portalu SZOI

Jeżeli logowanie wieloskładnikowe zostało włączone (aplikacja przeznaczona do logowania wieloskładnikowego została zarejestrowana), to podczas logowania po uzupełnieniu loginu oraz hasła wymagane jest dodatkowo uzupełnienie kodu weryfikacyjnego wygenerowanego w aplikacji:

1. W oknie logowania do SZOI należy uzupełnić login oraz hasło.
2. Podać kod weryfikujący wygenerowany w zewnętrznej aplikacji uwierzytelniającej.



Rys. 9 Logowanie do SZOI za pomocą kodu weryfikacyjnego

3. Jeżeli operator nie ma dostępu do aplikacji uwierzytelniającej, może skorzystać z kodu zapasowego zawartego w pliku TXT jaki został pobrany podczas rejestracji aplikacji (opcja **Zaloguj się za pomocą kodu zapasowego**).



Rys. 10 Logowanie do SZOI za pomocą kodu zapasowego

7 Logowanie MFA do Portalu SNRL

Jeżeli logowanie wieloskładnikowe zostało włączone (aplikacja przeznaczona do logowania wieloskładnikowego została zarejestrowana), to podczas logowania po uzupełnieniu loginu oraz hasła wymagane jest dodatkowo uzupełnienie kodu weryfikacyjnego wygenerowanego w aplikacji:

1. W oknie logowania do SNRL należy uzupełnić login oraz hasło.
2. Podać kod weryfikujący wygenerowany w zewnętrznej aplikacji uwierzytelniającej.



Rys.11 Logowanie do SNRL za pomocą kodu weryfikacyjnego

3. Jeżeli operator nie ma dostępu do aplikacji uwierzytelniającej, może skorzystać z kodu zapasowego zawartego w pliku TXT jaki został pobrany podczas rejestracji aplikacji (opcja **Zaloguj się za pomocą kodu zapasowego**).



Rys. 12 Logowanie do SNRL za pomocą kodu zapasowego