

ZARZĄDZANIE UWIERZYTELNIENIEM WIELOSKŁADNIKOWYM

W Portalu Świadczeniodawcy Narodowego Funduszu Zdrowia istnieje możliwość stosowania uwierzytelniania wieloskładnikowego. Uwierzytelnianie wieloskładnikowe znacznie podnosi bezpieczeństwo – zabezpieczenie przed dostępem do portalu osób nieuprawnionych.

Stosowanie do identyfikacji samych identyfikatorów użytkownika i haseł, obecnie, stało się już niewystarczające ze względu na duże zagrożenie włamaniami do systemu a także metody stosowane przez hakerów.

Wdrożenie mechanizmu **uwierzytelniania wieloskładnikowego (MFA)** w Portalu Świadczeniodawcy ma kluczowe znaczenie dla zapewnienia bezpieczeństwa. Klasyczne hasła nie są już bezpieczne głównie dlatego, że:

- użytkownicy nadal używają słabych haseł,
- używają tych samych haseł w wielu portalach,
- strony nadal źle zabezpieczają hasła, co powoduje możliwość wycieku haseł.

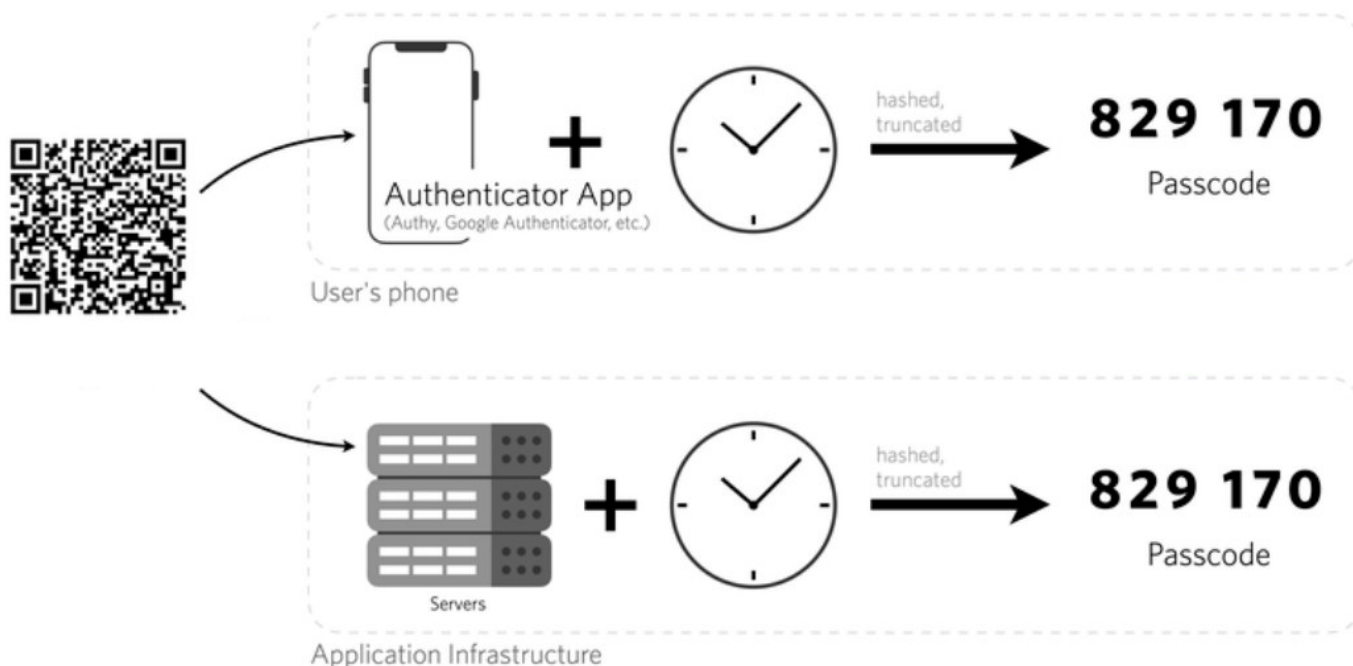
Czym jest uwierzytelnianie wieloskładnikowe?

Uwierzytelnianie wieloskładnikowe składa się z czegoś co użytkownik zna czyli np. hasła, kodu, PIN-u i dodatkowo czegoś co użytkownik ma czyli np. telefon, token sprzętowy, karta kodów. Mogą być również wykorzystywane indywidualne cechy użytkownika czyli odcisk palca, tęczówka (może być wykorzystywana biometria).

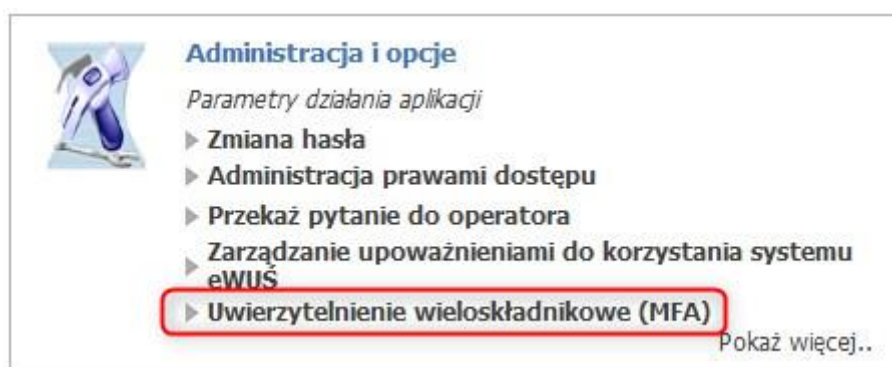
MFA wymaga dwóch lub więcej składników do uwierzytelnienia. W systemie Narodowego Funduszu Zdrowia zastosowano uwierzytelnianie dwuskładnikowe czyli składające się z hasła (jak do tej pory) i z systemu jednorazowych kodów wysyłanych na urządzenie świadczeniodawcy np. na telefon komórkowy.

Tokeny TOTP.

TOTP (Time-based One-Time Password), jest to mechanizm oparty na czasie. Od momentu wygenerowania hasła/kodu użytkownik ma określoną liczbę sekund na jego użycie, w przeciwnym wypadku straci ono ważność.



Operator Portalu Świadczeniodawcy ma możliwość zarządzania sposobem uwierzytelniania do portalu. Dostępność mechanizmu MFA w systemie Funduszu nie oznacza, że został on automatycznie włączony dla wszystkich świadczeniodawców. Rozpoczęcie stosowania uwierzytelniania dwuskładnikowego wymaga włączenia go przez operatora świadczeniodawcy, korzystając z funkcji **Włącz** w funkcji konfiguracji MFA.

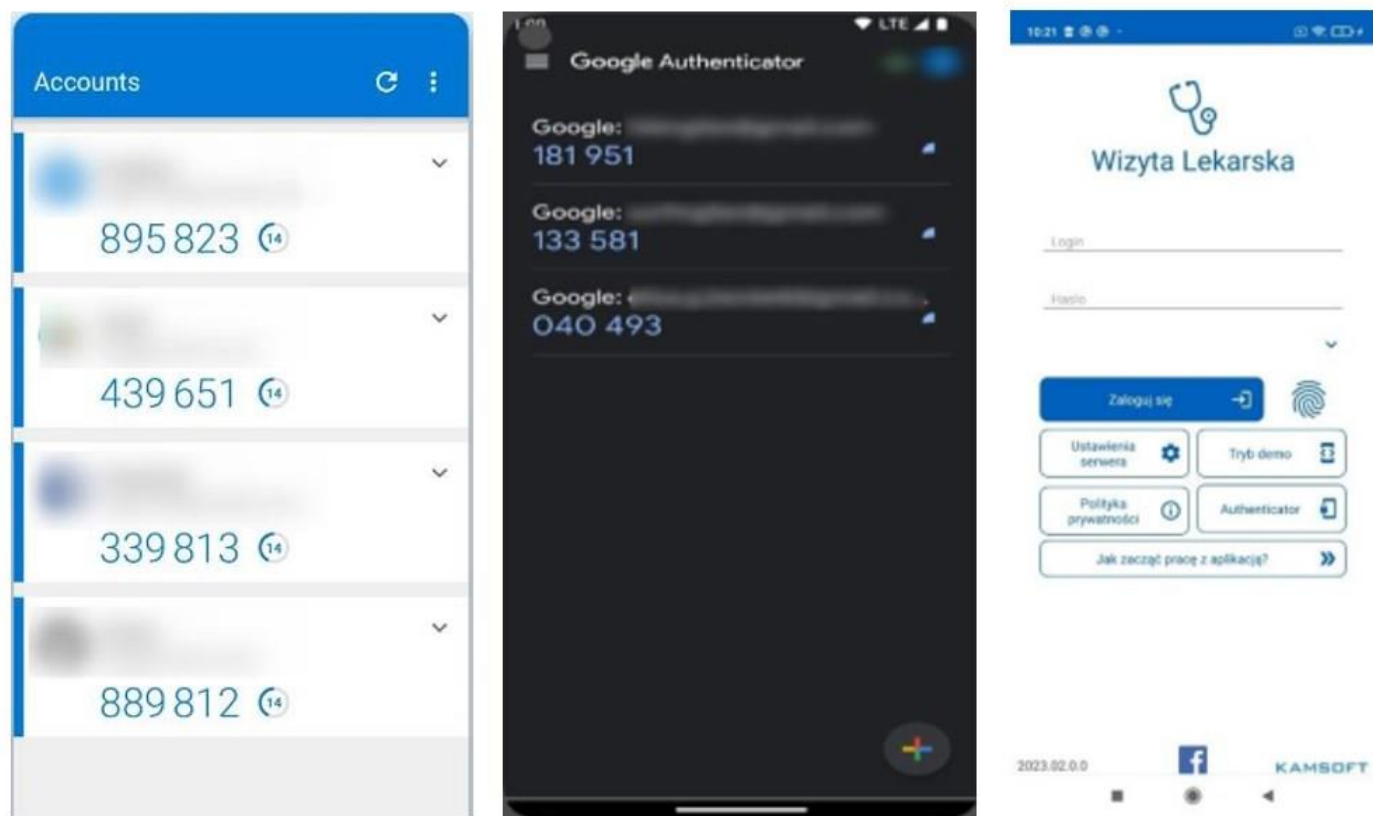


Zarządzanie uwierzytlenieniem wieloskładnikowym

Powrót Pomoc		
 Kod świadczeniodawcy: Nazwa świadczeniodawcy: Użytkownik:		
Składnik	Informacja	Akcje
Konfiguracja uwierzytlenienia	Nieaktywny	Włącz
Kody odzyskiwania	Nieaktywny	

Operator Portalu Świadczeniodawcy może włączyć mechanizm MFA wykorzystujący tokeny TOTP.

Aby móc skorzystać z tego mechanizmu konieczne jest posiadanie na urządzeniu aplikacji, która obsługuje otwarty standard TOTP. Taką aplikacją jest np. Microsoft Authenticator, Google Authenticator, Wizyta lekarska firmy Kamsoft, ale liczba aplikacji generujących tokeny TOTP jest bardzo duża i są to zarówno produkty darmowe jak i komercyjne.



Oprócz aplikacji generujących kody MFA na urządzenia mobilne jest cały szereg rozwiązań alternatywnych. Natomiast w przeciwieństwie do aplikacji na telefony komórkowe 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 prezentujemy zaledwie kilka przykładów:

- **Authenticator** - dodatek do przeglądarki Chrome <https://chromewebstore.google.com/detail/authenticator/bhghoaamapcdpbohphigoooaddinpkbai?pli=1>
- **Authenticator: 2FA Client** - dodatek do przeglądarki Microsoft Edge <https://microsoftedge.microsoft.com/addons/detail/authenticator-2fa-client/ocglkepbibnalbgmbachknlgldipeioio>
- **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, przykłady poniżej to aplikacje dostępne z Windows Store:

- **Authme - Two factor (2FA) authenticator** <https://apps.microsoft.com/detail/xp9m33rjsvd6jr?hl=pl-pl&gl=PL>
- **OTPKEY Authenticator** <https://apps.microsoft.com/detail/xp9mcl9t4jzf0b?hl=en-us&gl=US>
- **Oracle Mobile Authenticator** - <https://apps.microsoft.com/detail/9nblggh4nsh8?hl=en-us&gl=US>

Aplikacje o tych samych funkcjach występują również w środowiskach Linuxowych czy też dla platformy iOS. Należy mieć świadomość, że wyżej wymienione rozwiązania to tylko jedno z wielu dostępnych możliwości.

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

Aby móc włączyć MFA wykorzystujący tokeny TOTP, użytkownik musi zeskanować w aplikacji, którą ma zainstalowaną np. na telefonie kod QR wyświetlony w portalu.

Skanowanie kodu QR
Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.


Ręczne dodanie konta
Wprowadź poniższe informacje ręcznie w aplikacji do uwierzytelniania:
Nazwa konta:
Sekret:

W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej
Kod hasła jednorazowego:

Zamiast zeskanowania kodu QR użytkownik może go przepisać ręcznie czyli na żądanie wyświetlić kod (sekret) i przepisać/skopiować do aplikacji używanej do uwierzytelniania. Wpisanie kodu ręcznie da ten sam efekt co zeskanowanie kodu QR. W aplikacji do uwierzytelniania zostanie wygenerowany kod potwierdzający.

TOTP – Potwierdzanie konta

Twilio (Example Account)

765 286



Segment (Example Account)

003 457



Aby potwierdzić powiązanie aplikacji uwierzytelniającej z portalem należy wpisać 6-cyfrowy kod, generowany przez aplikację i użyć funkcji **Powiąż**. Nastąpi powiązanie uwierzytelnienia wieloskładnikowego.

W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej

Kod hasła jednorazowego:

Zweryfikowano pozytywnie

Kody odzyskiwania

Aby nie stracić dostępu do konta na wypadek utraty urządzenia z aplikacją uwierzytelniającą, wygenerowane zostały kody odzyskiwania jednorazowego użytku.
Aby kontynuować, naciśnij przycisk **Drukuj** lub **Zapisz**. Wydruk/plik zachowaj w bezpiecznym miejscu.

Od7bxut	
Zzrsgldf	
e073er5	
en6me6	
fxoqcjpv	

Kolejnym krokiem, wymaganym w procesie włączania MFA, jest wyświetlenie kodów odzyskiwania wraz z możliwością ich wydruku lub zapisania. Kody te pozwalają na awaryjne zalogowanie się wykorzystując MFA w przypadku utracenia urządzenia generującego tokeny TOTP lub wystąpienia problemu z użyciem aplikacji uwierzytelniającej. Są to kody jednorazowego użytku (raz wykorzystany kod staje się nieaktywny). Zaleca się te kody wydrukować, zapisać i schować w bezpieczne miejsce, nie ujawniać ich osobom niepowołanym.

Po wydrukowaniu/zapisaniu kodów operator zapisuje konfigurację za pomocą klawisza Zapisz konfigurację. Po poprawnym zapisaniu pokaże się informacja **Poprawnie zapisano konfigurację**.

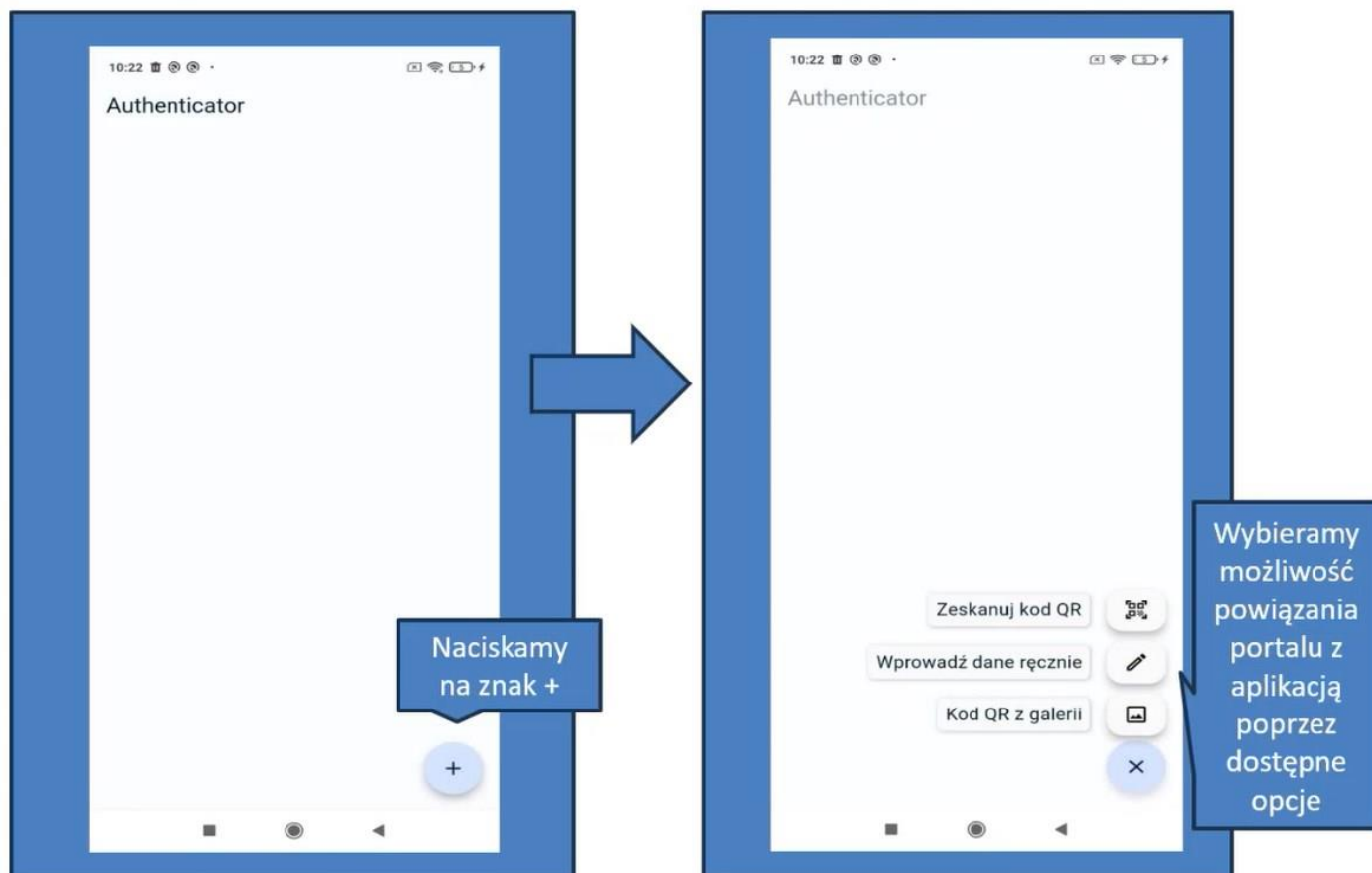
Włączanie MFA i powiązanie aplikacji do uwierzytelniania z portalem – wykaz czynności.

1. Aby włączyć MFA wykorzystujący tokeny TOTP operator musi skorzystać z linku **Włącz**.

Zarządzanie uwierzytlenieniem wieloskładnikowym

▶ Powrót ▶ Pomoc		
 Kod świadczeniodawcy: Nazwa świadczeniodawcy: Użytkownik:		
Składnik	Informacja	Akcje
Konfiguracja uwierzytlenienia	Nieaktywny	Włącz
Kody odzyskiwania	Nieaktywny	

2. Po otwarciu formatki w aplikacji do uwierzytelniania operator dodaje i skanuje kod QR na aplikacji zewnętrznej.



3. Zamiast zeskanowania można kliknąć w **Dodaj konto ręcznie**.

Administracja uwierzytelniania wieloskładnikowego (MFA)

[Powrót](#)
[Pomoc](#)



Kod świadczeniodawcy:
 Nazwa świadczeniodawcy:
 Użytkownik:

Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



[Dodaj konto ręcznie](#)

W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej

Kod hasła jednorazowego:

[Powiąż](#)

4. Po udanym powiązaniu urządzenia, aplikacja jest gotowa do uwierzytelnienia wieloskładnikowego.



5. Operator przepisuje kod z aplikacji zewnętrznej do portalu i klika w **Powiąż**.

Administracja uwierzytelniania wieloskładnikowego (MFA)

[Powrót](#) [Pomoc](#)



Kod świadczeniodawcy: 01221
Nazwa świadczeniodawcy: Niepubliczna przychodnia Jutrzenka
Użytkownik: magda_szkolenie

Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



Ręczne dodanie konta

Wprowadź poniższe informacje ręcznie w aplikacji do uwierzytelniania:

Nazwa konta: Portal NFZ OW08:ws-01221-magda_szkolenie
Sekret: HOFERKIMKYG6DPGXZF2XOXKTP4HM42ZHMNUJD58ZYLRDRKBMUNRH30TEWTGMXAOD

[Ukryj](#)

W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej

Kod hasła jednorazowego:

[Powiąż](#)

6. Po prawidłowym powiązaniu pokaże się informacja **Zweryfikowano pozytywnie** oraz lista kodów odzyskiwania.

Lista kodów odzyskiwania jest to lista 10 kodów, które można użyć w przypadku problemów z użyciem aplikacji uwierzytelniającej np. zgubienia lub uszkodzenia telefonu.

Kody należy zapisać lub wydrukować. Bez tej czynności program nie będzie mógł zakończyć konfiguracji.

W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej

Kod hasła jednorazowego:

Zweryfikowano pozytywnie

[Powiąż](#)

Kody odzyskiwania

Aby nie stracić dostępu do konta na wypadek utraty urządzenia z aplikacją uwierzytelniającą, wygenerowane zostały kody odzyskiwania jednorazowego użytku.

Aby kontynuować, naciśnij przycisk **Drukuj** lub **Zapisz**. Wydruk/plik zachowaj w bezpiecznym miejscu.

[Drukuj](#)

[Zapisz](#)

0d7bxut

2zrsgldf

e073er5

en6me6

fxoqcjpv

7. Po wydrukowaniu/zapisaniu kodów operator zapisuje konfigurację za pomocą klawisza **Zapisz konfigurację**. Po poprawnym zapisaniu pokaże się informacja **Poprawnie zapisano konfigurację**.

W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej

Kod hasła jednorazowego:

Zweryfikowano pozytywnie

Powiąż

Kody odzyskiwania

Aby nie stracić dostępu do konta na wypadek utraty urządzenia z aplikacją uwierzytelniającą, wygenerowane zostały kody odzyskiwania jednorazowego użytku.
Aby kontynuować, naciśnij przycisk **Drukuj** lub **Zapisz**. Wydruk/plik zachowaj w bezpiecznym miejscu.

Drukuj Zapisz

0d7bxut1	
2zrsgldh	
e073er5	
en6me6	
fxoqcjpw	
h2h6jhht	
id5kpxuc	
ok6zsuht	
t0l13aex	
vd5p72k	

Poprawnie zapisano konfigurację.

Wyjdź

Jeśli mechanizm logowania do portalu z wykorzystaniem mechanizmu MFA jest już aktywny to pojawią się dodatkowe funkcje/linki.

Zarządzanie uwierzytelnieniem wieloskładnikowym

Powrót Pomoc		
	Kod świadczeniodawcy: Nazwa świadczeniodawcy: Użytkownik:	
Składnik	Informacja	Akcje
Konfiguracja uwierzytelnienia	Aktywny	Wyłącz Kod qr Nowa konfiguracja
Kody odzyskiwania	Aktywny	Podgląd Generuj nowe

WYŚWIETLENIE KODU QR

Wyświetlenie kodu QR może być przydatne w sytuacji, gdy operator chce używać więcej niż jednego telefonu do uwierzytelniania – generowania kodów jednorazowych. W takim przypadku, dla aplikacji zainstalowanej

na kolejnym telefonie należy powtórzyć operacje powiązania aplikacji z kontem w Portalu. Należy ponownie wykonać skanowanie kodu QR lub wpisanie kodu ręcznie.

Operator może wyświetlić **Kod QR**.

Składnik	Informacja	Akcje
Konfiguracja uwierzytelnienia	Aktywny	Wyłącz Kod qr Nowa konfiguracja
Kody odzyskiwania	Aktywny	Podgląd Generuj nowe

Administracja uwierzytelniania wieloskładnikowego (MFA)

[▶ Powrót](#) [▶ Pomoc](#)



Kod świadczeniodawcy:
Nazwa świadczeniodawcy:
Użytkownik:

Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



Dodaj konto ręcznie

Należy przepisać lub skopiować kod (sekret) do aplikacji generującej jednorazowe kody.



Kod świadczeniodawcy:
Nazwa świadczeniodawcy:
Użytkownik:

Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



Ręczne dodanie konta

Wprowadź poniższe informacje ręcznie w aplikacji do uwierzytelniania:

Nazwa konta: Portal NFZ

Sekret: BWMH

Ukryj

KONFIGURACJA UWIERZYTELNIENIA WIELKOSKŁADNIKOWEGO (TOTP)

Aby potwierdzić zeskanowanie lub przepisanie kodu i przejść dalej należy wpisać token/kod 6 cyfrowy wygenerowany przez aplikację służącą do generowania tokenów TOTP a następnie kliknąć w **Powiąz**.

Administracja uwierzytelniania wieloskładnikowego (MFA)

[▶ Powrót](#) [▶ Pomoc](#)



Kod świadczeniodawcy:
Nazwa świadczeniodawcy:
Użytkownik:

Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



Dodaj konto ręcznie

W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej

Kod hasła jednorazowego:

Powiąż

LISTA KODÓW ODZYSKIWANIA

Kody odzyskiwania.

Kody odzyskiwania służą do awaryjnego logowania w przypadku braku możliwości skorzystania z aplikacji do uwierzytelniania, niezbędnej do uwierzytelniania MFA (zgubienie lub uszkodzenie telefonu, przywrócenie urządzenia do stanu fabrycznego).

Są to kody jednorazowego użytku, które zaleca się wydrukować i schować w bezpieczne miejsce.

Lista kodów odzyskiwania

► Powrót ► Pomoc



Kod świadczeniodawcy:
Nazwa świadczeniodawcy:
Użytkownik:



Kody odzyskiwania

W celu wygenerowania nowych kodów odzyskiwania przejdź do panelu **Nowe kody odzyskiwania**

Drukuj

Zapisz

Kod odzyskiwania	Użycie
2n7sa	Niewykorzystany
33tpu	Niewykorzystany
4wkst	Niewykorzystany
5w9fk	Niewykorzystany
ax25v	Niewykorzystany
o82f7	Niewykorzystany
s2hbg	Niewykorzystany
sk418	Niewykorzystany
snmjv	Niewykorzystany
stv76	Niewykorzystany

Aby wygenerować nowe kody odzyskiwania należy przejść do strony **Zarządzanie uwierzytelnieniem wieloskładnikowym** i skorzystać z linku **Generuj nowe** lub posłużyć się linkiem **Nowe kody odzyskiwania**.



Kody odzyskiwania

W celu wygenerowania nowych kodów odzyskiwania przejdź do panelu **Nowe kody odzyskiwania**

Drukuj

Zapisz

Kody, które zostały wykorzystane są oznaczone jako **Wykorzystane** oraz dodatkowo przekreślone.

Lista kodów odzyskiwania

► Powrót ► Pomoc



Kod świadczeniodawcy:
Nazwa świadczeniodawcy:
Użytkownik:

[Blurred information]



Kody odzyskiwania

W celu wygenerowania nowych kodów odzyskiwania przejdź do panelu **Nowe kody odzyskiwania**

Drukuj

Zapisz

Kod odzyskiwania	Użycie
1lsvyuaynv	Niewykorzystany
42avcqtuh3jc	Niewykorzystany
6axe6l1uluv	Wykorzystany
7qjmnzd1rd9	Niewykorzystany
9je7duvu6zei	Wykorzystany
acjq6dkzlz0pi	Niewykorzystany
k9j9xby3d8l0	Niewykorzystany
pr1zz3ecxej1	Niewykorzystany
v5dod80r5os	Niewykorzystany
zaw62t6nfst9	Niewykorzystany

Uwaga: Jeżeli z jakiegoś powodu, kody odzyskiwania zostaną przez osobę nieuprawnioną przechwycone, należy jak najszybciej anulować kody poprzez wygenerowanie nowych, które je nadpiszą.

GENEROWANIE NOWYCH KODÓW ODZYSKIWANIA

Aby wygenerować nowe kody odzyskiwania należy skorzystać z linku **Generuj nowe** na stronie **Zarządzanie uwierzytelnieniem wieloskładnikowym**.

Składnik	Informacja	Akcje
Konfiguracja uwierzytelnienia	Aktywny	Wyłącz Kod qr Nowa konfiguracja
Kody odzyskiwania	Aktywny	Podgląd Generuj nowe

Operator zostanie poproszony o potwierdzenie tożsamości poprzez wpisanie hasła do Portalu Świadczeniodawcy.

Potwierdź tożsamość do Portalu Świadczeniodawcy



Kod świadczeniodawcy:
Użytkownik:



Hasło:

Po wpisaniu hasła otworzy się strona z wygenerowanymi kodami odzyskiwania.

Przycisk **Zapisz**, zapisuje kody odzyskiwania.

Przycisk **Drukuj** umożliwia wydrukowanie kodów odzyskiwania.

Generowanie nowych kodów odzyskiwania

[▶ Powrót](#) [▶ Pomoc](#)



Kod świadczeniodawcy:
Nazwa świadczeniodawcy:
Użytkownik:



Kody odzyskiwania

Aby nie stracić dostępu do konta na wypadek utraty urządzenia z aplikacją uwierzytelniającą, wygenerowane zostały kody odzyskiwania jednorazowego użytku.
Aby kontynuować, naciśnij przycisk **Drukuj** lub **Zapisz**. Wydruk/plik zachowaj w bezpiecznym miejscu. Po zapisaniu/wydrukowaniu pojawi się przycisk **Zapisz konfigurację**, użyj go w celu zapisania nowych kodów.

Kod odzyskiwania	Użycie
02hp6ini0	Niewykorzystany
1xwo1b1l	Niewykorzystany
48xilas5t	Niewykorzystany
bd2z9:	Niewykorzystany
eu1ms	Niewykorzystany
fdqievcki	Niewykorzystany
gs86kzqh	Niewykorzystany
kfmt1e8	Niewykorzystany
x39fro9r	Niewykorzystany
xa0a4:	Niewykorzystany

Po zapisaniu lub wydrukowaniu kodów odzyskiwania należy zapisać konfigurację za pomocą przycisku **Zapisz konfigurację**.

Kod odzyskiwania	Użycie
1mcp3:	Niewykorzystany
1p6npy	Niewykorzystany
6p2bf8	Niewykorzystany
7du1ip	Niewykorzystany
8s007c	Niewykorzystany
cx0xjp	Niewykorzystany
f5ycgq	Niewykorzystany
ieg8pq	Niewykorzystany
rf9v84t	Niewykorzystany
rlblrwvf	Niewykorzystany

Zapisz konfigurację

Wyjdź