UWIERZYTELNIENIE WIELOSKŁADNIKOWE (MFA)

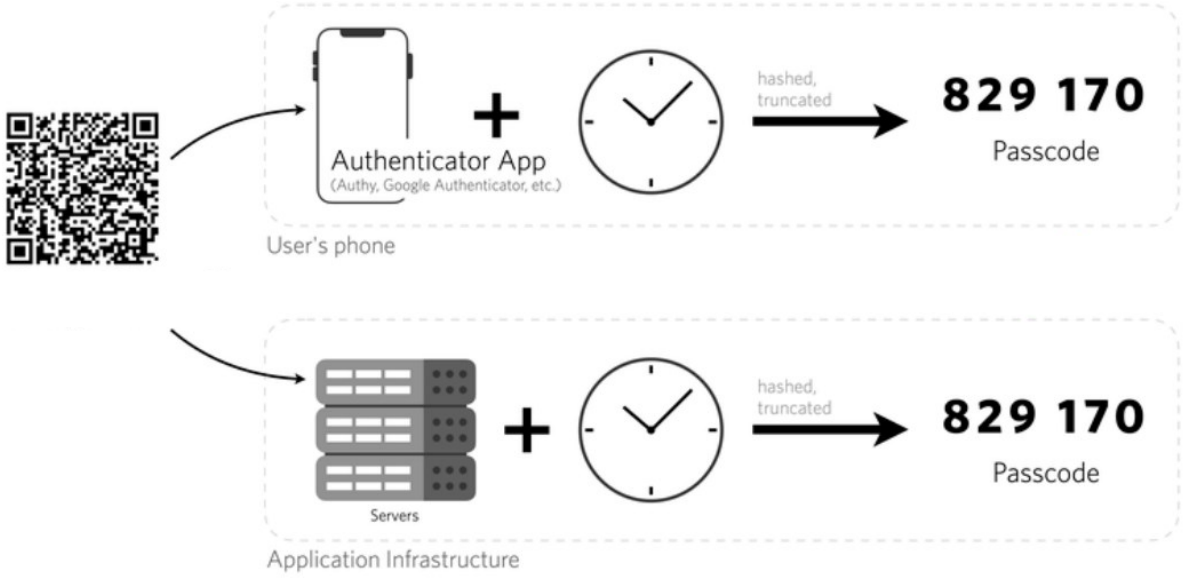
1. ZARZĄDZANIE UWIERZYTELNIENIEM WIELOSKŁADNIKOWYM

W Portalu Personelu 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.

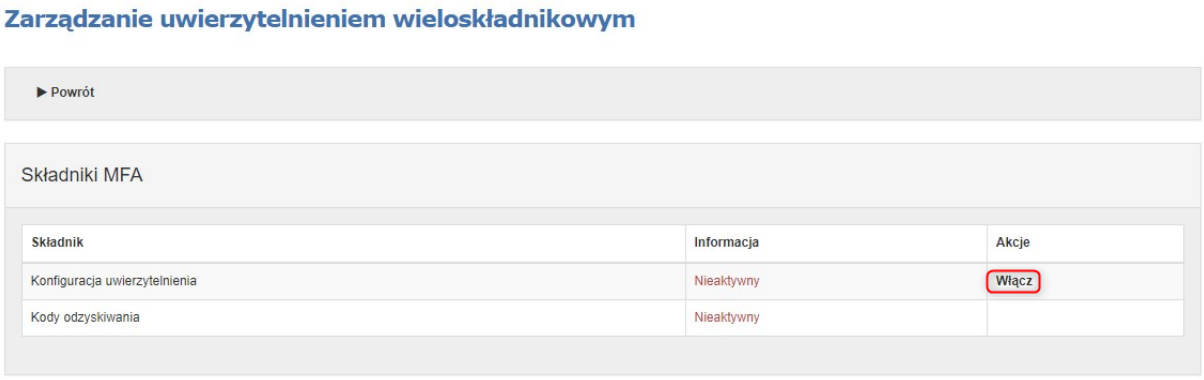
Wdrożenie mechanizmu **uwierzytelniania wieloskładnikowego (MFA)** w Portalu Personelu ma kluczowe znaczenie dla zapewnienia bezpieczeństwa. Często klasyczne hasła nie są już bezpieczne głównie dlatego, że użytkownicy np. nadal używają słabych haseł, nadal używają tych samych haseł w wielu portalach, 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
Operator Portalu Personelu może włączyć mechanizm MFA wykorzystując 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.

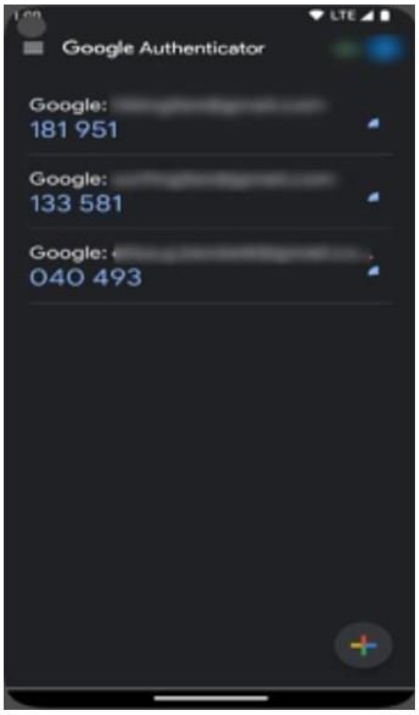


Operator Portalu Personelu ma możliwość zarządzania sposobem uwierzytelniania do portalu. Dostępność mechanizmu MFA w systemie Funduszu nie oznacza, że został on automatycznie włączony dla wszystkich świadczeniodawców. Rozpoczęcie stosowania uwierzytelniania dwuskładnikowego wymaga włączenia go przez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



Operator Portalu Personelu 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/bhghoamapcdpbohphigoooaddinpkbai?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, przykłady poniżej to aplikacje dostępne z Windows Store:

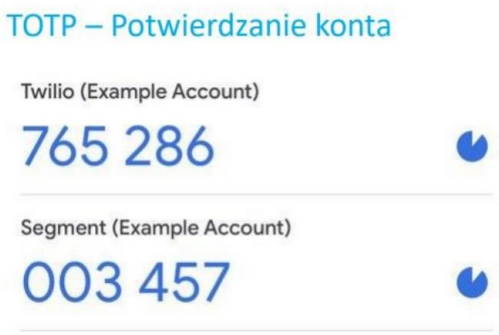
- **Authme - Two factor (2FA) authenticator** https://apps.microsoft.com/detail/xp9m33rjsvd6jr?hl=pl-pl&gl=PL
- **OTPKEY Authenticator** https://apps.microsoft.com/detail/xp9mcl9t4jfz0b?hl=en-us&gl=US
- **Oracle Mobile Authenticator** - https://apps.microsoft.com/detail/9nblggh4nsh8?hl=en-us&gl=US

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

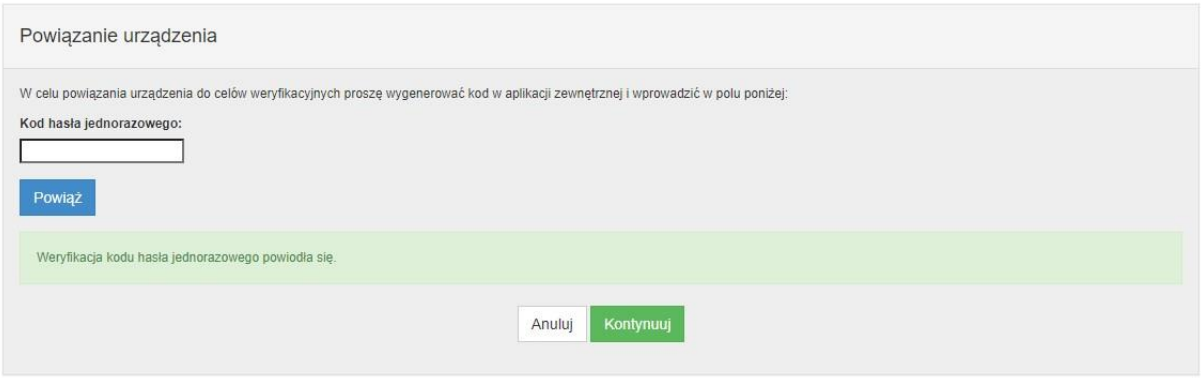
Rozpoczęcie korzystania z mechanizmu FMA wymaga jednorazowego wykonania czynności powiązania konta w portalu z aplikacją do uwierzytelniania.

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

Zamiast zeskanowania kodu QR użytkownik może go przepisać ręcznie czyli na żądanie wyświetlić kod 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.



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

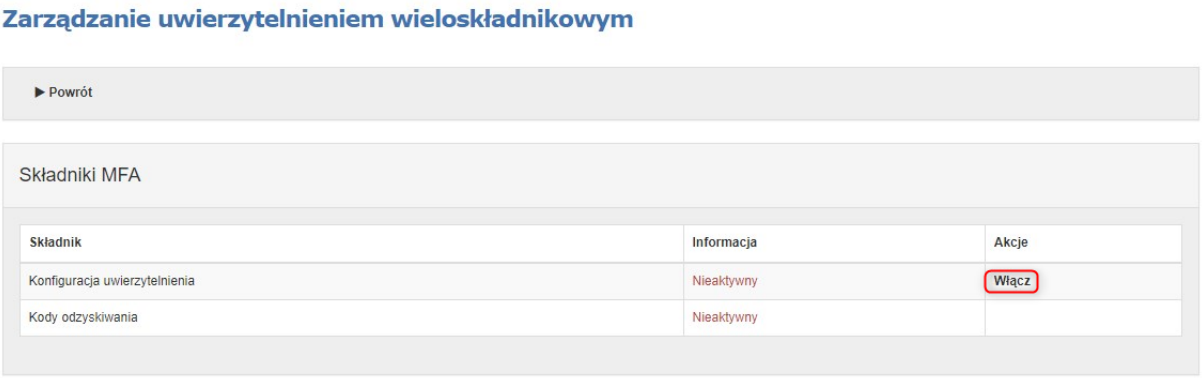


Kolejnym krokiem, wymaganym w procesie właczania MFA, jest wyświetlenie kodów odzyskiwania wraz z możliwością ich wydruku lub zapisania. Kody te pozwalają na awaryjne zalogowanie się wykorzystując MFA w przypadku utracenia urządzenia generującego tokeny TOTP lub wystąpienia problemu z użyciem aplikacji uwieżytelniajacej. 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.

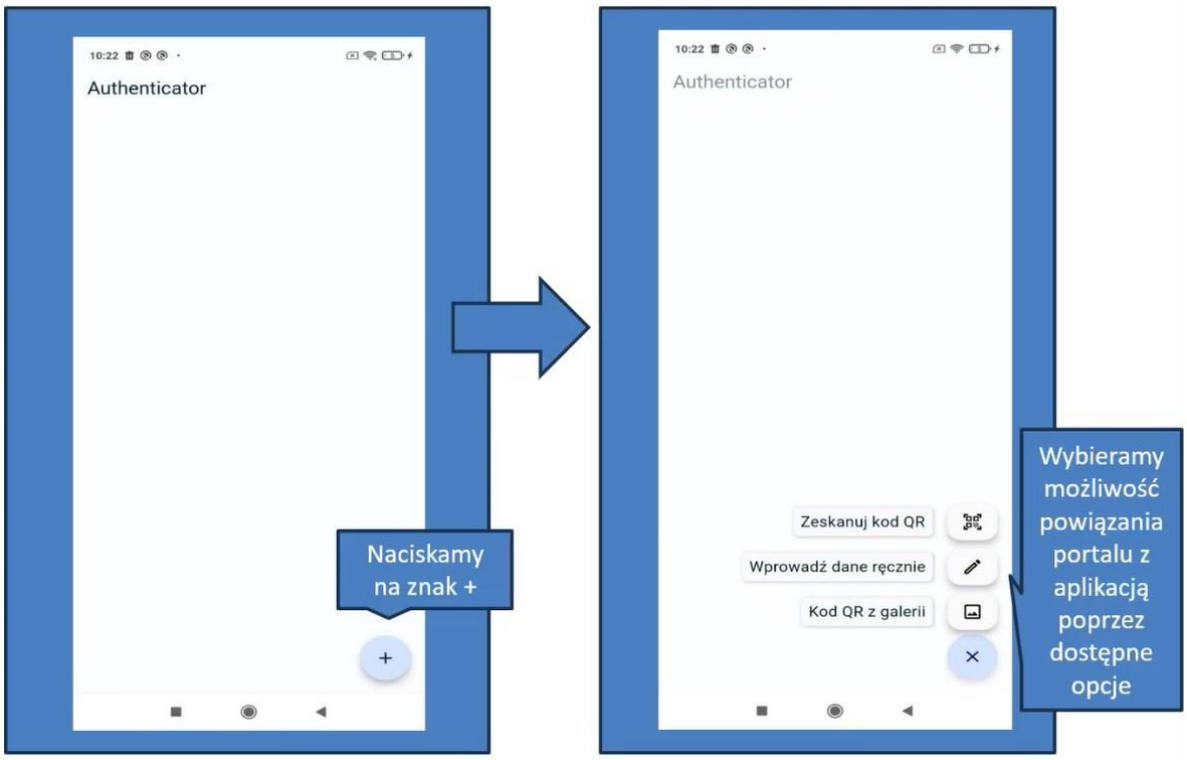
Po wydrukowaniu/zapisaniu kodów operator zapisuje konfigurację za pomocą klawisza Kontynuuj.

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

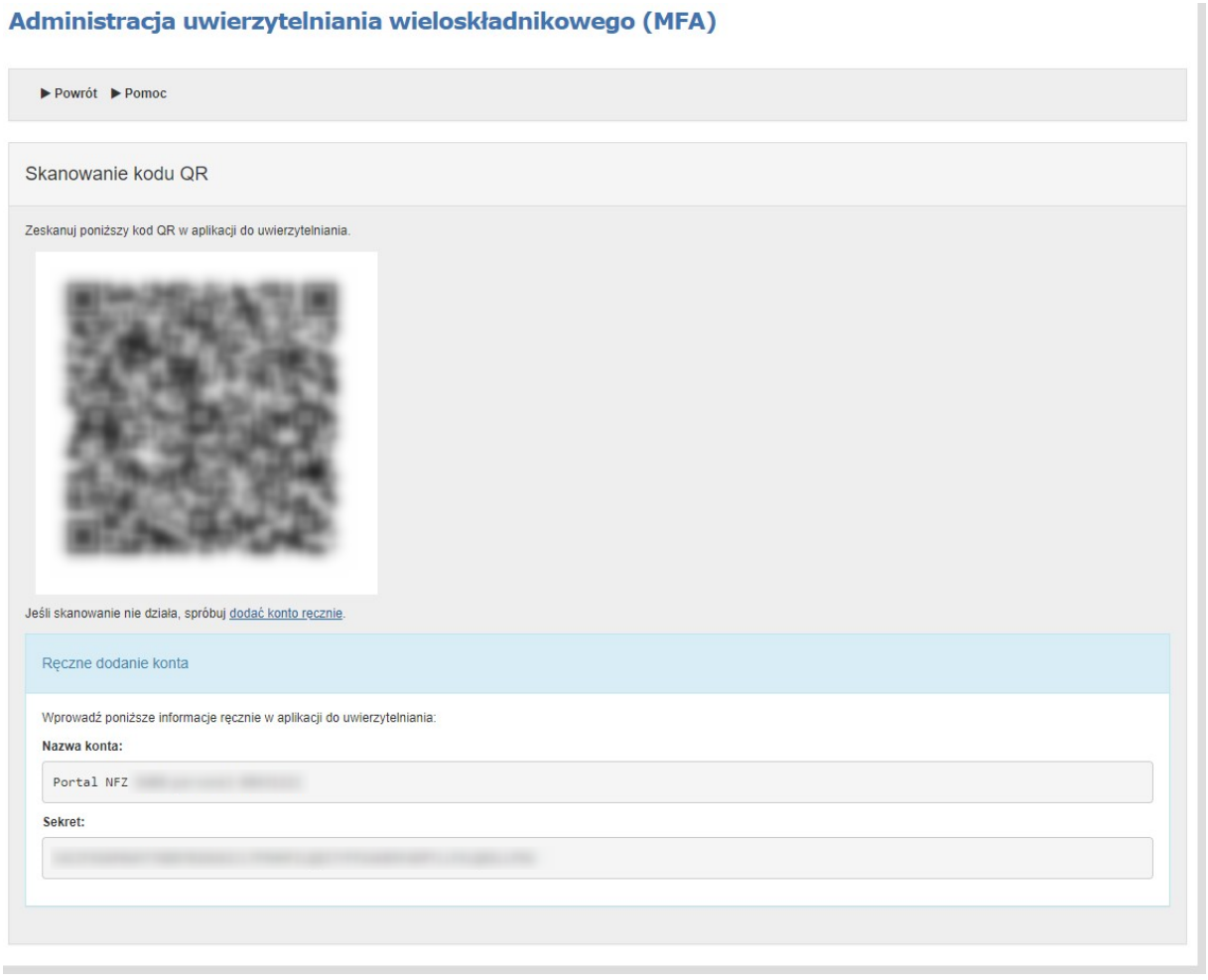
1. Aby włączyć MFA wykorzystujący tokeny TOTP operator musi skorzystać z linku **Włącz**.



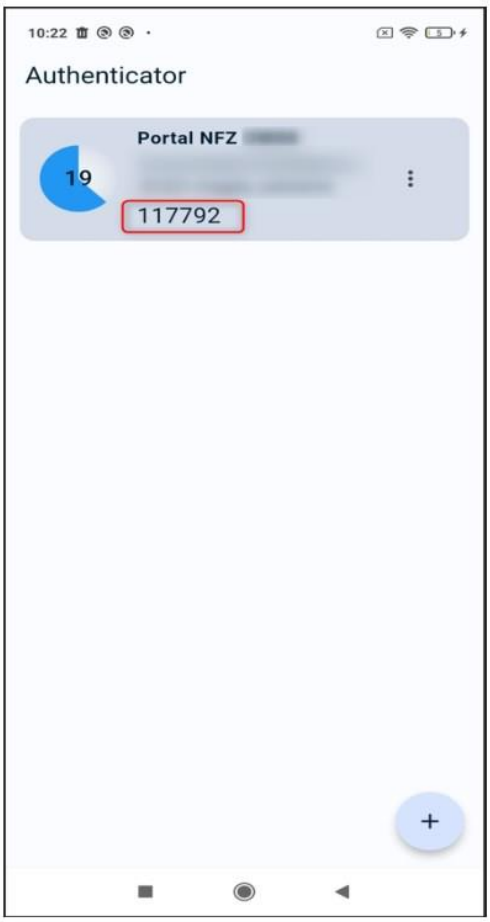
2. Po otwarciu formatki w aplikacji do uwierzytelniania operator dodaje i skanuje kod QR na aplikacji zewnętrznej.



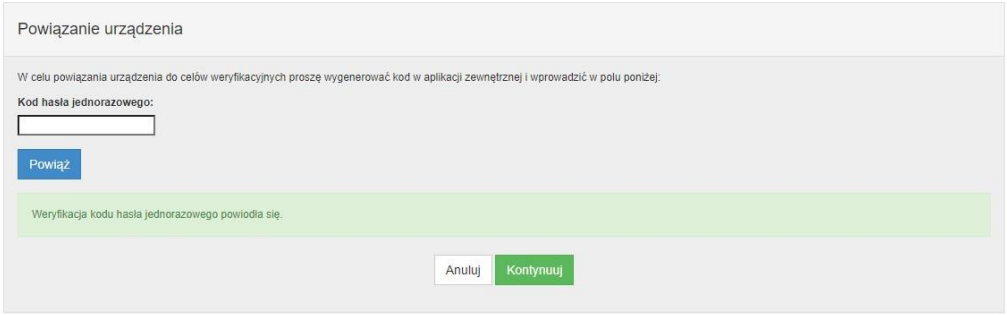
3. Zamiast zeskanowania można kliknąć w **Dodaj konto ręcznie**.



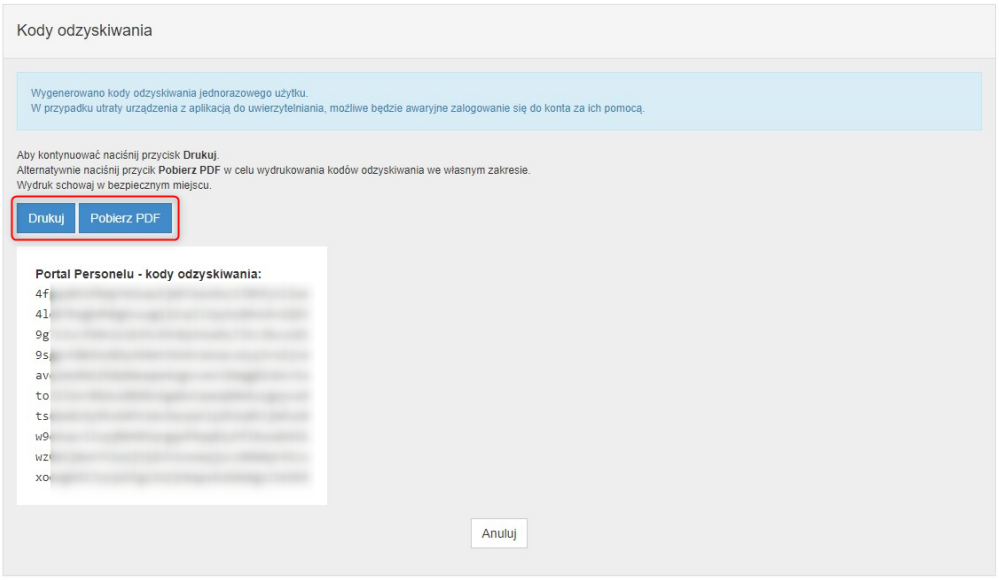
4. Po udanym powiązaniu urządzenia, aplikacja jest gotowa do uwierzytelnienia wieloskładnikowego.



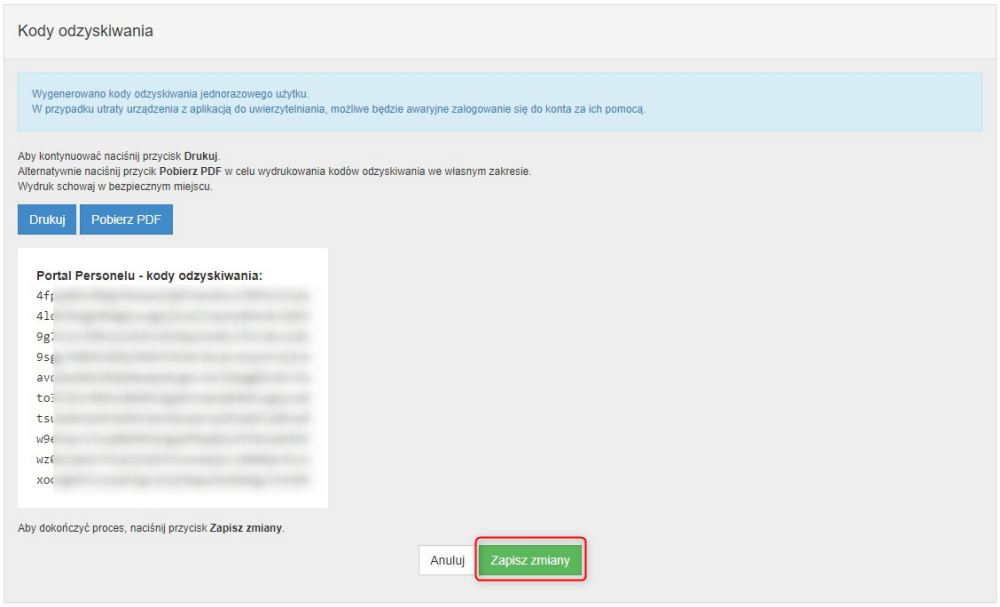
5. Operator przepisuje kod z aplikacji zewnętrznej do portalu i klika w **Powiąż**.



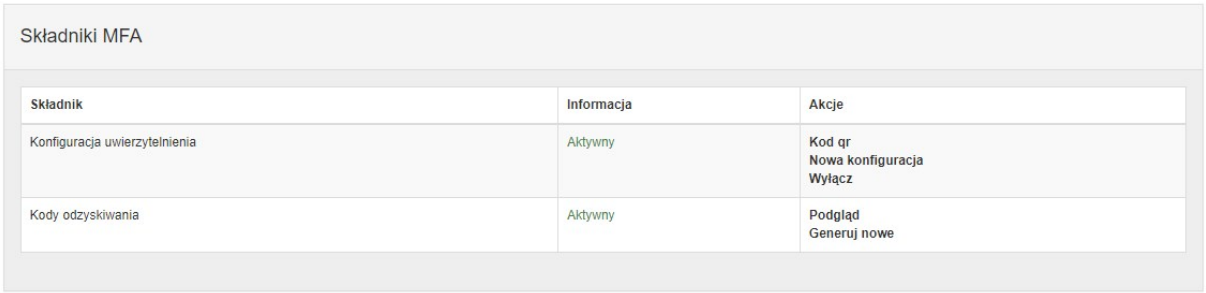
6. Po prawidłowym powiązaniu pokaże się informacja **Weryfikacja kodu hasła jednorazowego powiodła się** oraz lista kodów odzyskiwania.
Lista kodów odzyskiwania jest to lista 10 kodów, które można użyć w przypadku problemów z użyciem aplikacji uwierzytelniającej np. zgubienia lub uszkodzenia telefonu.
Kody należy zapisać lub wydrukować. Bez tej czynności program nie będzie mógł zakończyć konfiguracji.



7. Po wydrukowaniu/zapisaniu kodów operator zapisuje konfigurację za pomocą klawisza **Zapisz zmiany**.



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



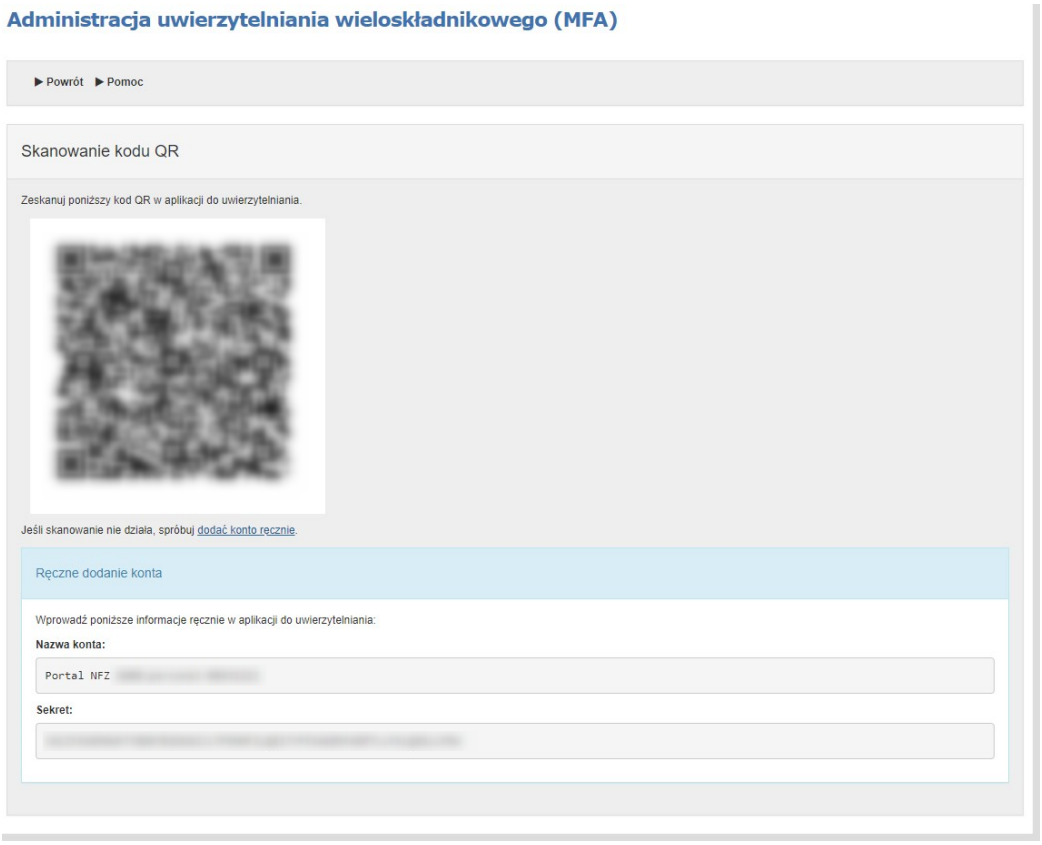
2. ADMINISTRACJA UWIERZYTELNIANIA WIELOSKŁADNIKOWEGO (TOTP)

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

A. 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 QG lub wpisanie kodu ręcznie.

Operator może wyświetlić **Kod QR**.

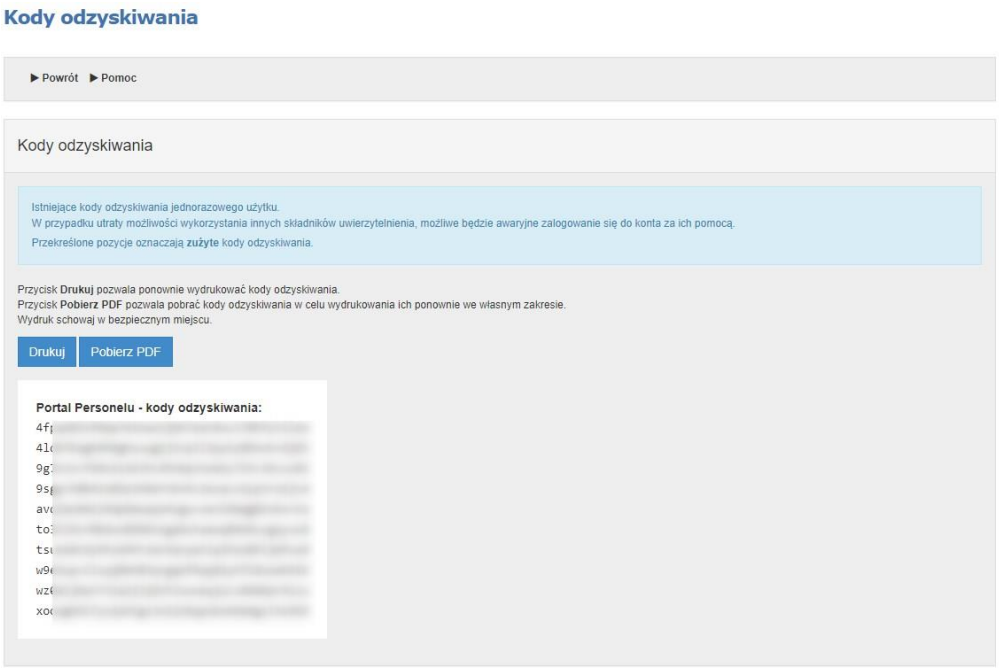


B. LISTA KODÓW ODZYSKIWANIA

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.



Aby wygenerować nowe kody odzyskiwania należy przejść do strony **Zarządzanie uwierzytelnieniem wieloskładnikowym** i skorzystać z linku **Generuj nowe.**

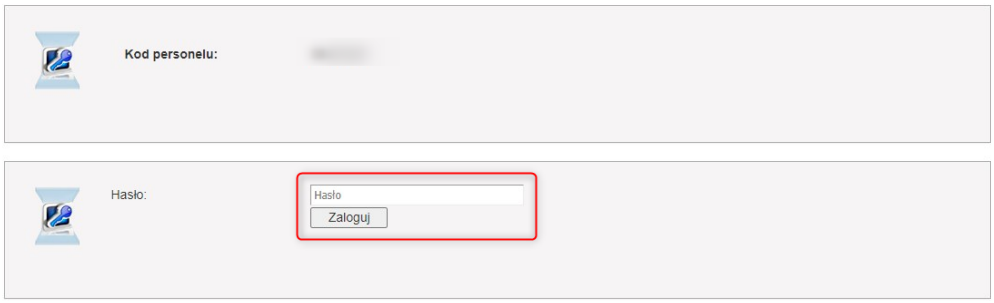
Kody, które zostały wykorzystane są oznaczone jako **Wykorzystane** oraz dodatkowo przekreślone.

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

C. GENEROWANIE NOWYCH KODÓW ODZYSKIWANIA

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

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



Po wpisaniu hasła otworzy się strona z wygenerowanymi kodami odzyskiwania.
Przycisk **Zapisz**, zapisuje kody odzyskiwania.
Przycisk **Drukuj** umożliwia wydrukowanie kodów odzyskiwania.